Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 5, Issue 1 (2025) p.17-57
DOI: https:doi.org/10.52907/jipit.v5i1.578

Gaps in Consumer Protection Regimes: Protecting Nigerians from Algorithmic Harms in the Digital Economy

*Ihuoma K. Ilobinso**

ABSTRACT

The adoption of digital technologies, particularly Artificial Intelligence (AI), big data, and algorithmic decision-making, has transformed consumer markets, offering unprecedented convenience and personalization. However, these innovations also present novel and complex challenges, such as dark patterns, personalized advertising, and algorithmic pricing, which undermine consumer autonomy, transparency, and fairness. This paper critically examines how Nigeria's consumer protection framework, notably the Federal Competition and Consumer Protection Act (FCCPA) 2018 and the Nigeria Data Protection Act 2023 (NDPA), responds to these emerging threats. It finds that while existing laws address traditional market imbalances, they are insufficient to regulate opaque and exploitative digital practices. Strengthening the legal and regulatory framework is therefore essential to safeguarding consumer rights in an AI-driven economy. Drawing on regulatory experiences in the European Union, the United States, and India, this paper examines the limitations of Nigeria's current regulatory regime and offers recommendations to reform consumer protection laws to ensure optimal protection for consumers in the digital marketplace.

Keywords: Consumer Protection, Artificial Intelligence, Targeted Advertising, Dynamic Pricing, Unfair Trade Practices

* Legal practitioner and lecturer at the Department of Commercial and Industrial Law, University of Lagos, Nigeria. Her research focuses on the intersection of law and technology, with emphasis on the impact of emerging technologies on vulnerable groups.

TABLE OF CONTENTS

I. INTRODUCTION

Consumer protection has undergone significant transformation over the years, evolving in response to shifts in market dynamics, technological advancements, and increasing consumer vulnerability (Howells et al., 2019). While it aims to address traditional imbalances of power, information, and resources between consumers and sellers, the modern digital economy, driven by Artificial Intelligence (AI), big data, and algorithmic decision-making, presents new and complex risks. This paper explores how Nigeria's consumer protection framework addresses these emerging challenges, particularly in the context of opaque and exploitative digital practices.

Historically, consumer protection mechanisms were informal and unstructured, emerging from customary practices and moral obligations (Cartwright, 2001). The industrial revolution and urbanization prompted the first legislative responses to abusive business practices and unsafe products. By the mid-twentieth century, consumer protection laws became more institutionalized, particularly in response to globalization, mass production, and the rise of consumerism (Trentmann, 2006). This period saw the emergence of national regulatory bodies and the establishment of foundational consumer rights (Khan, 2017). The advent of the internet, along with the rapid growth of e-commerce, digital platforms, and cross-border transactions, ushered in a new era of consumer protection. These developments necessitated reforms to ensure that consumer protection frameworks address the unique challenges of the digital environment, mandating that businesses provide pre-contractual information about transactions in a transparent manner and that consumers receive a cooling-off period during which they can withdraw from purchases without penalty or explanation (Ilobinso, 2023).

However, recent advancements in AI, big data analytics, and machine learning have introduced more complex challenges to consumer protection. Businesses increasingly rely on al-

gorithms to automate critical decisions, such as pricing, product recommendations, and marketing strategies (OECD, 2023). While these innovations offer personalized services, convenience, and efficiency, they also pose risks related to transparency, fairness, and accountability. Manipulative practices such as dark patterns, algorithmic price discrimination, and targeted advertising exploit consumer behavior, potentially leading to financial harm and loss of autonomy (CMA, 2028).

These risks are compounded by limited regulatory oversight and the opaqueness of algorithmic processes. Furthermore, existing legal regimes may not adequately address the unique risks posed by digital and algorithmic commerce. In Nigeria, the Federal Competition and Consumer Protection Act (FCCPA, 2018) provides a foundation for consumer protection, but significant gaps remain in regulating AI-driven practices, data manipulation, and algorithmic transparency.

This paper, therefore, examines the extent to which Nigeria's current framework mitigates these harms and draws on international models, particularly from the European Union (EU) and the United States (US), to recommend reforms that strengthen Nigeria's consumer protection in the digital and AI-driven marketplace.

This paper is structured as follows: the first part, being this introduction, is followed by Part II, which discusses dark patterns, how they operate, why they are harmful to consumers, and the extent to which existing consumer protection and data protection laws respond to this emerging threat. It argues that dark patterns constitute a modern form of unfair trade practice and should be legally recognized and regulated. Part III discusses personalized advertising, its benefits, and the challenges it poses for consumers, with a view to regulating it. Part IV examines the implications of algorithmic pricing strategies for consumer welfare and market fairness, and how consumer data is used to set prices in a dynamic, often opaque manner, resulting in discriminatory outcomes, information asymmetry, and diminished

consumer autonomy. It also highlights how AI-driven pricing algorithms can facilitate anti-competitive practices. Part V offers regulatory and policy recommendations to reform consumer protection laws and ensure they provide optimal protection for consumers in the digital marketplace.

II. DARK PATTERNS AS UNFAIR PRACTICES

The term 'dark patterns' refers to user interface (UI) or User experience (UX) designs that are intentionally crafted to manipulate or deceive users into making decisions that they would otherwise not have made (Narayanan et al., 2020). The Guidelines for Prevention and Regulation of Dark Patterns (2023) issued by the Central Consumer Protection Authority (CCPA) of India provides a comprehensive definition of dark patterns as any:

> 'practices or deceptive design pattern using user interface or user experience interactions on any platform that is designed to mislead or trick users to do something they originally did not intend or want to do, by subverting or impairing the consumer autonomy, decision making or choice, amounting to misleading advertisement or unfair trade practice or violation of consumer rights' (CCPA, 2023).

The rise of dark patterns challenges the traditional objectives of consumer protection law, which is to redress the imbalance of power, information, and resources between consumers and businesses (Mathur et al., 2019). The imbalance allows companies to engage in misleading advertising, impose hidden charges, and deploy other unfair trade practices.

Dark patterns undermine consumer autonomy and choice, and subvert the consumer's capacity to make independent decisions (Sharma et al., 2023). They also raise privacy concerns (EDPB, 2023). In response, consumer law has evolved to empower consumers with rights, access to information, and mechanisms to prevent exploitation (OECD, 2022). For instance, Article IV of the United Nations Guidelines for Consumer Protection reinforces this evolution by requiring fair, honest, and ethical

dealings with consumers, specifically discouraging abusive marketing tactics and deceptive practices.

Unfair trade practices have been defined across jurisdictions as deceptive, misleading, or unethical conduct by businesses that undermines the consumer's ability to make informed choices.[1] Legal provisions such as Section 5 of the US Federal Trade Commission (FTC) Act (15 USC 45), articles 5 to 9 of the European Union's Unfair Commercial Practices Directive, regulations 3 to 7 of the United Kingdom's Consumer Protection from Unfair Trading Regulations, and sections 123 to 127 of Nigeria's FCCPA aim to prevent such conduct. However, these frameworks were not initially designed to address the manipulations enabled by digital interfaces. Traditional consumer protection laws focus on false or misleading claims, but dark patterns exploit cognitive biases through digital design (such as layouts, defaults, and nudges). Because they rely on interface architecture rather than outright misstatements, they blur the line between persuasion and manipulation, often producing small but cumulative harms, and increasingly drawing on personalization and real-time testing that traditional legal frameworks never anticipated. As a result, dark patterns evade existing prohibitions on 'unfair' or 'deceptive' practices, accentuating the need for updated rules that explicitly address design-based manipulation.

While existing laws may not explicitly address dark patterns, regulatory frameworks are increasingly evolving to encompass manipulative digital practices. Through regulatory actions and the courts, particularly by the FTC (for instance, in the Supreme

[1] Section 5 of the U.S. Federal Trade Commission Act declares unfair or deceptive acts or practices in or affecting commerce unlawful; EU Unfair Commercial Practices Directive (2005/29/EC) prohibits commercial practices that are misleading or aggressive and likely to cause the average consumer to take a transactional decision they would not have otherwise taken; UK Consumer Protection from Unfair Trading Regulations 2008 prohibits unfair, misleading, and aggressive commercial practices that materially distort the economic behavior of consumers; Sections 120–124 of the Federal Competition and Consumer Protection Act (FCCPA) 2018 prohibit misleading representations, unfair contract terms, and deceptive marketing; Section 127 requires that consumer agreements not be unfair, unreasonable, or unjust.

Court case of *FTC v. Sperry & Hutchinson C. (1972))* and the EU Unfair Commercial Practices Directive, modern legal interpretations acknowledge that a practice need not be overtly false or coercive to be considered unfair (European Commission, 2022). It is sufficient if a practice misleads, exploits power imbalances, or interferes with rational consumer decision-making. In this respect, dark patterns align with the conceptual definitions of unfair trade practices, as they leverage interface design to subtly manipulate user behavior rather than resorting to overt misrepresentation.

Dark patterns, therefore, represent a modern form of unfair trade practice, where the interface itself, not the contractual terms, is the mechanism of exploitation. Consequently, they warrant explicit recognition and regulation as a distinct category of unfair trade practices. The FTC, in its report, stated that research shows that dark patterns are highly effective at influencing consumer behavior. For example, a study discussed at the workshop organized by the FTC in April 2021 found that:

> 'dark patterns doubled the percentage of consumers who signed up for a dubious identity theft protection service, as compared to consumers who were presented with a neutral interface. Moreover, these effects increased significantly when test subjects were exposed to more than one dark pattern' (FTC, 2022).

Dark patterns have become very pervasive as businesses have been found to design the user interface of their websites, apps, or devices in a manner that intentionally deceives or pressures consumers into spending more money, sharing personal data, signing up for unwanted services, and making it difficult to unsubscribe from services (Sharma et al., 2023). They do this by tricking consumers into accepting tracking cookies and consenting to data collection. They manipulate consumers into making purchases they ordinarily would not make through techniques such as emotional triggers, urgency tactics, persuasive design, and forced continuity (Zard & Shears, 2023). Moreover, studies have shown that emotions influence purchasing decisions (Shiv

& Fedorikhin, 2019). To properly understand dark patterns and their various forms, the following sub-section examines their main types.

1. Subscription trap or Roach motel

One form of dark pattern is the 'Subscription Trap/Roach Motel', where businesses design seamless subscription processes for services while making cancellation complex, lengthy, or simply impossible. The designs are made to keep subscribers trapped and continuously being charged for services they do not use or wish to discontinue, thereby hindering consumer autonomy. This has been the experience of many consumers. For example, comedian Trevor Noah once made a tweet stating that it is 'amazing how you can subscribe to any service instantly & they take your $ with one click but when you try to cancel, suddenly you need to call their helpline which is always too busy and so you have to find a dragon to fly you to Mordor to slay your subscription in the flesh'.

In *FTC v. Vonage Holdings Corp.,* the US Federal Trade Commission brought an enforcement action against Vonage, a voice-over internet protocol provider, alleging that it engaged in unfair and deceptive practices by making it difficult for consumers to cancel their services, thereby violating section 5 of the FTC Act and Section 5 of the Restore Online Shoppers' Confidence Act ('ROSCA'). The defendant required consumers to speak with their agent to cancel services, and consumers complained that they encountered delays and hurdles in getting the company to cancel. In some cases, they were charged even after attempting to cancel and had to restart the cancellation process. In 2022, Vonage agreed to a $100 million settlement. They also agreed to simplify their cancellation process. In the same vein, ABCmouse, an online learning platform for children, agreed to a $10 million settlement in the case of *FTC v Age of Learning Inc.,* resolving the court action in which it was alleged that the defendant engaged in deceptive marketing and made it difficult to cancel

the subscription. Similar efforts were made by the EU Consumer Protection Cooperation (CPC) Network and the Norwegian Consumer Council (Forbrukerradet) with respect to the Amazon Prime subscription process in 2022 (EC, 2025) (Myrstad, 2022).

2. Forced continuity

In addition to the subscription trap, some businesses engage in 'Forced Continuity' where subscribers to a free service are enrolled automatically in a recurring subscription after a free trial without a clear or timely notification. In *FTC v. Age of Learning Inc.,* one of the allegations against ABCmouse was that it violated the ROSCA by failing to provide clear information about its billing practices. Consumers complained that they were required to provide payment details to access the free-trial membership. However, the company did not provide clear information that the subscription will be renewed automatically and indefinitely upon the end of the initial period. The parties settled out of court. The company agreed to pay $10 million in consumer refunds. While ABCmouse did not formally acknowledge engaging in unfair business practices, it was legally bound by the settlement to change its practices and compensate consumers.

3. Sneak into the basket

Another form of dark pattern is adding additional items, such as products, services, payments to charity, or donations, to the transaction at checkout without the consumer's consent. In some cases, the consumer might not notice the added item. For instance, some airlines add optional services like seat selection, luggage, and insurance charges at checkout without prior disclosure at the time of purchase (OECD, 2022). Some businesses sneak donations to charity into transactions without the consumers' notice or consent. In some cases, consumers do not notice the charge until after they have paid.

4. Confirm shaming

This form of dark pattern uses phrases, images, videos, or audio to guilt-trip or create a sense of fear or shame in the consumer, so as to make them purchase a product or service or continue a service subscription. For instance, manipulative language like 'No thanks, I don't care about the environment' is used when trying to manipulate consumers to buy eco-friendly goods.

5. False urgency

The interface of a platform could also be designed to create a false sense of urgency and scarcity, pressuring consumers into impulse buying by dynamically adjusting stock availability, even when there is no need for urgency. This can be found in e-commerce sites where stock availability messages like 'Only 2 left in stock' or 'Only 1 room left' are flashing in red. These messages are not often based on the actual inventory level. In November 2024, the European Commission and national authorities launched an investigation into the Temu e-commerce platform for alleged unfair practices, including pressure selling, fake discounts, forced gamification, misleading information, and fake reviews. Temu was formally notified of potential infringements of EU consumer protection law and required to respond and undertake corrective measures (European Commission, 2024).[2]

6. Disguised ads or content camouflage

This dark pattern disguises advertisements as regular content, intentionally blurring the line between promotional and genuine material. By using deceptive design, strategic placement, or ambiguous labeling, businesses present ads as ordinary content, social media posts, or navigation buttons, effectively

[2] As at the time of writing, there is no publicly available final decision or enforcement outcome arising from the investigation launched in November 2024. The absence of a concluded enforcement action underscores the complexities and challenges associated with regulating dark patterns.

misleading consumers into making purchases or engaging with the content under pretenses.

This often happens where businesses pay influencers to promote their products without requiring them to disclose that the promotion or endorsement is sponsored. For instance, Warner Bros. Home Entertainment settled out of court a charge by the FTC, which alleged that it deceived consumers during a marketing campaign when it failed to adequately disclose that it paid influencers such as PewDiePie to play the video game 'Middle Earth: Shadow of Mordor' and post it on YouTube and social media (FTC, 2016). The company instructed the influencers to place the disclosure in a box that would appear 'below the fold', where consumers are unlikely to see it. FTC alleged that the sponsored video got over 5.5 million views. In 2020, the UK's Competition and Markets Authority (CMA) commenced an investigation into Instagram for failing to prevent hidden ads on its app and website, over concerns that social media influencers were posting content about businesses that disclosed they were incentivized to do so (CMA, 2020).

The European Commission, in coordination with the Consumer Protection Cooperation (CPC) Network, initiated an enforcement action against Star Stable Entertainment in March 2025 regarding potential unfair commercial practices in its online game directed at vulnerable children (European Commission, 2025). Some of the practices identified by the Commission which violates EU consumer protection laws was that advertisements within the game urged children to purchase in-game currency or items; dark patterns, particularly false urgency, was used to pressure children into making quick transactional decisions; that there was lack of transparency with respect to the purchase and use of in-game currency; and that the company allegedly failed to ensure that the influencers that promoted the game disclosed that they were paid or incentivized to do so, thereby misleading the young vulnerable consumers.

A. The Regulation of Dark Patterns

Sections 123 to 124 of the FCCPA broadly prohibit false, misleading, fraudulent, or deceptive 'representations', particularly with respect to unfair contract terms, misleading ads, and generally misrepresentation. The provisions did not anticipate psychological manipulations or addictive designs that cause harm to consumers. Certain design practices, such as false urgency, pre-ticked subscription boxes, or misleading 'free trial' claims, may qualify as deceptive representations within the meaning of the Act, since they convey information likely to mislead consumers about availability, consent, or pricing. However, many dark patterns do not rely on overt misstatements, but instead they manipulate the architecture of choice—for instance, by obscuring cancellation options (subscription trap and forced continuity) or exploiting cognitive biases through interface design (for instance, where the 'cancel' button is tiny and greyed-out or disguised). Because such tactics distort consumer decision-making without necessarily making a 'representation', they may fall outside the scope of Section 123. This highlights the inadequacy of traditional consumer protection laws, which are well-suited to regulating informational misrepresentations but less effective against more subtle, design-based manipulations.

Several other jurisdictions are increasingly recognizing and addressing dark patterns as a distinct category of consumer exploitation. In 2022, the United States FTC released the report 'Bringing Dark Patterns to Light', which provides extensive guidance on identifying and curbing manipulative design strategies. The report outlines specific examples, including subscription traps and forced continuity, that erode consumer autonomy. Similarly, the European Union's Unfair Commercial Practices Directive classifies manipulative designs as potentially unfair practices, emphasizing actions that distort or impair consumer decision-making (Lupiáñez-Villanueva et al., 2022). Article 25 of the EU Digital Services Act (DSA, 2022) and Recital 67 of the interpretative guidance further explain that dark patterns typ-

ically involve design, structure, or interface functionalities that prevent users from making autonomous, informed choices. It explicitly prohibits dark patterns in online interfaces, and it provides that:

> 'Providers of online platforms shall not design, organize or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions'.

It is important to note that DSA applies only to large online platforms such as Facebook, Instagram, and Google, not to all businesses in the online marketplace.

California's Consumer Privacy Rights Act (CPRA) defines dark pattern as 'a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation' (California Civil Code, 2023, § 1798.140 (l)). It provides that any consent obtained through such design is deemed invalid (California Civil Code, 2023, § 1798.140 (h)). This is to illustrate that Nigeria's consumer protection framework needs to evolve beyond conventional misrepresentation models to address the peculiar challenges posed by digital market manipulation.

In 2023, the Central Consumer Protection Authority of India issued a Guideline for the prevention and Regulation of Dark Patterns. The Guideline defines dark patterns and prohibits their use. It provides that non-compliance can lead to action under the Consumer Protection Act, 2019, including penalties for engaging in unfair trade practices. The Guideline serves as a framework for identifying and mitigating manipulative design strategies.

The European Commission is currently drafting legislation to protect consumers in the digital market against manipulative and unfair commercial practices—the Digital Fairness Act. This initiative was informed by the Commission's 2024 Digital Fairness Fitness Check Report. The report found that existing

consumer protection laws do not effectively address new challenges customers face online, particularly dark patterns that exploit consumers' cognitive biases to manipulate them. Aside from protecting consumers from harm, establishing specific rules that define and prohibit dark patterns will provide legal certainty for regulators and businesses. This will help businesses understand their obligations, ease compliance, and reduce litigation risks. It will also empower regulators by providing clear rules for enforcement actions.

Therefore, while Nigeria has some legal provisions that could be adapted to address dark patterns, there is a pressing need for a more specific regulatory intervention. These should include more precise definitions, a prohibition on dark patterns, platform accountability, and enforcement mechanisms to ensure that digital consumer protections keep pace with the growing sophistication of online manipulation.

III. PERSONALIZED ADVERTISING

Personalized advertising, often referred to as targeted or behavioral advertising, is the practice of delivering advertisements to consumers based on the collection, analysis, and use of their personal data, browsing history, online behavior, demographic attributes, or inferred preferences. Unlike traditional advertising, which speaks to a mass audience, personalized advertising is uniquely intrusive because it penetrates the private, data-driven sphere of consumers' lives. This uniqueness lies in the automated profiling mechanisms that operate in the background without the consumer's active awareness or participation. These strategies leverage AI, machine learning (ML), and big data analytics to process vast volumes of consumer data, including location, online activity, purchasing patterns, app usage, and demographic details such as age, gender, income, relationship status, and social media accounts.

The data is collected through various tracking mechanisms, such as web cookies, web beacons, device fingerprinting, mobile app tracking, and smart devices. ML algorithms continuously analyze these data to identify behavioral patterns, segment users into marketable categories, and predict individual preferences. For instance, a consumer's behavior, interests, values, and lifestyles can be predicted when a consumer spends some time on a particular webpage, clicks on an item, or engages with a post by liking, sharing, or commenting—as such activities signal the consumer's interest in specific products or services. These insights are used to deliver highly tailored advertisements that maximize user engagement. For example, a user identified as interested in fitness products may begin to see a stream of targeted ads for supplements, workout gear, or weight-loss or weight-gain programs.

Additionally, personal information consumers voluntarily provide, such as sex, age, and country of residence, can also be used to reach relevant audiences. Other data can include education level, income bracket, relationship status, parental status, and employment sector. Targeted advertising can also be predictive, using AI and ML. For instance, Target, a store in the USA, made headlines when it predicted from the consumer data that the consumer was pregnant and sent her marketing booklets for diapers (Duhigg, 2012). This highlights the exceptional risks of personalization compared to conventional marketing.

There are claims that smartphones secretly listen to users' conversations and collect related data for targeted advertising, as users often notice ads connected to their recent discussions (Widmer, 2025). This concern was central to a 2019 class action filed against Apple in the California Federal Court, alleging that the company's voice assistant, Siri, violated users' privacy by recording private conversations and sharing them with third parties without consent (*Lopez* v. *Apple Inc*., 2019). Reports indicated that Siri was sometimes unintentionally activated, allowing contractors reviewing its performance to overhear personal and

sensitive exchanges. Some plaintiffs also observed that advertisements appeared soon after they had verbally discussed certain products (Stempel, 2025). While denying the unfair practice, Apple agreed to a $95 million settlement in 2024 (Nairn, 2025). Companies, like Google and Meta, generally deny actively eavesdropping on users' private conversations for advertising purposes. Instead, they explain that targeted advertisements are based on data collected through users' digital activities across websites and applications (Widmer, 2025).

Notwithstanding, targeted advertising offers several benefits for both consumers and businesses. Since they are personalized, they reduce the generic ads individual consumers would otherwise receive. In other words, individual consumers receive more relevant adverts about goods and services they are interested in. Campaigns can be launched, modified, or terminated at any time, providing flexibility and responsiveness. Advertisers can monitor performance in real time by tracking click-through rates, purchase conversions, and other metrics, enabling timely adjustments to optimize results (Oko-Epelle et al., 2022). Despite these benefits, there are concerns about data privacy, behavioral manipulations, consumer autonomy, and transparency.

A. Data Privacy Concerns in Personalized Advertising

Targeted advertising relies heavily on personal data, as advertisers use information collected from online activity to profile individual consumers and influence their purchasing decisions. While Nigeria's Data Protection Act (NDPA) and the Federal Competition and Consumer Protection Act (FCCPA) recognize key principles such as consent, transparency, and the right to information, these instruments do not yet provide comprehensive safeguards against the risks of algorithmic profiling, behavioral manipulation, and opaque data ecosystems that drive targeted advertising.

Although the NDPA grants data subjects the right to privacy and requires clear information on data collection, purpose,

and sharing (NDPA Sections 25-27), it lacks specific provisions mandating algorithmic transparency or requiring advertisers to disclose when ads are targeted based on behavioral profiling. Consumers are often unaware of when automated decision-making tools are used to personalize content or offers, and the NDPA does not prescribe mechanisms for independent auditing or accountability of these algorithms. Similarly, while the NDPA gives individuals the right not to be subject to decisions based solely on automated processing (Section 34 NDPA), this right is practically ineffective where consumers cannot detect such processing or where consent is bundled into complex privacy policies that discourage informed choice. Many online businesses still rely on default tracking settings and vague or overly technical privacy notices, contrary to the spirit of section 27(3) of the NDPA, which requires that consent be freely given, specific, and informed.

The FCCPA also does not explicitly regulate the intersection between consumer protection and data-driven advertising, leaving uncertainty about overlapping mandates between the Federal Competition and Consumer Protection Commission (FCCPC) and the Nigeria Data Protection Commission (NDPC). Therefore, the gap lies not in the absence of legal principles, but in the lack of explicit, detailed, and enforceable rules governing algorithmic profiling, ad transparency, and accountability for digital advertisers.

In the European Union, the GDPR does not operate in isolation. It is complemented by the ePrivacy Directive (2002/58/EC), which regulates privacy and confidentiality in electronic communications. The ePrivacy Directive specifically addresses tracking technologies and direct marketing practices that are essential to personalized advertising. It requires that websites obtain prior, informed user consent before storing or accessing cookies or similar identifiers on a user's device (Article 5(3)). It also establishes rules for sending unsolicited direct marketing communications via electronic means, such as email, SMS, or automated calling systems (Article 13). Together, the GDPR and the ePrivacy Di-

rective ensure both data protection and communications privacy, forming a dual-layer framework for responsible digital marketing.

By contrast, Nigeria lacks an equivalent to the ePrivacy Directive. The NDPA (2023) governs the general processing of personal data but does not establish explicit obligations concerning online tracking or unsolicited electronic marketing communications. Consequently, several online advertising practices, particularly those relying on behavioral tracking, operate in a grey area that is only indirectly addressed under the NDPA or through consumer protection and advertising regulation under the FCCPA and the ARCON Code. This underscores the need for targeted legislative intervention or subsidiary regulations to operationalize these protections.

B. Behavioral Manipulation and Consumer Autonomy

Some advertising strategies exploit users' cognitive biases, emotional states, and vulnerabilities. They use algorithms that analyze consumers' moods or mental states based on online behavior (Nie et al., 2024). For instance, individuals flagged as lonely or experiencing self-esteem issues may be targeted with advertisements for beauty enhancement products, dating apps, or weight loss programs when they are most emotionally susceptible (Susser, Roessler, & Nissenbaum, 2019). Users who are flagged as financially desperate or low-income may be targeted with high-interest short-term loans or exploitative credit facilities (Eubanks, 2018). Additionally, betting companies could push advertisements to individuals who have been profiled as having the tendency to become addicted to gambling or to re-engage individuals who are trying to quit gambling (ICO, 2025).

This form of manipulation raises ethical concerns. Consumers may be nudged into purchases not through rational decision-making, but through exploitation of their emotional or psychological state. This practice undermines consumer autonomy. What makes personalized advertising especially problematic is

that it blurs the line between persuasion and manipulation. Existing Nigerian laws prohibit misleading or deceptive representations, but they do not capture subtle psychological exploitation that occurs without overt misstatements.

There are concerns that children are also profiled and targeted by advertisers. This usually occurs where the adverts are delivered through shows or games played by children (UNICEF, 2019). Children are particularly susceptible to persuasive techniques used in the digital environment, such as the bright visuals, cartoon characters, and reward-based prompts that appeal to emotions rather than reason. Businesses also push personalized content that exploits children's interests to increase the likelihood of impulsive clicks or requests to parents. These adverts often blur the line between entertainment and marketing, manipulating children's choices without them realizing they are being marketed to.

Algorithms may inadvertently expose children to inappropriate adverts that could harm their mental health, self-esteem, and body image. This gap in protection underscores the inadequacy of Nigeria's regulatory approach when compared to the European Union's General Data Protection Regulation (GDPR), which expressly prohibits profiling and automated decision-making involving children. Article 22(1) of the GDPR provides that data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling', and Recital 71 clarifies that such automated decision-making 'should not apply to a child.' This prohibition reflects the understanding that children are particularly vulnerable and often lack the cognitive maturity to comprehend complex data-driven decisions or provide informed consent.

In contrast, the NDPA contains no equivalent prohibition on profiling children. Section 31(1) of the NDPA merely requires data controllers to obtain 'verifiable parental or guardian consent' before processing a child's personal data and to ensure that such processing is in 'the best interest of the child.' While this

aligns with Article 3 of the United Nations Convention on the Rights of the Child and Section 1 of Nigeria's Child's Rights Act, it does not directly restrict profiling or automated targeting of children. Consequently, the NDPA provides general protection rather than a categorical ban, leaving a regulatory gap in one of the most vulnerable areas of digital advertising. The Nigerian Code of Advertising Practice (2023), issued by the Advertising Regulatory Council of Nigeria, similarly urges caution in advertising to minors but focuses on content ethics rather than data-driven profiling (Osinbajo, 1991).

C. Erosion of the Right to Information and Informed Consent

The right to information is a fundamental consumer right. This right ensures that consumers are provided with accurate, timely, and sufficient information about a product and a transaction so they can make informed choices (Ilobinso, 2022). The FCCPA recognizes the consumer's right to information presented in plain language and in an understandable manner. It also requires that consumers be provided with information about a product, its price, quality, and terms, etc. Section 123 of the FCCPA prohibits false, misleading, or deceptive representations in connection with the promotion or supply of goods or services. This right applies irrespective of the mode of transaction and therefore extends to digital advertisements and promotional messages, including those disseminated through influencers, social media, and automated advertising platforms.

Sections 17 and 18 of the FCCPA prohibit deceptive marketing and require businesses to disclose material information affecting consumer decisions. The lack of transparency and accountability is generally a problem, as the algorithms used for advertising are often opaque, making it difficult for consumers and regulators to understand how decisions are made and to detect biases, discrimination, and unfair pricing.

Some advertisers disguise advertisements as regular content in contravention of Section 2(1)(g) of the Advertising Regulatory Council of Nigeria (ARCON) Act and Code of Advertising Practice. The ARCON Guidelines on digital and social media advertising require that all paid endorsements or sponsored content be clearly disclosed to the public and not disguised as authentic user-generated content (Pavestones Legal, 2025). Some businesses use deceptive design, strategic placement, or ambiguous labeling to present advertisements as ordinary content, social media posts, or navigation buttons, thereby misleading consumers into making purchases or engaging with the content under pretenses. Failure to label promotions as paid or sponsored undermines the consumer's right to know the commercial intent behind the message. While FCCPA Section 123 prohibits misleading representations, it does not explicitly recognize the category of deceptive practices that exploit cognitive biases, thereby leaving regulators to stretch existing provisions. Such practices can distort consumer autonomy, especially when algorithms target users based on their behavior, preferences, or vulnerabilities.

D. Personalized Advertising and the Existing Regulatory Gaps

Although the provisions of the FCCPA and NDPA can serve as a legal basis for regulating deceptive algorithmic advertising techniques, they do not adequately address the full scope of legal risks arising from personalized advertising. The uniqueness of personalized advertising lies in its data-driven, predictive, and manipulative design, which differs fundamentally from traditional marketing. Current Nigerian regulations, though helpful, remain piecemeal rather than comprehensive, leaving consumers vulnerable to opaque algorithmic practices.

On the one hand, the FCCPA prohibits unfair, misleading, and deceptive marketing and trade practices under sections 123 to 125. In other words, it already covers certain aspects of targeted advertising, particularly those that involve misrepresentation, such as advertisements that present harmful products as

harmless or exaggerate the benefits of a product. However, the FCCPA speaks in general terms about representations and does not explicitly address data-driven advertising practices in which the harm stems not from false claims but from the manipulative use of consumer data. For instance, practices such as behavioral profiling or microtargeting can unduly influence consumer decision-making without making any objectively false claims, thereby falling outside the traditional scope of 'misleading' representation and making enforcement difficult.

The FCCPA also requires businesses to provide consumers with pre-contractual information, including the price, a description of the goods, the mode of delivery, and the place of business. Yet these obligations relate primarily to the transactional content of the sale rather than the informational ecosystem of digital targeting. Crucially, the FCCPA does not require businesses to disclose that consumers are being profiled, the logic behind the targeting, or the reason they are being shown specific advertisements. It also does not create a consumer right to opt out of targeted advertising. Likewise, it fails to provide an explicit prohibition on the use of consumer data to exploit vulnerable individuals, such as children, the elderly, financially distressed, or persons struggling with addictions. These omissions leave significant gaps in protecting consumers from non-transparent, manipulative, and discriminatory dimensions of targeted advertising.

The NDPA, on the other hand, represents an important step toward recognizing consumers' privacy rights, particularly in the context of data-driven practices. While the NDPA provides the overarching legal foundation for personal data governance in Nigeria, its role in regulating personalized advertising is indirect rather than sector-specific. This position mirrors the relationship between the EU General Data Protection Regulation (GDPR) and digital advertising in Europe. Under the GDPR, personalized advertising is not prohibited, but it is strictly conditioned on compliance with data protection principles, particularly lawful

processing (Article 6), informed consent (Article 7), transparency obligations (Articles 13 - 14), and the right to object to processing for direct marketing (Article 21). Additionally, Article 22 and Recital 71 restrict automated profiling that significantly affects individuals, especially children.

In the same way, the NDPA governs the collection, processing, and sharing of consumer data that underpin targeted advertising but does not itself regulate advertising practices or content. The NDPA ensures that any data used for personalized marketing must be collected with the data subject's freely given and informed consent (s. 26), that individuals are entitled to be informed of how their data is processed (s. 34(1)(a)-(b)) and that data subjects have the right to object to such processing (s. 35(1)(a)). However, unlike the European Union's broader and complementary regulatory framework, which combines the General Data Protection Regulation (GDPR) with the ePrivacy Directive and the Digital Services Act (DSA, 2022) to impose explicit advertising transparency obligations, the NDPA operates largely in isolation. It does not mandate advertisers to disclose why a consumer sees a specific advert, which data was used for targeting, or who sponsored the content.

Therefore, while data protection laws like the GDPR and the NDPA form the backbone of lawful data use in advertising, consumer protection and advertising laws, notably the FCCPA and ARCON Code, remain the primary instruments for addressing unfair, deceptive, or manipulative advertising conduct. The NDPA safeguards privacy and consent, while the FCCPA ensures fairness and transparency in commercial communication. Nigeria's challenge thus lies not in the absence of legal provisions, but in the fragmentation of regulatory responsibilities and the lack of clear, advertising-specific transparency obligations akin to those under the EU DSA and ePrivacy Directive.

IV. ALGORITHMIC PRICING STRATEGIES AND CONSUMER HARM

To maximize revenue and improve market efficiency, businesses deploy AI, ML, and data analysis to set and adjust prices of products offered to consumers (MacKay, 2022). The price adjustment is done in real time, based on factors such as demand fluctuations, consumer behavior, competitor pricing, inventory levels, and currency fluctuations. This pricing model, known as algorithmic pricing, is often used by businesses in the e-commerce, transportation, finance, and hospitality industries. While not all algorithmic price strategies are innately harmful to consumers or illegal, as in some cases they lead to improved customer service and satisfaction, some algorithmic pricing strategies, like personalized pricing, where prices are adjusted based on competitors' behavior, raise consumer protection, competition, and data privacy concerns.

Personalized pricing raises concerns about consumer harm because prices for goods and services are not simply adjusted due to a surge in demand or timing, but instead based on knowledge derived from individual consumer data. Consumers are tracked and their data obtained from their online activities. Such data include consumers' browsing history, purchase patterns, the device used (BBC, 2012), income level, and geographic location. In personalized pricing, different prices are displayed for different consumers for the same products (Ennis and Lam, 2020). For instance, consumers who use more expensive devices, live in upscale areas, or shop at high-end stores are charged more because the system has been trained to perceive such people as able and willing to pay higher prices. This is unlike situations in which the price adjustments apply to all consumers equally or in which consumers are aware of the biased treatment and can make informed decisions about whether to proceed with a transaction.

According to an experiment done by Mahambare et al. (2024), where IOS (iPhone) and Android devices were used simultane-

ously to make hotel reservations, the iPhone was charged a much higher price than the Android device for the same date, same type of room, and same hotel. In 2022, the Netherlands Authority for Consumers and Markets (ACM) investigated the online marketplace 'Wish' for employing undisclosed personalized pricing strategies and promoting potentially deceptive discounts (Rott, 2022). Wish had been adjusting prices based on factors such as consumers' purchase history and geographic location without informing customers. In response to ACM's actions, Wish ceased the use of personalized pricing in the European Union as of May 25, 2022, and prohibited merchants from offering false discounts on its platform (Rott, 2022).

Generally, price discrimination is mostly legal and has been practiced by businesses for centuries to maximize profit (Stole, 2007). Traditional price discrimination involved simple market segmentation, in which consumers such as students and seniors received discounts based on their status. However, advancements in digital technology have transformed this once-simple practice into a data-driven, opaque system. Algorithms now analyze vast amounts of personal and behavioral data to predict each consumer's willingness to pay and automatically adjust prices in real time. This automation enables businesses to change prices within minutes, something that would have taken days using traditional methods, while also making it difficult for consumers to understand or detect when and why different prices are being offered. For instance, Amazon adopts a dynamic pricing model that makes over two hundred and fifty million US dollars in price adjustments every day. This volume of price adjustment cannot be compared with that in the traditional market, where human intervention is required for implementation (Naceva, 2024).

In 2011, the price of a book being sold on Amazon, 'The Making of a Fly' by Peter A. Lawrence, skyrocketed to twenty-three million US dollars due to two competing algorithmic pricing strategies used by two different sellers (Eisen, 2011). The first seller used an algorithm that automatically set the book's price

slightly higher than the second seller's. In contrast, the second seller's algorithm automatically sets the price of the book to a price slightly lower than the first seller's price. This resulted in the book's price spiraling upwards to twenty-three million US dollars per copy (Eisen, 2011). This demonstrates how unsupervised algorithmic pricing can go wrong and how it affects goods and services.

Studies have shown that personalized pricing based on consumer data is mainly perceived as discriminatory and unfair (Poort & Zuiderveen Borgesius, 2019). It raises concerns about fairness and transparency, as consumers are often unaware that they are being charged different prices from other customers and that their data is being used to adjust those prices. This lack of transparency creates information asymmetry between businesses and consumers and raises questions about whether there is genuine party autonomy in such transactions. On the one hand, businesses, armed with sophisticated algorithms and extensive consumer data, possess superior information that enables them to set strategic, individualized prices. On the other hand, consumers remain unaware that the prices they see may have been adjusted based on personal data such as their browsing history, location, or purchasing power. In such circumstances, it is difficult to argue that both parties are making informed transactional decisions. When consumers unknowingly pay higher prices due to algorithmic manipulation, their economic interests are directly undermined.

While Nigeria and several other jurisdictions currently lack explicit legal frameworks regulating unfair algorithmic pricing, this does not mean such practices fall entirely outside the scope of legal scrutiny. For instance, both the UK's Consumer Protection from Unfair Trading Regulations 2008 and Nigeria's Federal Competition and Consumer Protection Act (FCCPA) prohibit misleading or deceptive commercial practices. In this context, personalized pricing algorithms that adjust prices based on user data without adequate disclosure may violate provisions requir-

ing fair, transparent, and informed consumer transactions. While not directly addressed, unfair algorithmic pricing may be implicitly covered under existing consumer law frameworks, though enforcement remains a challenge. This is because algorithmic pricing systems are often opaque, proprietary, and dynamically adaptive, making it difficult for regulators and consumers to detect discriminatory pricing practices or establish intent and causation. This challenge is compounded in cross-border digital markets, where traders may be located outside the consumer's jurisdiction, limiting investigative reach. The absence of explicit regulatory standards and technical audit powers significantly constrains enforcement.

Additionally, algorithmic price adjustments based on personal attributes such as age, gender, ethnicity, disability, or socio-economic status may amount to discriminatory practices, potentially violating Section 42(1) of the Constitution of the Federal Republic of Nigeria (1999 as amended), which prohibits discrimination on such grounds. For instance, opaque data used to determine pricing, particularly in sectors like insurance, raises concerns about indirect discrimination. When consumers are unaware of how their data is used or are denied the ability to opt out, pricing algorithms may unintentionally reinforce existing social biases, disproportionately impacting vulnerable groups (CMA, 2021).

Due to the central role of personal data in personalized pricing, data protection frameworks such as the NDPA play an important supporting role in ensuring lawful data use. Although the NDPA does not directly regulate pricing practices, since this is not its primary objective, it provides safeguards for how businesses collect and process personal data. Section 25 mandates that data processing must have a lawful basis, usually requiring the consumer's informed consent, particularly where sensitive data is involved. However, in practice, many consumers remain unaware that their data contributes to price personalization, and privacy notices, where consent is typically sought, are often lengthy and difficult to understand.

Section 27 of the NDPA requires data controllers to disclose the type and purpose of data collected, the impact of its processing, and whether automated decision-making (such as algorithmic pricing) is involved. Failure to disclose such information constitutes a breach of data protection rights. The NDPA further provides consumers with the right not to be subject to automated decisions that significantly affect them and the right to opt out of such processes. Accordingly, consumers should be offered transparent alternatives to algorithmic pricing and mechanisms to challenge such outcomes.

Growing global concern about opaque and exploitative pricing strategies has led to regulatory scrutiny. For example, the UK's Competition and Markets Authority launched a review following the public backlash over dynamic price hikes for the Oasis Reunion Tour in November 2024 (CMA, 2021). Similarly, in October 2024, the Australian government initiated consultations to reform consumer protection laws in response to concerns around AI-driven pricing and unfair trading practices (Gilbert + Tobin, 2024).

A. AI-Driven Pricing and the Risk of Collusion

In addition to concerns about algorithmic pricing being unfair to consumers, there are concerns that it reduces market competition, leads to higher prices, and limits consumer choice. Competition laws protect consumers by ensuring fair market practices and preventing anti-competitive practices. This is based on the idea that when markets are competitive, consumers benefit from diverse alternatives and access to high-quality products at competitive prices (Adekunle, 2022). The increasing use of algorithms to adjust prices has raised competition law challenges, especially regarding collusive price fixing.

Price fixing is the practice in which companies agree to set higher prices for products rather than allowing market forces to determine prices. This results in consumers paying higher prices than they should ordinarily pay for products. The practice of us-

ing AI to adjust prices is raising concerns about its potential to result in algorithmic collusion (OECD, 2017). AI-driven pricing algorithms can enable collusive price fixing explicitly, implicitly (tacit collusion), Hub and Spoke Collusion, and self-learning collusion.

Algorithms can be used to monitor and generally implement existing price-fixing agreements. In this instance, businesses use algorithms to detect and respond to deviations from their price-fixing agreements, thereby reducing the risk of errors or accidental deviations from the collusive agreement. Unlike traditional collusive price-fixing agreements, which require direct human communication, algorithmic cartels use AI tools to automate price monitoring. The AI system tracks the competitors' prices, where it detects deviations from their agreements. The algorithm automatically punishes the deviating party by lowering their prices (Ezrachi and Stucke, 2016). For instance, in 2016, the UK Competition and Markets Authority (CMA) found that two competing online sellers had breached competition law in this light (CMA, 2016). The case involved Trod Limited and GB Eye Limited, sellers on Amazon Marketplace. Trod raised concerns that GB Eye, as a competing seller on Amazon Marketplace, was undercutting its prices. In response, the two companies agreed not to undercut each other. Their arrangement aimed to maintain identical prices whenever possible, to raise prices in an amicable manner, and to share sales. To enforce this agreement, both sellers used automated pricing software to monitor and adjust their prices, ensuring neither undercut the other. They also maintained communication to oversee the pricing arrangement and address any issues related to the software's operation. The CMA determined that GB Eye and Trod had violated competition law by engaging in an illegal price-fixing cartel and issued fines. While software providers were not implicated in this case, the CMA warned that they could also face legal consequences if they assist clients in using software to facilitate anti-competitive agreements.

A similar case was filed in the US District Court, Northern District of California*, US v. David Topkins*, where the defendant, who was the Director of Trend, a company that sells posters online, pleaded guilty to participating in an illegal price fixing conspiracy with competitors (US Department of Justice, 2015). The US Department of Justice brought the action against the conspirators for using pricing algorithms to coordinate, fix, increase, maintain, and stabilize prices of certain posters sold through Amazon, thereby violating the Sherman Antitrust Act (15 USC § 1). The algorithm was used to prevent competing sellers from undercutting each other.

Anti-competitive practices can also occur when algorithms are used to facilitate tacit collusion. This happens where businesses use price-matching algorithms to track and align their prices without explicit agreement, human intervention, or direct communication. In this case, there is an unspoken understanding between competitors to fix prices. Unlike explicit collusion, which is a violation of competition law, tacit collusion, especially AI-powered collusions, is complex and challenging to regulate due to the lack of formal agreements. Algorithmic tacit collusion could occur where competitors use the same or similar algorithms or price tools from the same third-party provider. This is referred to as 'Hub and Spoke'. The AI algorithm in this category tracks and adjusts its prices in real time based on competitors' pricing patterns (Ezrachi et al., 2015). In some cases, the AI model deployed could learn that increasing prices to synchronize and match competitors' prices maximizes profit (OECD, 2019).

In recognition of this emerging threat that algorithmic collusive price fixing poses to competition and consumer welfare and the difficulty of regulating it through competition regimes, US Senator Amy Klobuchar proposed the Preventing Algorithmic Collusion Act (Klobuchar, 2025). The bill aims to prevent anti-competitive practices implemented through pricing algorithms by prohibiting the use of algorithms that can facilitate collusion through the use of nonpublic competitor data, creating

an antitrust law enforcement audit tool, increasing transparency, and enforcing violations under the Sherman Act and the FTC Act, among other purposes. The Act makes it unlawful for a person to use or distribute any pricing algorithm that uses, incorporates, or was trained with nonpublic competitor data. It defines nonpublic competitor data as any information that is not widely available or easily accessible to the public, and that is derived from, or otherwise provided by, another person who competes in the same or a related market.

Aside from the Preventing Algorithmic Collusion Act, there are other US state government bills, such as the California Preventing Algorithmic Collusion Act 2024, that prohibit the use of pricing algorithms that rely on nonpublic competitor data. By focusing primarily on nonpublic competitor data, the Preventing Algorithmic Collusion Act does not address all forms of collusion that could occur when businesses use AI pricing tools that learn to maintain high prices using publicly available competitor data independently.

Algorithmic collusion presents peculiar challenges for regulators as it is usually very difficult to detect, prove, and enforce. To establish collusive price fixing, existing competition laws require evidence of an explicit agreement to coordinate prices. However, AI pricing algorithms operate autonomously, making it difficult to prove that competitors deliberately engaged in price-fixing. Even where collusion is established, it may be challenging to determine which competitor initiated the behavior or whether a business can be held liable for an unintended consequence of a self-learning algorithm.

While this paper does not undertake a complete competition law analysis, it acknowledges algorithmic collusion as part of the broader ecosystem of digital market harms. Any reform of Nigeria's consumer protection framework must be cognizant of this intersection between competition and consumer law, particularly in addressing the opaque pricing practices enabled by AI and ML. Although there are currently no reported cases of algo-

rithmic collusion in Nigeria, concerns about price coordination and unfair pricing in digital marketplaces have begun to draw the attention of regulators such as the Federal Competition and Consumer Protection Commission (FCCPC), indicating a growing awareness of the potential risks (Digital Policy Alert, 2025).

V. MODERNIZATION OF CONSUMER PROTECTION IN THE DIGITAL ERA

A. Recommendations

The following measures are proposed to strengthen Nigeria's consumer protection framework in the digital environment:

i). The National Assembly should amend the FCCPA to expressly prohibit manipulative practices such as dark patterns and discriminatory personalized pricing. Alternatively, the FCCPC should issue regulatory guidelines in the same light. These reforms should also restrict the use of sensitive data for advertising and pricing purposes.

ii). The FCCPC, in collaboration with the NDPC, should require businesses to clearly disclose when advertisements or prices are personalized, including the main parameters used in profiling. Companies should present such disclosures in concise, accessible, plain language.

iii). The FCCPC and NDPC should mandate a one-click opt-out mechanism for targeted advertising, personalized recommendations, and personalized pricing. The Regulators should prohibit pre-ticked boxes, default settings that maximize data collection, and overly complex privacy notices.

iv). The FCCPC should expressly prohibit targeted advertising and personalized pricing practices directed at

vulnerable groups, including children, elderly persons, individuals experiencing financial distress, and persons with addiction-related vulnerabilities. Regulators should subject higher-risk sectors, such as digital lending, gambling, and health-related platforms, to stricter compliance requirements and monitoring scrutiny.

v). The FCCPC and NDPC should require businesses, particularly large digital platforms, to conduct Algorithmic Impact Assessments (AIAs) and User Interface Audits before deploying personalized advertising or pricing tools. Additionally, the government should strengthen these regulatory agencies by investing in technical expertise, forensic data capabilities, and digital monitoring tools to ensure effective oversight.

vi). The government, through relevant ministries and agencies, should implement nationwide digital literacy programs to enable consumers to recognize manipulative online practices and understand their rights under data and consumer protection laws. They should also partner with civil society, academia, and the media to enhance public awareness and oversight.

B. Conclusion

Consumer protection has historically evolved to address imbalances in power, information, and resources between businesses and consumers. However, the digital marketplace introduces a new layer of complexity, where harms arise not from overt misrepresentations but from the subtle exploitation of data, behavioral biases, and opaque algorithmic practices. As this paper shows, dark patterns, personalized advertising, and algorithmic pricing strategies collectively undermine consumer autonomy, fairness, and trust in the marketplace.

Nigeria's current legal framework provides an important foundation. The FCCPA prohibits traditional misleading and

unfair practices, while the NDPA enshrines principles of fairness, transparency, and lawful data processing. However, both instruments are framed in general terms and do not yet address the specific risks arising from a digital economy, such as dark patterns, personalized advertising, or algorithmic pricing.

By contrast, other jurisdictions are undertaking initiatives to regulate digital manipulation. The EU's Digital Services Act explicitly prohibits dark patterns on large platforms, while the forthcoming Digital Fairness Act aims to provide consumers with enhanced protection against manipulative design. The United States Federal Trade Commission has begun issuing enforcement actions against manipulative subscription traps, and legislators have proposed laws, such as the Preventing Algorithmic Collusion Act, to tackle AI-driven pricing collusion. India's 2023 Guidelines on Dark Patterns also provide regulators with a clearer basis for enforcement. These comparative developments underscore how Nigeria's framework remains underdeveloped in addressing the sophisticated risks of digital commerce.

For Nigerian consumer protection to remain effective in the digital age, reforms must move beyond general prohibitions of deception and unfairness toward explicit recognition of new forms of digital manipulation. This includes clear definitions of dark patterns, transparency obligations in profiling and personalized advertising, stronger consumer rights to opt out of targeted practices, and explicit prohibitions on the exploitative use of consumer data.

General legal provisions are often inadequate for addressing harms in the digital economy. Nigerian consumers rarely enforce their rights through litigation due to high costs and procedural delays (Ilobinso, 2023). Unless rights are clear, specific, and actionable, they remain underutilized. Explicit rules would arm consumers with stronger tools while also discouraging businesses from exploiting legal ambiguity.

For regulators, specificity provides legal certainty and confi-

dence in enforcement. Agencies such as the FCCPC need explicit mandates to act decisively against emerging harms, without targeted provisions, regulators risk overstretching general clauses and facing legal challenges that undermine enforcement.

Finally, clear statutory rules deter harmful business practices by signaling that unfair conduct, such as dark patterns and other exploitative practices, is unlawful. In so doing, they enhance consumer trust, promote fair competition, and safeguard Nigeria's digital marketplace.

REFERENCES

Adedeji, A. (2022). Consumer protection and competition law in Nigeria – Concentric or overlapping interests? In F. Monye et al. (Eds.), *Compendium of Consumer Protection Law in Nigeria.* Lagos. Nigeria: Princeton & Associates Publishing.

Authority for Consumers and Markets (ACM). (2022). Following ACM actions, Wish bans fake discounts and blocks personalized pricing. https://www.acm.nl/en/publications/following-acm-actions-wish-bans-fake-discounts-and-blocks-personalized-pricing (RetrievedMarch 11, 2025)

BBC. (2012, June 26). Travel site Orbitz offers Mac users more costly hotels. https://www.bbc.com/news/technology-18595347 (Retrieved March 28, 2025)

Cartwright, P. (2001). *Consumer protection and the criminal law: law, theory, and policy in the UK*: Cambridge University Press.

Central Consumer Protection Authority CCPA. (2023) The Guidelines for Prevention and Regulation of Dark Patterns, issued by the https://www.nls.ac.in/wp-content/uploads/2021/04/Dark-Patterns.pdf (Retrieved December 26, 2025)

Competition and Markets Authority CMA (2018). Pricing algorithms: economic working paper on the use of algorithms to facilitate collusion and personalised personalized pricing. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf (Retrieved December 26, 2025)

Competition and Markets Authority CMA. (2016). Amazon Marketplace online sellers fined £160k for price-fixing: Case study. https://www.gov.uk/government/case-studies/online-sellers-price-fixing-case-study (Retrieved December 26, 2025)

Competition and Markets Authority CMA. (2021). Algorithms: How they can reduce competition and harm consumers: Summary of responses to the consultation. https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers (Retrieved December 26, 2025)

Competition and Markets Authority CMA. (October 2020). Instagram to tackle hidden advertising after CMA action [Press release]. GOV.UK. https://www.gov.uk/government/news/instagram-to-tackle-hidden-advertising-after-cma-action (Retrieved December 26, 2025).

Digital Policy Alert. (2025, August). DPA Digital Digest: Nigeria. https://digitalpolicyalert.org/digest/dpa-digital-digest-nigeria (Retrieved December 26, 2025)

Duhigg, C. (2012, February 16). How companies learn your secrets. *The New York Times.* https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (Accessed July 2025).

Eisen, M. (2011, April 23). Amazon's $23,698,655.93 book about flies. It's not a joke. *Michael Eisen Blog*. http://www.michaeleisen.org/blog/?p=358 (Retrieved December 26, 2025).

Ennis, S. F., & Lam, W. (2020). Personalised Personalized Pricing and Disclosure. Department for Business, *Energy and Industrial Strategy (BEIS) Research Paper Number 2021/008*.

Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. New York, NY: St. Martin's Press.

European Commission (2022). Guidance on the interpretation and application of Directive 2005/29/EC.

European Commission. (2025). Coordinated actions: Social media, online games and search engines. https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/social-media-online-games-and-search-engines (Accessed July 2, 2025).

European Commission. (2025). Market places and digital services. Retrieved-June 27, 2025, from https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/market-places-and-digital-services_en.

European Commission. (November 2024). Commission and national authorities urge Temu to respect EU consumer protection laws. European Commission Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5707 (Accessed July 2, 2025).

European Data Protection Board [EDPB]. (2023) Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en. (Retrieved 15 May 2025).

Ezrachi, A., & Stucke, M. E. (2016). Virtual competition: The promise and perils of the algorithm-driven economy. *Harvard University Press*.

Ezrachi, A., & Stucke, M. E. (2017). Artificial intelligence & collusion: When computers inhibit competition. *University of Illinois Law Review*.

Federal Trade Commission FTC (2022). Bringing dark patterns to light (Staff Report). https://www.ftc.gov/system/files/ftc_gov/pdf/P214800+Dark+Patterns+Report+9.14.2022+-+FINAL.pdf (Retrieved December 26, 2025).

Federal Trade Commission FTC. (2020, September). Children's online learning program ABCmouse to pay $10 million to settle FTC charges of illegal marketing and billing practices [Press release]. https://www.ftc.gov/news-events/news/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc-charges-illegal-marketing (Retrieved December 26, 2025).

Federal Trade Commission FTC. (July 2016). Warner Bros. settles FTC charges it failed to adequately disclose it paid online influencers to post gameplay

videos [Press release]. https://www.ftc.gov/news-events/news/press-releases/2016/07/warner-bros-settles-ftc-charges-it-failed-adequately-disclose-it-paid-online-influencers-post (Retrieved December 26, 2025).

Federal Trade Commission v. Vonage Holdings Corp., No. 2:22-cv-05889 (D.N.J. filed Oct. 2022). https://www.ftc.gov/system/files/ftc_gov/pdf/Vonage-Stipulated-Final-Order.pdf (Retrieved December 26, 2025).

Gilbert + Tobin. (2024). Insights: Unfair trading practices, dynamic pricing, AI and other consumer law reforms on the government's agenda. https://www.gtlaw.com.au/insights/unfair-trading-practices,-dynamic-pricing,-ai-and-other-consumer-law-reforms-on-the-governments-agenda (Retrieved December 26, 2025).

Google Safety Center. (2025). Is Google Assistant always listening to me? https://safety.google/assistant/ (Retrieved July 2025)

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2020). Dark patterns: Past, present, and future: The evolution of tricky user interfaces. *Queue*, 18(2), 67–92. https://doi.org/10.1145/3400899.3400901 (Retrieved December 26, 2025).

Hern, A. (2019, July 26. Apple contractors 'regularly hear confidential details' on Siri recordings. *The Guardian*. https://www.theguardian.com/technology/2019/aug/02/apple-halts-practice-of-contractors-listening-in-to-users-on-siri (Retrieved May 12, 2021)

Howells, G., Ramsay, I., & Wilhelmsson, T. (2019). *Handbook of research on international consumer law* (2nd ed.). Edward Elgar Publishing.

Ilobinso, I. K. (2022). A critical analysis of the consumers' right to information in online transactions. *International Review of Law and Jurisprudence*, vol. 4.

Ilobinso, I. K. (2023). adequacy of the existing consumer protection legislation in the protection of online consumers in Nigeria: A Critical Analysis. In B. Kanyip, A. Oyewunmi, et al. (Eds.), *Rethinking commercial & industrial law in Nigeria: essays in honour of Professor Chioma Kalu Agomo* (pp. 300–318). Ibadan, Nigeria: Ababa Press.

Information Commissioner's Office ICO. (2025). About this guidance | Direct marketing guidance. https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-guidance/about-this-guidance/ (Retrieved December 26, 2025).

Khan, M. A. (2017). The origin and development of consumer protection laws in United Kingdom. Journal of Asian and African Social Science and Humanities, 3(3), 38–52.

Klobuchar, A. (2025, February 6). Klobuchar, colleagues introduce antitrust legislation to take on algorithmic price fixing, bring down costs [Press release]. *USU.S. Senator Amy Klobuchar*. https://www.klobuchar.senate.gov/public/index.cfm/2025/2/klobuchar-colleagues-introduce-antitrust-legislation-to-take-on-algorithmic-price-fixing-bring-down-costs (Retrieved December 26, 2025).

Lopez v. Apple, Inc., No. 4:19-cv-04577 (N.D. Cal. August 22Aug. 22, 2019). Retrieved from https://www.govinfo.gov/app/details/USCOURTS-cand-4_19-cv-04577/context (Retrieved December 26, 2025).

Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., et al. (2022). Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation – *Final report. European Commission: Directorate-General for Justice and Consumers.* Publications Office of the European Union.

MacKay, A., & Weinstein, S. N. (2022). Dynamic pricing algorithms, consumer harm, and regulatory response. *Washington University Law Review*, 100(1), 111–174.

Mahambare, V., Todi, S., & Kankarika, P. (2024, December). Hotel bookings cost more on iPhones. That's price discrimination — and it's not always bad. ThePrint. https://theprint.in/opinion/hotel-bookings-cost-more-on-iphones-thats-price-discrimination-and-its-not-always-bad/2413949/ (Retrieved February 2025)

Mathur, A., Acar, G., Friedman, M. G., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), Article 81. https://doi.org/10.1145/3359183 (Retrieved December 26, 2025).

Meta. (2025). Are Facebook and Instagram listening to your conversations? Privacy Centre. https://web.facebook.com/privacy/dialog/is-facebook-listening-to-my-conversation (Retrieved July 2025)

Myrstad, F. (2022, July 1). Amazon makes it easier to cancel Prime following complaints from European consumer organisations. *Forbrukerrådet – Norwegian Consumer Council.* https://www.forbrukerradet.no/siste-nytt/amazon-makes-it-easier-to-cancel-prime-following-complaints-from-european-consumer-organisations/ (Accessed June 27, 2025)

Naceva, N. (2024). The ultimate guide to Amazon dynamic pricing strategy in 2024. *Influencer Marketing Hub.* https://influencermarketinghub.com/amazon -dynamic-pricing/ (Retrieved August 2025)

Nairn, C. (2025, September 4). Judge approves $95 million Apple settlement over Siri privacy case. Courthouse News Service. https://www.courthousenews.com/judge-approves-95-million-apple-settlement-over-siri-privacy-case/ (Accessed October 2025)

Nie, L., Zhao, Y., Li, C., Luo, X., & Liu, Y. (2024). Shadows in the interface: A comprehensive study on dark patterns. *Proceedings of the ACM on Software Engineering, 1(FSE)*, Article 10. https://doi.org/10.1145/3643736 (Retrieved December 26, 2025).

OECD. (2017). Algorithms and collusion: Competition policy in the digital age. https://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm (Retrieved December 26, 2025).

OECD. (2022). The role of online marketplaces in protecting and empowering consumers: Country and business survey findings (OECD Digital Economy Papers, No. 329). OECD Publishing. https://doi.org/10.1787/20716826 (Retrieved December 26, 2025).

OECD. (2022). Dark commercial patterns (OECD Digital Economy Papers No. 336). OECD Publishing. https://doi.org/10.1787/1e1d6c9f-en (Retrieved December 26, 2025).

OECD. (2023). Algorithmic competition. OECD Roundtables on Competition Policy Papers, No. 296. OECD Publishing. https://doi.org/10.1787/cb3b2075-en (Retrieved December 26, 2025).

OECD. (2023). Consumer vulnerability in the digital age (OECD Digital Economy Papers No. 355). OECD Publishing. https://doi.org/10.1787/4d-013cc5-en (Retrieved December 26, 2025).

Oko-Epelle, L., Omowale, A., & Sunday, A. A. (2022). Regulating online advertising in the internet age: A study of Advertising Practitioners Council of Nigeria (APCON). *Indian Journal of Scientific Research,* 10(4), 848.

Osinbajo, Y., & Fogam, K. (1991). *Nigerian media law*. Lagos. Nigeria: Gravitas.

Pavestones Legal. (2025). Influencer and digital marketing regulation in Nigeria. https://pavestoneslegal.com/influencer-and-digital-marketing-regulation-in-nigeria/ (Retrieved December 26, 2025).

Poort, J., & Zuiderveen Borgesius, F. J. (2019). Does everyone have a price? Understanding people's attitude towards online and offline price discrimination. *Internet Policy Review*, 8(1). https://doi.org/10.14763/2019.1.1391 (Retrieved December 26, 2025).

Rott, P., Strycharz, J., & Alleweldt, F. (2022). *Personalised pricing. Publication for the Committee on Internal Market and Consumer Protection,* Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

Sharma, S. J. & Sharma, I. (2023) Dark Patterns in a bright world : An analysis of the Indian Consumer Legal Architecture, *International Journal on Consumer Law and Practice*: Vol. 11, Article 7. Available at: https://repository.nls.ac.in/ijclp/vol11/iss1/7 (Retrieved December 26, 2025).

Shiv, B., & Fedorikhin, A. (1999). Heart and mind in conflict: The interplay of affect and cognition in consumer decision making. *Journal of Consumer Research,* 26(3), 278–292. https://doi.org/10.1086/209563 (Retrieved December 26, 2025).

Stempel, J. (January 2025). Apple to pay $95 million to settle Siri privacy lawsuit. *Reuters*. https://www.reuters.com/legal/apple-pay-95-million-settle-siri-privacy-lawsuit-2025-01-02/ (Retrieved March 2025)

Stole, L. A. (2007). Price discrimination and competition. In M. Armstrong & R. H. Porter (Eds.), *Handbook of Industrial Organization* (Vol. 3, pp. 2221–2299). Elsevier. https://doi.org/10.1016/S1573-448X(06)03034-4 (Retrieved December 26, 2025).

Trentmann, Frank, ed. (2006) *The making of the consumer: knowledge, power and identity in the modern world: cultures of consumption series*. Oxford, UK: Berg Publishers

United Nations Children's Fund UNICEF. (2019, March). Children and digital marketing: Rights, risks and opportunities – Discussion paper. https://www.unicef.org/childrightsandbusiness/media/256/file/Discussion-Paper-Digital-Marketing.pdf (Retrieved December 26, 2025).

USU.S. Department of Justice. (2015, April). Former e-commerce executive pleads guilty to price-fixing in the Antitrust Division's first online marketplace prosecution. *DOJ Press Release.*

Victor, V., Nathan, R. J., & Fekete-Farkas, M. (2020). Consumer response towards personalized pricing strategies in online marketing. *International Journal of Technology Marketing*, 15(2–3), 199–218. https://doi.org/10.1504/IJTMKT.2020.109674 (Retrieved December 26, 2025).

Widmer, M. (February 2025). Is your phone listening to you for ads? Targeted advertising 101. *Grapeseed Media.* https://grapeseedmedia.com/blog/targeted-advertising-is-your-phone-listening-to-you/ (Retrieved March 2025)

Zard, L., & Sears, A. M. (2023). Targeted advertising and consumer protection law in the European Union. *Vanderbilt Journal of Transnational Law*, 56, 799–846.