Temilola Allen-Ijewere

Cookies in Context: An Empirical Study Evaluating Web Tracking and Policy Compliance Across Nigeria and Ghana

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway University of London.

Information Security Group
Royal Holloway, University of London
September 2025

Table of Contents

List of Abbreviations & Acronyms

CCPA - California Consumer Privacy Act
DPA - Data Protection Authority
ECOWAS - Economic Community of West African States
EU - European Union
FCCPC - Federal Competition and Consumer Protection Commission
GDPA - Ghana Data Protection Act
GDPC - Ghana Data Protection Commission

GDPR - General Data Protection Regulation
NDPA - Nigeria Data Protection Act
NDPC - Nigeria Data Protection Commission
VPN - Virtual Private Network

List of Figures &Tables

List of Figures

Executive Summary

As digital adoptions continue to rise across West Africa, in-depth conversations surrounding the protection of data privacy and user consent are becoming increasingly important to fully safeguard and digitally protect citizens. At the heart of this, is the use of cookies (small tracking technologies embedded in websites that collect and process user data, with or without consent). While countries such as Nigeria and Ghana have introduced and established data

protection laws, research into the extent at which organisations and websites in these countries comply with cookie-related obligations remains limited.

This study aims to fill the gap by assessing the extent to which top websites across Nigeria and Ghana adhere to the cookie compliance requirements established in their national data frameworks. A comparative legal-technical approach is adopted, assessing cookie compliance in Nigeria and Ghana, with the European Union's General Data Protection Regulation (GDPR) serving as the benchmark and gold standard for best practice. Through experimental web-testing and observations of 100 high-traffic websites (50 per country), this study analyses and evaluates the presence, design and functionality of cookie notices — including pre- and post-consent tracking behaviours — across three browser configurations: Brave (with shields 'ON' and 'OFF') and Google Chrome (with default settings).

Websites will be accessed from the United Kingdom using Nord VPN to replicate local access from each target country to ensure region-specific implementations are captured. Further tools such as Brave Browser to detect tracking activity and consent banners. Focusing solely on measuring compliance in practice, no legal recommendations will be offered.

A structured compliance rubric was employed to classify websites into three categories: fully compliant, partially compliant, or non-compliant, based on legal and technical indicators. The experiment's findings reveal significant gaps between legislative intentions and real-world implementation, with alarming non-compliance across both jurisdictions, regardless of browser settings. Cookie notices were found to be frequently missing, employed dark patterns or failed to function in line with legal expectations for valid informed consent.

Although Nigeria's Data Protection Act, 2023 and Ghana's Data Protection Act, 2012 are closely modelled after GDPR's consent standards, the existing enforcement gaps, lack of public awareness, and non-specific technical guidance undermine their effectiveness. Furthermore, the study draws on regional insights to explore broader challenges facing digital economies in West Africa.

Finally, this research contributes original data to a largely under-investigated area and demonstrates that regulatory adoption alone is inadequate without consistent and constant enforcement and user education. With a focus solely on measuring compliance in practice, no legal recommendations will be offered.

Introduction

The increasing reliance on digital technologies across West Africa has introduced questions surrounding data protection and users' online privacy across the region. Central to these growing concerns are the ever-present cookies and other tracking technologies found online, that are often operating without users' knowledge. These technologies often collect, process and transfer an individual's personal data, which can later be used for advertising purposes. Within Europe, the widely respected regulatory framework, the General Data Protection Regulation (GDPR), has established comprehensive standards for cookie consent and

transparency, whereas across West Africa, similar developments in regulatory frameworks have occurred at a noticeably slower pace, often lacking in enforcement, specificity or clarity. The following preliminary literature review critically explores the evolving landscape of cookie notices, consent mechanisms and tracking practices of websites across West Africa and contextualising within the existing legislation environments of two major West African nations, Nigeria and Ghana. Doing so highlights significant gaps in citizens' awareness, legal compliance and enforcement by these nations. Due to the limited observed investigations and research regarding online privacy across West Africa, this study seeks to contribute to this space by assessing the realities of cookie compliance by websites against emerging data protection regimes.

Chapter 1: Introduction and Background

1.1 Background and Context

In the global conversation on data protection and digital privacy, the regulation of cookies, tracking technologies and PETs (Privacy-enhancing technologies) has emerged as a key challenge that needs to be tackled. These invisible tools aggregate and collect vast amounts of personal data from users (Ajala et al., 2024), sometimes with their consent, other times without their informed consent. At the centre of this discourse is whether organisations are truly fulfilling their legal obligations to obtain meaningful, informed consent from users (Cha et al., 2019).

On the European continent, establishment of the General Data Protection Regulation (GDPR) was a global turning point for data protection and transparency (Goddard, 2017; (Aseri, 2020). On the contrary, regions such as West Africa, data protection legislation is less developed (Abdulrauf, 2020; Prinsloo and Kaliisa, 2022). While certain countries like Nigeria and Ghana have made progress legally, the effectiveness of these frameworks remains under-explored.

The following research addresses the gap by investigating how popular websites accessed from Nigeria and Ghana handle cookie consent, how their practices compare to GDPR expectations, and the level of compliance with Nigeria and Ghana's respective data protection legislation.

To contextualise this study, Nigeria and Ghana represent two of West Africa's largest populations, with Nigeria's approximate population of 232.6 million (World Bank Group, 2021) and Ghana's approximate population of 34.43 million (Statista, 2025) as of 2024. Internet usage in both nations continue to rise, driven by rapid mobile phone adoption (Ochinanwata, Igwe and Radicic, 2023). As seen in the traffic analytics provided by the Semrush database in Appendix A and Appendix B, Nigerian users showcase extremely high engagement with platforms such as google.com, youtube.com, facebook.com and betting sites such as bet9ja.com, livescore.com and sportybet.com. In a similar fashion, Ghanaian users demonstrate frequent visits to platforms such as google.com, chatgpt.com, and betting websites such as sportybet.com. Additionally, both nations also demonstrate significant traffic towards pornography and social media communication platforms. These usage patterns and

high levels of frequency emphasise the importance of cookie consent compliance for high-traffic platforms operating in this region.

1.2 Research Problem and Motivation

Academic research in the data protection domain often tend to fall into two distinct categories; legal analysis of laws and technical audits of compliance. Yet, much of the research remains Eurocentric, with a heavy focus on the enforcement of the GDPR across Europe. This has led to geographical bias, in which the legal and technical intricacies of cookies are well documented in Europe. As Abebe et al., (2021) highlight, little is known about how the same issues present themselves in developing regulatory economies, especially in West Africa.

Furthermore, there is minimal comparative literature that examines how African economies adhere to global standards or the dynamics of tracking in low-enforcement regions due to structural, technological or socio-political factors that hinder enforcement. The absence of such research is problematic, as these developing regions become high-risk environments for exploitative data practices. (Abebe et al., 2021)

By conducting controlled browser experiments, simulating the average user, in two of West Africa's most digitally advanced countries, this study contributes original data and analysis to a field currently in its early stages of research within Africa.

1.3 Research Aim and Objectives

The aim of this dissertation is; to critically evaluate the cookie compliance of the top websites utilised by citizens in Nigeria and Ghana, against each country's data protection requirements.

Achieving this aim, specific research objectives will be followed:

1. Identify and analyse national legal frameworks that govern cookie consent and online privacy in Nigeria and Ghana.

2. Audit the cookie practices of the top-ranked websites in each country using technical tools and make observations.

3. Compare the observed websites' compliance against respective legal requirements.

4. Explore how unique browser settings affect a user's exposure to online tracking.

5. Propose opportunities for further research by identifying emerging challenges and gaps.

1.4 Scope of the Study

This research focuses on Nigeria and Ghana as a result of their relatively developed legislative frameworks and higher digital growth in West Africa. A comparative approach is employed using GDPR guidelines as the compliance benchmark, due to its global influence and impact to both countries' legal structures. Ekpo, Okokon and Akpakpan (2024) note that the "GDPR significantly influenced the NDPA", while researchers such as Spirkl (2024) further support that the "GDPR has influenced data protection laws in Anglophone countries", which includes Ghana.

The experiment is strictly limited to observational testing of websites through controlled browser environments, and does not involve interacting with any backend systems or server logs. Although Virtual Private Networks (VPNs) are used to simulate local access from a citizen of Nigeria or Ghana, physical access from within the countries may potentially provide different results. Websites were accessed between May - August 2025, and the results discussed reflect the state of compliance during that time period.

Chapter 2: Literature Review

2.1 Online Tracking and Consent Mechanisms: Key Concepts

An intrinsic feature of the digital economy is the collection and processing of user data through online tracking mechanisms. Amongst widely deployed tracking technologies are cookies. Originally designed with the intent to enhance user experience by enabling the storage of user preferences and session continuity (Turner and Dasgupta, 2003), cookies have since evolved into essential tools for behavioural understanding, profiling, personalised advertising and user analytics (Trusov, Ma and Jamal, 2016).

Cookies are small files stored on a user's browser when they visit a website (Harding, Reed and Gray, 2001). While some cookies are essential for core site functionalities (maintaining log-in sessions, or shopping carts), an increasing number are for more intrusive or malicious purposes. Cahn et al., (2016) discuss that the purpose of cookies can range from selling user data to third parties to analytical cookies that monitor a user's browsing behaviour to advertising cookies that track across different websites to provide users with personalised content. Thus, cookies are no longer just a technical function of a website, but have instead become entrenched within the digital economy (Chester, 2012; Trusov, Ma and Jamal, 2016).

Emergence of these tracking practices has in turn resulted in the establishment and development of regulatory frameworks around the world. At the foundation of digital privacy laws exists the principle of user consent, whether it be informed, prior and explicit user consent. Most data protection regulations, particularly ones that have been influenced by the European Union's GDPR, forbid the use of non-essential tracking technologies without a user's informed and active consent (Koch, 2019; European Commission, 2024). Consequently, this led to the widespread adoption of modern cookie notices and pop-ups that

request consent before the use of tracking technologies, as a way of achieving legal compliance.

However, the effectiveness of these consent mechanisms remains debatable. Nouwens et al., (2020) exposed the manipulative potential of design as a systemic audit of 10,000 websites found that only 12% of consent notices met the minimum GDPR requirements. Nouwens et al., (2020) identified that dark patterns, interface tricks designed to nudge users into accepting tracking, were widespread, and further experimental studies confirmed that removal of a “reject” button increased user consent rates by over 20%. This study demonstrated how easily users’ choices could be steered through nudging without a user’s full awareness of the nudge.

2.2 GDPR and Its Global Influence

Introduction of the European Union’s General Data Protection Regulation (GDPR) in 2018 marked a major point in global privacy policy and cookie practices. Designed to modernise previous data privacy laws across EU member states, the regulation remarkably reshaped the handling of personal data, not only within the European Union (EU), but also by organisations worldwide.

At its foundation, the GDPR established seven key principles that foster all lawful processing of personal data; lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability (Article 5, GDPR; (European Commission, 2024). These principles are supported by data subject rights, including; the right to access (Article. 15), rectification (Article 16), erasure or “right to be forgotten” (Article 17), restriction of processing (Article 18), data portability (Article 20), and the right to object (Article 21). Article 25 also states that organisations must implement data protection by design and by default, Article 33 - 34 states that organisations are subject to strict rules regarding data breaches and Chapter 5 is related to cross-border transfers (Chapter V, EUR-Lex, 2016)

One of the most noteworthy contributions of the GDPR globally is its explicit definition of consent. Under Article 4(11), consent must be “freely given, specific, informed, and unambiguous”, typically demonstrated through a clear affirmative action (EUR-Lex, 2016). This leaves significant implications for cookies that are not strictly necessary, as they are now considered to handle personal data processing. As such, under Recital 32 and Article 6(1)(a), websites are legally obliged to obtain prior consent before cookies can be placed on users’ devices.

The consequence of this consent requirement has been the introduction of cookie banners or notices across websites either targeting EU users or that have EU visitors. These notices are meant to empower users to ‘accept’ or ‘reject’ the use of non-essential cookies, yet in practice, many banners fail to meet the GDPR’s standard for valid consent. As Degeling et al., (2019) demonstrated through a large-scale study of over 6,500 websites, that there has been partial compliance with GDPR’s consent requirements. Although it is important to note the proportion of websites displaying privacy policies and cookie banners did rise significantly post-GDPR, technical implementations may have lagged, with some websites failing to fully prevent

tracking before users granted their consent. The disconnect between regulation and practical outcomes does raise significant questions about the effectiveness of consent notices.

Beyond Europe, GDPR's influence is far, due to its territorial scope of Article 3 (EUR-Lex, 2016), particularly Article 3(1) that states the GDPR applies to any regulation, regardless of their location, that provides goods or services to EU citizens or monitors their behaviour. Consequently, global platforms such as Google, Meta and Amazon have had to adapt their privacy policies to align with the regulation. However, research has found that high-profile platforms frequently failed to block third-party cookies until consent was received, or misled users through ambiguous language.

The global ripple effect of the GDPR is apparent in the various jurisdictions that have since introduced or revised their data protection legislation using the GDPR has inspiration. Particularly in Africa where examples include Nigeria's Data Protection Act (2023) or Mauritius's Data Protection Act (2017), which explicitly reference GDPR principles. These frameworks tend to mirror the emphasis on lawful bases for data processing, user consent and the user's individual rights. However, their effectiveness remains dependent on the nation's enforcement ability, and digital literacy.

In summary, the GDPR has fundamentally reshaped and redesigned the global discussion on online privacy and has introduced meaningful individual rights in the digital age. Its consent standards have redefined how websites and users engage around tracking technologies and cookies (Linden et al., 2020). However, as this dissertation will explore, there remains a discrepancy between regulatory frameworks and practical implementation outside of the EU.

2.3 Global Developments in Cookie Compliance and Data Protection

The evolution of cookie practices and consent notices/mechanisms globally has seen significant developments from the introduction of comprehensive data protection laws i.e the GDPR. Numerous empirical studies have aimed to assess both the technical compliance of websites, user engagement and user attitudes towards privacy notices.

Narayanan (2020) conducted a detailed study that examined the factors influencing user attitudes towards cookie consent banners and notices within the European Union. Narayanan's findings showcased that user attitudes towards cookies are heavily swayed by the clarity, design and wording of consent banners, and that simplified, transparent notices increased trust significantly, while vague or manipulative notices fostered distrust. Additionally, participants' own pre-existing knowledge influenced their attitudes as well. Users with more understanding felt more empowered to actively reject cookie notices, therefore highlighting that legal literacy does play a vital role in the effectiveness of consent and privacy policy frameworks.

Similarly, Strycharz et al., (2021) reinforced Narayanan's findings as Strycharz et al., (2021)'s research portrayed that users that were better informed about their privacy rights and the

extent of tracking technologies became less susceptible to manipulation through dark patterns or nudges. Both these findings expose a crucial vulnerability in this space, and that is; without intentional widespread public awareness, then regulatory efforts can be undermined, and non-compliance can continue.

Previously mentioned, research by Utz et al., (2019) and Nouwens et al., (2020) identified that user's actions can be manipulated through the design of the cookie notice, which can result in unfair or unfavourable choices for users. Supporting this, Kretschmer, Pennekamp and Wehrle (2021), through an expansive audit of cookie banners and privacy policies, produced further empirical validation by demonstrating that a large proportion of cookie banners did not offer equally noteworthy options for individuals to refuse consent, implying that dark patterns had evolved to exploit loopholes and force users to accept cookies by design, which is a direct violation of GDPR standards.

Santos, Bielova and Matte (2019) compliment previously discussed studies by combining legal and technical analyses to determine whether cookie banners genuinely achieved compliance. They found that a significant proportion of sites set cookies prior to consent or made the users opt-out process unnecessarily difficult, which violates most data protection legislation such as the GDPR. Most critically, (Papadogiannakis et al., 2021) identified trends in which certain websites utilised new tracking technologies to completely bypass traditional cookie consent mechanisms, bypassing GDPR, thus demonstrating the race between regulation and innovation.

When read together, these global studies convey a nuanced picture with legal frameworks pushing organisations towards transparency, the practical and meaningful methods of receiving consent are charged with manipulation, technological innovation and malicious design practices. These findings do highlight the need for regulatory design to be paired with continuous technical auditing and enforcement to achieve long-term protection for users online.

2.4 Empirical Studies on User Awareness and Consent Behaviour

Over the last two decades, a growing body of research has explored how users perceive, understand and interact with cookie notices. In an early experimental study, Miyazaki (2008), found that the disclosure of cookie usage positively influenced consumer trust in a site, suggesting that this transparency could mitigate and ease users' feelings of betrayal when made aware of tracking activities. On the other hand, succeeding research does indicate that cookie notice design features heavily alter the results of Miyazaki's study.

Kuyk et al., (2018), using a mixed-method survey in Germany, found that most users regarded cookie notices as a nuisance rather than as a tool for their privacy protection. Despite participants expressing a general concern about online privacy, Kuyk et al., found that users frequently engaged in habitual acceptance of cookies and disregarded the notice, depending on their level of need for the website. It was discovered that the framing and language of cookie notices had limited impact on users but instead users' perceptions were influenced more by the website's external reputation and other convenience factors.

Nevertheless, further experimental evidence from Utz et al., (2019) confirmed that subtle aspects of interface design, including banner placement and choice architecture, significantly affect consent acceptance rates by users. This large-scale experiment with 80,000 unique users revealed that banners placed at the bottom of the screen gained more attention and presenting users with a simple binary choice of “Accept” vs “Decline” increased acceptance rates, whereas a user’s individual selection of cookie categories resulted in a decreased inclination to accept cookies. Similarly, through controlled experiments, Machuletz and Böhme (2020) illustrate that default options like “accept all” greatly increase the likelihood of user-given consent, even when multiple different purposes for data collection and processing were listed. Furthermore, the study found that participants often failed to recall what they had given their consent too, thus indicating that consent was given without users’ fully understanding what they agreed to.

Nouwens et al., (2020) exposed the manipulative potential of design as a systemic audit of 10,000 websites found that only 12% of consent notices met the minimum GDPR requirements. Nouwens et al., (2020) identified that dark patterns, interface tricks designed to nudge users into accepting tracking, were widespread, and further experimental studies confirmed that removal of a “reject” button increased user consent rates by over 20%. This study demonstrated how easily users’ choices could be steered through nudging without a user’s full awareness of the nudge.

Considering a more qualitative approach through interviews, (Borberg et al., 2022) reveals that when users were confronted with manipulative cookie prompts on a website, they often felt disempowered and resigned from proceeding further. Many participants of the study did perceive cookie banners as barriers rather than assisting informed choice, with some describing that they simply accept terms to be able to continue browsing, despite being uncomfortable and aware of the underlying data practices.

Looking beyond user perceptions, some cookies and tracking technologies operate covertly. Using OpenWPM tool, Englehardt and Narayan (2016) crawled one million websites and found that web tracking is indeed prevalent. Although this research is dated and pre-GDPR, it quantified and visualised how an ordinary user browsing popular websites can accumulate thousands of cookies, that can be used for ad tracking, thus raising concerns about the sheer scale of covert tracking systems on popular websites. Santos, Bielova and Matte (2019) further supports this as they found many cases in which users clicking “refuse” or opting out, did not actually prevent covert tracking cookies from being placed, which is a direct contravention of the GDPR, and fully undermines meaningful informed choice.

Collectively, these empirical studies showcase that while the European Union’s GDPR has stimulated greater transparency around cookies and online privacy, there remain significant challenges, typically around covert operations and enforcement. Users may be poorly informed, manipulated through design, subconsciously nudged or inadequately protected even when users attempt to assert control over their choices online. It is imperative to note that these findings draw primarily from European research, they offer crucial lessons for emerging nations with developing regulatory environments to consider as similar patterns may begin to emerge as their nations grow.

2.5 Comparative Reflections: Global vs West Africa

While global cookie compliance studies predominantly focus on Europe, due to the region's mature data protection framework, researchers' findings in this region offer a solid foundation for comparing and understanding the realities of online privacy in emerging regions such as West Africa. A review of the global literature reveals a few key but consistent themes. User consent is often superficial, with dark patterns manipulating user choices and covert tracking remains a widespread issue despite strict regulations (Narayanan, 2020; Bollinger, 2021; Santos et al., 2019). Despite the stringent and sophisticated nature of the GDPR, there still exist enforcement gaps and design tricks that undermine users' ability to make genuine, informed decisions on giving their consent.

On the contrary, West African countries such as Nigeria and Ghana are all at an early stage of regulatory development. As outlined in Section 2, Nigeria's new Data Protection Act, 2023 aligns more closely with GDPR, with its enforcement mechanisms still being developed and low public awareness (Nwosu, 2022; Aloamaka, 2023). Likewise, Ghana's Data Protection Act, 2012 mandates user consent but this has not resulted in widespread compliance or public education (Amasah, Odoi & Arthur, 2022; Cetin, 2024).

In Europe, the experience as demonstrated by Degeling et al., (2018) and Nouwens et al., (2020) shows that robust laws require persistent and continuous enforcement and technical audits to ensure compliance. Without these measures, "forced consent" through malicious design nudging and non-compliant tracking remain rampant in the online space. This carries significant implications for West Africa, where social and economic barriers may exacerbate the problems seen in Europe. From Kretschmer, Pennekamp and Wehrle's (2021) research, a legally developed environment remains difficult to regulate effectively; thus, West African nations must anticipate even greater challenges as the region's legislation continues to develop.

Additionally, studies from Strycharz et al., (2021) showcase that user empowerment depends on public education at all levels and about their technical and legal rights and not only on legal frameworks. This gap is crucial for West Africa as studies by Izuogu (2019) and Kanu et al., (2024) demonstrate that citizens of the chosen countries for this research often lack awareness of their digital rights or the use of tracking technologies by organisations online. Without intentional efforts to raise awareness and improve standards for consent notices online, then issues such as "decision fatigue" and manipulation have a higher likelihood of being more problematic in West Africa than in Europe.

Finally, global studies such as (Papadogiannakis et al., 2021) warn that some websites and companies are evolving and moving towards more complex tracking technologies that bypass traditional cookie consent. Countries in West Africa thus must not only catch up with basic privacy policy and cookie notice enforcement but must also prepare and develop for future technological advancements that will demand even stronger regulatory and technical enforcements.

Contrasting some critical perspectives, Prinsloo and Kaliisa (2022) discuss that Nigeria and Ghana have made notable strides towards legislative enforcement of data privacy, particularly in educational contexts. Although their study focused more on student data privacy, the research is valuable in reflecting broader national data, as students make up a significant portion of contribution to each economy. This position appears to contradict other empirical findings that point towards sporadic enforcement and limited public awareness (Nwosu, 2022), signalling that compliance outcomes can vary depending on sector-specific applications.

To summarise, global research provides a roadmap for West African countries to use but also brings to light serious challenges that these same nations are likely to face as their digital regulatory environment develops. The simple adoption of GDPR inspired laws without a focus on improving enforcement capacity, user awareness or preparing for future tracking technologies may be detrimental for developing nations.

2.6 Identified Gaps and Research Opportunities

Reviewing existing literature and empirical studies highlights several gaps that warrant or in some cases, require more urgent attention. Most noticeably, there is a lack of region-specific research that measures the prevalence of cookies, the design of cookie notices and the effectiveness of the notices and subsequent legislation. While European-focused studies provide detailed mappings of compliance issues, they cannot be assumed to directly relate to West African contexts. Additional variables including lower digital literacy rates, different trust dynamics between users and institutions and the varying abilities to enforce legislation means that organisational compliance results could differ significantly per country. However, no large-scale experimental field studies similar to Degeling's web crawl have been conducted across West African websites to date.

Supporting the need for greater transparency and user education, Tchao et al., (2017) found that only 5% of the 104 respondents were aware of cookies and firewalls, which illustrates a lack of understanding surrounding basic digital privacy concepts. Participants expressed strong concerns about unauthorised data collection and the vulnerability around the misuse of their personal data, but internet usage was still relatively high. Overall, the research highlights that privacy concerns are not negligible in West Africa and there is a need for increased literacy and transparent data practices. Their findings reinforce the broader gap this dissertation seeks to address by evaluating cookie policy compliance in the region.

Chapter 3: Legal & Regulatory landscape in West Africa

3.1 Introduction to Data Protection in West Africa

In the West African context, countries such as Nigeria and Ghana have adopted GDPR-inspired principles, but as the empirical findings later on will demonstrate, the practical enforcement of these standards remains unbalanced, and the unique regional challenges of digital illiteracy, institutional oversight and a developing technical infrastructure that require attention.

In West Africa, a region characterised by rapid mobile adoption, and growing internet connectivity (Ochinanwata, Igwe and Radicic, 2023), has begun to formalise its response to online privacy and data governance. Although being historically under-regulated, the past decade has witnessed the introduction of several data protection frameworks, indicating a shift towards more structured governance.

Yet, while legislative frameworks such as the NDPA, 2023, and GDPA, 2012 exist, questions still remain about the practical enforcement of these laws. Many West African nations currently face unique regional challenges, including but not limited to, scarce regulatory resources, low digital literacy, institutional oversight and a developing technical infrastructure that require attention or may possibly impede effective privacy implementation.

Nevertheless, understanding how cookie consent is regulated across jurisdictions is essential for evaluating the global and regional landscape of compliance. Table 1 below provides a comparative summary of major data protection laws, including GDPR, CCPA (California Consumer Privacy Act), Nigeria's Data Protection Regulation and Nigeria's Data Protection Act, and Ghana's Data Protection Act. Each law differs in its approach to defining personal data, obtaining consent, and enforcing user rights.

Table 1: Comparative Overview of Key Data Protection Laws

Law/Regulation	Year	Jurisdiction	Consent Framework	User Rights	Cookie-Specific Provisions
GDPR (General Data Protection Regulation)	2018	European Union	Opt-in, freely given, informed, and specific	Access, rectification, erasure, objection, restriction, portability	Cookies must not be set before consent unless strictly necessary (Art. 6, Rec. 32)
CCPA / CPRA (California Privacy Rights Act)	2020/2023	California, USA	Opt-out model for data sales; limited consent requirement	Access, deletion, correction, opt-out of sale	No direct cookie laws; cookies fall under "identifiers" in personal data

NDPR (Nigeria Data Protection Regulation)	2019	Nigeria	Consent required for personal data processing	Access, rectification, portability, erasure	Cookies not explicitly addressed but implied under “processing”
NDPA (Nigeria Data Protection Act)	2023	Nigeria	Aligns more closely with GDPR; explicit consent basis	Enhanced user rights; introduces enforcement authority (NDPB)	Awaiting further regulations for cookie-specific guidance
Ghana DPA (Data Protection Act)	2012	Ghana	Consent required for collection and processing	Access, correction, blocking, erasure	Does not mention cookies specifically
ECOWAS Supplementary Act A/SA.1/01/10	2010	West Africa (Regional)	Requires explicit, informed consent	Data minimisation, transparency , purpose limitation	No direct provisions on cookies; depends on domestic adoption

In West Africa, the ECOWAS Supplementary Act A/SA.1/01/10 functions as a regional instrument aimed at harmonising privacy standards. Modelled loosely on early European frameworks, the ECOWAS Act requires that data be processed lawfully, fairly, and with informed consent. However, the implementation of the Act remains uneven across member states. For instance, while Nigeria has progressed by replacing the NDPR with the more comprehensive NDPA, in 2023, other states such as Ghana continue to operate under older legislation, and nations like Sierra Leone and Cameroon have yet to pass enforceable data protection laws (see Appendix C). In practice, this means that legal protections regarding cookie use and online tracking remain underdeveloped or non-existent in much of the region. Kuaban et al., (2024) touch upon how nations such as Cameroon are struggling to establish themselves in a rapidly evolving landscape, further implying that legislative development of data protection laws is scarce.

Despite these emerging regulatory frameworks, empirical studies continue to show that users often misunderstand what cookies are and how they function. Ha et al. (2006) highlighted that many users believe cookies are solely for remembering logins or settings, without realising their use in advertising and surveillance. This misconception directly impacts how users respond to consent banners. A user who does not fully understand what they are consenting to cannot, by legal definitions, provide informed consent.

The landscape of tracking, consent, and regulation is thus marked by technical complexity, regulatory ambition, and practical failure. On one hand, legal regimes such as the GDPR have created a clear standard that places user consent at the heart of data processing. On the other hand, actual implementations frequently fall short due to manipulative designs, enforcement difficulties, or gaps in digital literacy. These tensions are likely to be amplified in emerging economies like those in West Africa, where regulatory capacity is limited, enforcement remains sporadic, and public understanding of digital privacy is low.

3.2 Nigeria - NDPR and NDPA 2023

Nigeria's journey towards a comprehensive data protection policy for its citizens began with the Nigeria Data Protection Regulation (NDPR) in 2019, who were issued by the National Information Technology Development Agency (NITDA). Although the NDPR laid foundational principles for lawful data collection and processing, it did not explicitly mention cookies or tracking technologies (NITDA, 2019). Instead, the NDPR directly addressed consent, transparency and data minimisation through broader provisions as seen in Sections 2.2 and 2.5, which required data controllers to obtain the informed consent of data subjects. Under the NDPR, enforcement was initially limited, with sanctions dependent on the number of data subjects affected or a % of annual gross revenue, whichever is higher. However, practical enforcement under NDPR remained inconsistent, and many organisations showed basic privacy notices without providing users meaningful control over the tracking technologies used against them (Nwosu, 2022).

Nevertheless, the adoption of the 2023 Nigeria Data Protection Act (NDPA) that was signed into Law by President Tinubu (Data Protection Africa, 2023). The Act steered Nigeria's approach towards online privacy towards international standards, such as the GDPR, and formally required that consent be "unambiguous, specific, and freely given," (Federal Republic of Nigeria Official Gazette, 2023), thus challenging the country's prior practices that allowed users to give implied consent through continued website use rather than explicit consent. As Nwosu (2022) and Aloamaka (2023) demonstrate the shift towards requiring explicit consent introduces a stricter expectation of compliance for organisations using cookies to adhere to. Although, both researchers do acknowledge that challenges persist particularly around enforcement of the law and the lack of users' awareness of their online privacy. Empirical observations on simulated browsing experiments by Izuogo (2019) revealed that Nigerian websites often deployed third-party cookies without obtaining informed consent from users, which reflects a further gap between regulation and real-life practices.

Overall, while Nigeria's legal framework is becoming more robust, the need for consistent enforcement and public education on their digital privacy rights remain critical to ensuring compliance with the nation's cookie consent standards.

3.3 Ghana - Data Protection Act 2012

Ghana established its data protection standards with the Data Protection Act 2012 (Act 843), making it one of the early African nations to establish legislation on personal data protection. This Act requires that a user's personal data be collected with the knowledge and consent of the data subject – Section 20 (Data Protection Act, 2012) thereby aligning with principles that are like GDPR's *opt-in* model. However, in similar fashion to the NDPA, cookies and tracking technologies are not explicitly mentioned, consequently leaving this aspect of privacy up to the interpretation of organisations.

Early evaluations of e-government websites by Nwaeze, Zavarsky and Ruhl (2017) found that among Anglophone West African nations, Ghana was the only country with a formalised data and privacy protection framework, specifically for e-government systems. This early establishment of privacy practices for government owned websites does highlight Ghana's progressiveness in legislation adoption compared to its neighbouring countries. However, translation of these frameworks into the real-world remains uncertain, as recent studies highlight the enforcement and implementation gaps.

Analysis by Amasah, Odoi and Arthur (2022) reveal that while Ghana recognises the expectation the privacy in cyberspace as a constitutional right, the effectiveness of this remains limited. These researchers emphasised that individuals' rights to privacy extends to their online activities and the need for greater regulatory specificity is stressed to effectively address emerging risks to citizens, such as online tracking. Notably, their research clearly points out that governmental bodies and large institutional actors are often more protected by existing laws in the cyberspace, than regular citizens, suggesting a gap in protection in practice.

Additionally, Cetin (2024) further criticises the underuse of Ghana's Data Protection Act, assigning it to low public awareness and weak enforcement. This lack of awareness and limited enforcement leads many users to thus rely on personal protective measures i.e browser privacy settings, rather than on institutional or national safeguards. Accordingly, although a legal framework exists to protect citizens, its practical impact on regulating cookie practices in Ghana remains limited. Supporting this, Baako, Umar and Gidisu (2019) study demonstrated that compliance with Ghana's Data Protection Act remains inconsistent in practice, as their survey of 20 active e-commerce websites found that 45% of the sites did not display a privacy policy, and 60% failed to inform users about their data collection. Despite the study's relatively small sample size, that may not be fully representative of the entire e-commerce sector, it spotlights a concerning trend of non-compliance in online data collection practices within Ghana.

3.4 The GDPR: Legal Requirements on Cookie Consent

The GDPR which came into force in May 2018, is widely regarded as the most comprehensive and influential data protection framework to exist. Its legal directives have shaped global practices regarding user consent, especially around cookies. At its core, is the principle of lawful processing, outlined in Article 6(1)(c) (EUR-Lex, 2016), which specifies that a user's personal data may only be processed through a legal basis. In particular, consent holds relevance when organisations seek to utilise non-essential cookies or cookies for one or more purposes (EUR-Lex, 2002).

Despite this, the GDPR itself does not explicitly define cookies, and instead its enforcement works in tandem with the European Union's ePrivacy Directive 2009/136/EC, which came into force in May 2011 (European Data Protection Supervisor, 2025). Together, these frameworks form the core of the legal obligations' organisations have to follow regarding cookie deployment. The landmark ruling by the European Union's Court of Justice in the Plant49 GmbH case (Case C-673/17) clarified that storing or accessing cookies on a user's device is considered to be data processing under the GDPR. Specifically, the ruling confirmed that consent for cookies must be both informed and explicit, thus rejecting pre-ticked boxes that a user must deselect to refuse consent as being valid (InfoCuria Case-law, 2019).

Article 4(11) of the GDPR states that consent must be freely given, specific, informed and unambiguous (EUR-Lex, 2016). Further reinforced by Recital 32 which explicitly requires that user consent must involve a clear affirmative action (Recital 32, EUR-Lex, 2016). As a result, websites must inform users about the types of cookies being used i.e essential or non-essential cookies and must also gain their active agreement before these non-essential cookies can be set on their devices. These rights in tandem have made it so that it is no longer adequate for websites to rely on implied consent from prolonged browsing, as a form of agreement.

The regulation places a burden on data controllers to ensure that users are fully aware of what they are consenting to. Nevertheless, Article 7 outlines the conditions to be met for consent to be valid, including providing users with the option to withdraw consent at any time, in a manner that is accessible, using clear and plain language (Article 7, EUR-Lex, 2016). Additionally, Article 5(1)(a) stipulates that all data should be processed lawfully, fairly and in a transparent manner (EUR-Lex, 2016), thus directly affecting how cookie notices are designed and displayed. Website owners and organisations must avoid persuasive tactics such as cookie walls or accept only walls, which force visitors to accept tracking as a condition for access to their service, as these violate GDPR's principle of freely given consent (Kretschmer, Pennekamp and Wehrle, 2021).

Outside of just obtaining consent, organisations must also demonstrate that it was legitimately obtained. Article 5(2), the accountability principle, obliges data controllers to retain records that prove as evidence of user interactions with consent interfaces (Article 5(2), EUR-Lex, 2016). As a result, consent is transformed from being just a symbolic checkbox into a legal obligation that is mandatory to be auditable and verifiable by third-parties. As a complement, Article 25 mandates that privacy should be embedded into a system's design, otherwise

known as ‘privacy by design and by default’ (EUR-Lex, 2016). This concept includes presenting clear choices to users and ensuring that developers disable non-essential cookies until legal consent has been given.

Lastly, within the GDPR’s robust framework is its enforcement authority. Various supervisory authorities across member states monitor compliance, conduct audits and issue sanctions for discovered violations (Recital 36, (EUR-Lex, 2016; Recital 79, EUR-Lex, 2016). GDPR’s administrative fines are up to “€20 million or, in the case of an undertaking, 4% of the total annual worldwide turnover” (Article 83(6) EUR-Lex, 2016). This is based on the severity and type of infringement. Examples of these enforcement authorities in action include France’s CNIL 50 million fine against Google LLC for insufficient and non-compliant consent mechanisms (European Data Protection Board, 2019).

For a summary of the entire GDPR framework, including its consent framework, user rights and cookie-specific provisions, see Table 1: Comparative Overview of Key Data Protection Law.

3.5 Regional Efforts: ECOWAS Supplementary Act

The Economic Community of West African States (ECOWAS) has made significant progress towards harmonising the nations of West Africa in developing data protection and cybersecurity laws across its member states. Central to this is the ECOWAS Supplementary Act A/SA.1/01/10 on the Protection of Personal Data in the ECOWAS region. Adopted in February 2010, it lays the foundational legal principles for ensuring the safeguarding of personal data within the region (Orji, 2017; Bassey, Etefia and Ebong, 2024). It serves as a common framework to guide national legislations, especially in member states that lack comprehensive data protection regimes.

This Act reflects a clear influence from global models such as the EU’s Data Protection Directive 95/46/EC, which came before the GDPR. Yet, it predates the GDPR’s stricter controls on consent and cookies. The ECOWAS Supplementary Act introduces key definitions and obligations for data controllers, including: ensuring the lawfulness of processing; protecting the integrity and confidentiality of data; and guaranteeing data subjects’ rights to access, rectify, and object to the processing of their information (Economic Community of West African States, 2010, Art. 23-29, p.10-11). These rights are similar to many of the foundational rights later implemented under the GDPR, but the Act itself does not explicitly include provisions for cookie usage or online tracking technologies, as these concepts were not yet mainstream regulatory concerns in 2010. (See Appendix C).

Regarding the enforcement procedure, Article 14 (1) of the ECOWAS Supplementary Act requires each member state to establish a national data protection regime that will be responsible for supervising and enforcing compliance (p. 7, Economic Community of West African States, 2010). These authorities will also be required to cooperate to ensure the consistency and effectiveness of standards across the region. On the contrary, as establishment and implementation have heavily relied on national political readiness and institutional ability (Lewis, 1996; Jeffries, 1993), the region is left straddled with differing levels

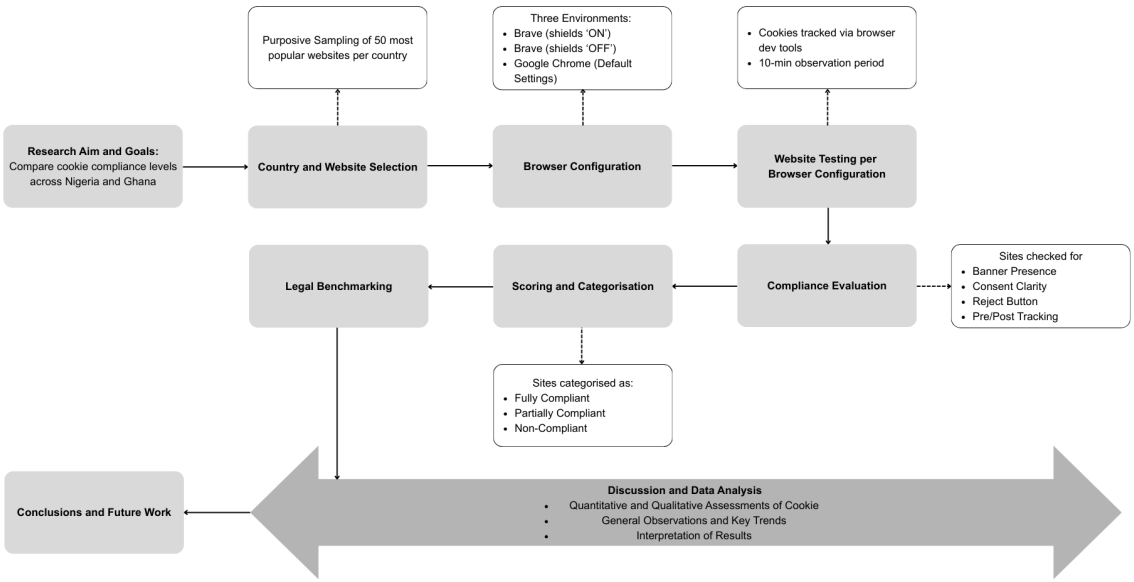
of enforcement and public awareness between countries. In the context of this research, Nigeria's own authority, the Nigeria Data Protection Commission (NDPC), was established in 2023 under the NDPA, 2023, nearly thirteen years after the ECOWAS Supplementary Act was signed. Additionally, other ECOWAS states are still developing their enforcement frameworks or have neither framework or enforcement authority (see Appendix D).

Nevertheless, the ECOWAS Supplementary ACT does not explicitly mention cookie consent or cookie notice requirements, but instead it provides a general obligation for data processing to be transparent and lawful (Article 25(1), Article 27, Economic Community of West African States, 2010). As a result, it provides a legal basis for the disclosure of tracking technologies, and the requirement of lawfully obtained consent.

In conclusion, the ECOWAS Supplementary Act on Data Protection represents a regional milestone in promoting digital individual rights and standardising privacy laws across West Africa. However, its limited scope and weak enforcement mechanisms showcase a need for modernisation and targeted provisions that address cookie consent and tracking technologies in a more explicit and enforceable manner.

Chapter 4: Methodology

Figure 1: Study Design Overview of this Paper: *Adapted with inspiration from Harper, Mehrnezhad and Leach, 2023*



4.1 Research Design

The following research adopted a comparative experimental design to evaluate cookie compliance and online tracking practices across four West African nations, with reference to

each nation's respective legal frameworks. This research aimed to measure the extent to which websites or owner(s) of websites in these four countries align with data protection requirements, specifically around cookie consent mechanisms, informed consent, cookie notice transparency, and post-consent behaviour.

Due to the nature of online tracking, an observational experimental approach was taken, allowing for controlled testing under standardised conditions. Three different browser configurations were used to identify variations in cookie behaviour and to test whether cookie banners and consent tools operated in compliance with the applicable legislation.

This specific design allowed for both quantitative analysis (# of cookies set before/after 10 minutes and consent), and qualitative assessment (content and placement of cookie notices on websites), which were scrutinised alongside the legal analysis.

The comparative experimental approach utilised in this study draws inspiration from Mehrnezhad (2020), who conducted a cross-platform evaluation of privacy notices and tracking behaviours across websites and mobile applications within the EU. This researcher's rigorous, browser-based approach to testing, served as a foundational model for structuring the current study’s experimental flow and legal compliance rubric.

4.2 Country and Website Selection

The research covered two major West African countries - Nigeria and Ghana - each chosen for their levels of legislative maturity, as both nations had fully comprehensive legal frameworks that could be used in reference for assessing the level of compliance a website displayed.

For each country, a purposive sampling approach was utilised to select websites based on the following criteria: high national visibility; geographical closeness; likelihood of processing personal data from local users; and ease of accessibility

Utilising semrush database, as of May 2025, as seen in Appendix A and B, websites were chosen based on their traffic rankings in descending order. In total, 50 websites per nation were selected, totalling 100 websites investigated.

4.3 Tools and Experimental Setup

To ensure a controlled testing environment, three different browsers and three different configurations were utilised for each website visited.

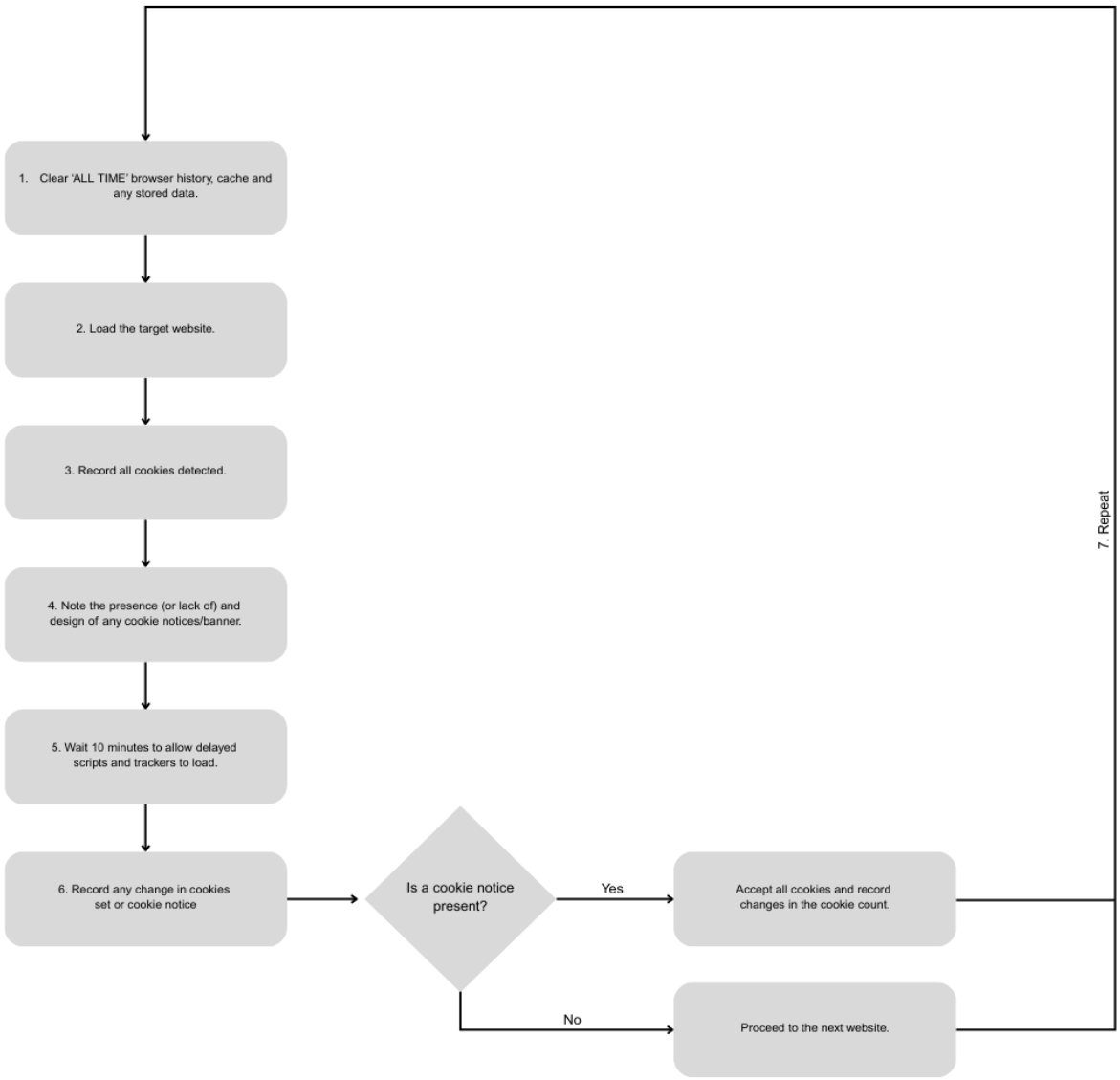
Configuration 1: Brave browser with shields ‘ON’

Configuration 2: Brave browser with shields ‘OFF’

Configuration 3: Google Chrome (default settings)

For further control, the following procedure was employed:

Figure 2: Experimental Procedure in a Flowchart: *Adapted with Mehrnezhad (2020)*



The necessary cookie data was captured by observing the browser developer tools.

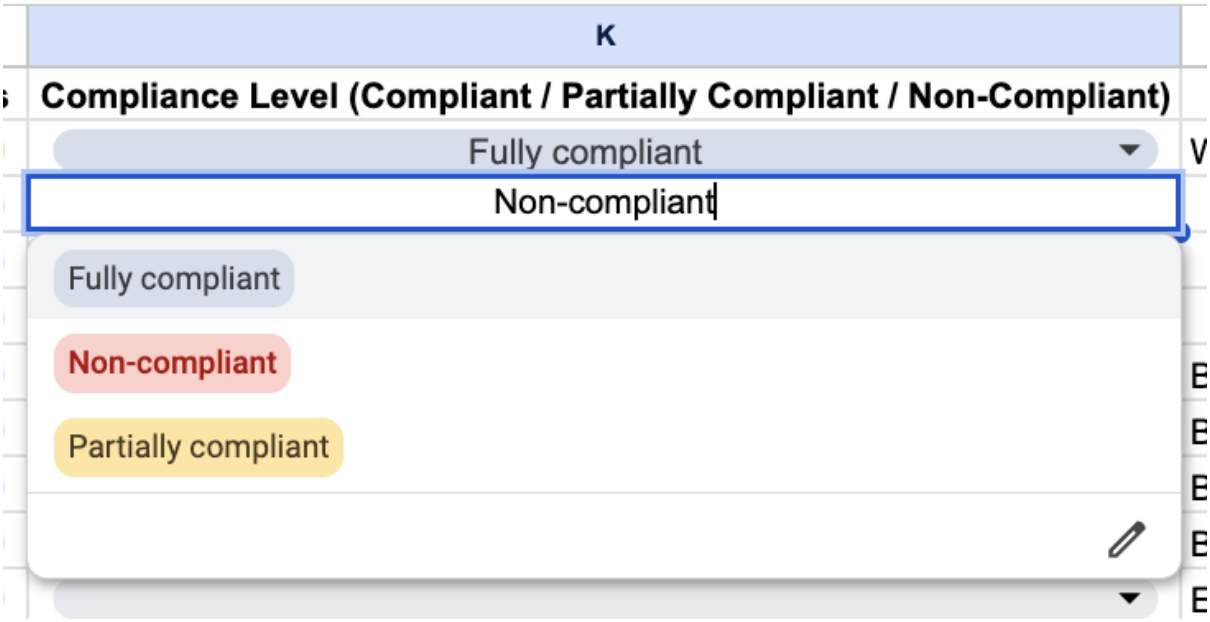
4.4 Compliance Evaluation Checklist

The evaluation framework utilised in this research combined legal criteria (drawn from each nation's respective legislation) and technical indicators observed in the experiments.

The key compliance indicators used included: the presence of a cookie banner before non-essential cookies were set; the clarity of information provided in the banner or linked policy; any observable usage of dark patterns; true consent functionality - (not forced consent); if visitors had granular control - allowing acceptance/rejection of cookies; and the websites pre-consent and post-consent behaviour.

Nevertheless, a scoring rubric was used to categorise results as ***Fully Compliant, Partially Compliant or Not Compliant****, as seen in Figure 3 below.*

Figure 3: Compliance Scoring Rubric Used



4.5 Ethical Considerations and Limitations

This study did not involve human participants or the processing of personal data, but adhered to institutional research ethics guidelines by ensuring: website testing was limited to publicly accessible websites; no attempt was made to circumvent security controls; and data collection focused solely on cookies and publicly observable consent mechanisms.

Limitations to this study include: websites may alter behaviour dynamically, meaning their compliance status could change in the future; geolocation and IP factors may influence banner presentation; one browser update occurred during the research period, which could affect detection accuracy; one VPN update occurred during the research period, which could affect geolocation; and the absence of detailed regulatory enforcement rules may limit the precision of compliance benchmarks.

Chapter 5: Findings & Results

5.1 Introduction

This chapter presents the empirical results of the experimental tests conducted on the 50 most visited websites in Nigeria and Ghana. The findings are structured to firstly present the overall patterns in cookie practices before exploring country-level compliance trends and making comparative insights. Both quantitative - cookie counts, and compliance scores) and qualitative (consent banner design, clarity of information, visitor granular control) results are reported.

The results are not interpreted in depth in this chapter, instead that analysis has been reserved for Chapter 6: Discussion, but have been presented in a way that highlights a clear link to the legal frameworks set out in previous chapters.

5.2 Overview of Websites Tested

A total of **100** websites were tested across two jurisdictions using Brave (with Shields ON), Brave (with Shields OFF), and Google Chrome (default settings):

- **Nigeria**: 50 websites
- **Ghana**: 50 websites

Websites were selected using Semrush's database (as of May 2025), which was a list of each nation's 50 most visited websites based on user traffic across all industries, including commercial services, media outlets, and global platforms, as reproduced in Appendix A and Appendix B for further reference.

5.3 General Patterns in Cookie Practices

5.3.1 Pre-Consent Cookie Placement

A recurring and concerning pattern was the deployment of third-party cookies before any consent was obtained. Even with Brave Shields ON, tracking cookies and scripts were detected on 90–95% of websites across Nigeria and Ghana.

Table 2: Average Cookies per Browser Configuration

Browser Configuration	Average Cookies (Pre-Consent)	Average Cookies (Post-Consent)
Brave with Shields ON	5.610545791	5.804347826

Brave with Shields OFF	30.44472711	41.95555556
Google Chrome (Default Settings)	57.38132388	71.90232108

5.3.2 Post-Consent Behaviour

Where banners were present (e.g., *google.com*, *temu.com*, *chatgpt.com*), cookie volumes sometimes increased post-consent, which is expected. However, many banners appeared to be **non-functional**, as the number and type of cookies remained constant even after clicking buttons—implying **false or ineffective consent mechanisms**.

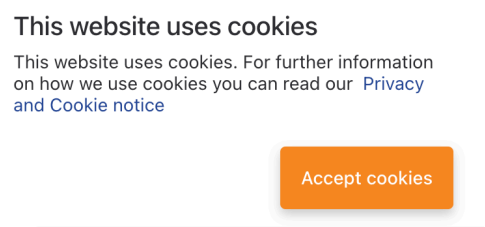
Figure 4: Lack of Change in # of Cookies Pre-Consent and Post-Consent

# of Cookies (Pre-10mins & consent)	# of Cookies (Post-10mins & consent)
3	3
4	4
13	13
3	3
10	10

5.3.3 Banner and Reject Button Visibility

Of the 100 websites tested across Nigeria (8) and Ghana (18), a few results are shocking. The study found that should a visitor on Google Chrome access the 100 websites tested, only 26 websites (8 in Nigeria, 18 in Ghana) displayed banners with visible 'accept' and 'reject' buttons. Next, the partially compliant cookie notices utilised 'accept only' buttons with no 'reject' option available, as seen in Figure 5 below and in Appendix E. Lastly, over 90% of tested websites had no banner or insufficient cookie notices that do not gain legitimate user consent.

Figure 5: Example of 'Accept' only Dark Pattern Used.



5.4 Country-Level Results

5.4.1 Nigeria

A. Brave browser with shields ON

Overview

In this first browser configuration, Brave browser was utilised with shields 'ON', displayed a significant failure in cookie consent compliance across the 50 websites tested. It revealed a shortfall in NDPA-aligned cookie consent practices, with only five websites displaying full or partial compliance. However, Brave's shields are known to automatically block intrusive tracking technologies and cookie notices altogether, which may have had a noticeable impact on the number of observable websites that complied with the legal expectations set the the NDPA, 2023.

General Compliance Findings

Two websites of the fifty tested, were found to be fully compliant: google.com, and temu.com. These websites sufficiently met Nigeria's Data Protection standards by delaying cookie consent placement until after user interaction and provided clearly visible cookie notices with clear options for user consent. One website, jumia.com.ng was categorised as partially compliant due to presenting a cookie banner with an appropriate 'accept' button but no subsequent 'reject' option could be found. In hindsight, this site can be categorised as more non-compliant with NDPA's legislation. The remaining forty-seven sites were high-traffic platforms such as *x.com, youtube.com, and amazon.com,* which were all non-compliant as they failed to meet basic consent requirements, due to deploying cookies before consent was granted.

Pre-Consent Tracking

During the initial ten-minute page loading, despite the active Brave shields, many websites still succeeded in placing cookies before user consent was given. Cookie volumes ranged from 0 to 28, with some of the most common cookie purposes for advertising, analysing and session management (e.g. NID or guest_id_ads). On average, approximately, 5.391304348 cookies were placed per site prior to consent.

Post-Consent Tracking

Following the ten-minute observation period, the volume of cookies steadily increased across the 50 sites tested. The range varied from 0 to 27 cookies, averaging approximately 5.739130435 cookies being placed after user consent was given. The common cookie purposes also included being for further personalised advertising, session management and analytics for guest users to the site. As seen in figure 6 below, some of these cookies are specifically tailored to visitors on the site, who do not have a registered account yet.

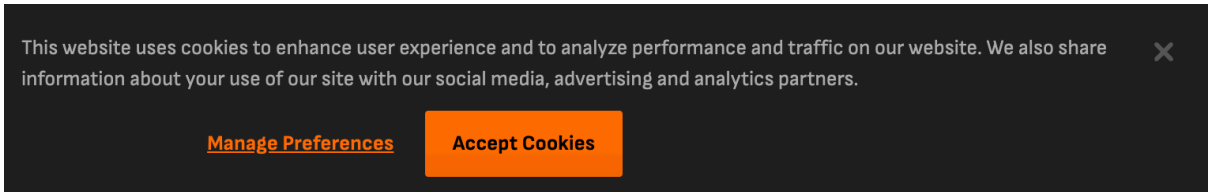
Figure 6: Example of a Guest Cookie Deployed

Name	Value
__cf_bm	TS8Owsw3DCBRQ1RK1Bf2qRtX0ViBI3zn...
d_prefs	MjoxLGNvbnNlbnRfdmVyc2lvbjoyLHRleH...
gt	1937726723912569123
guest_id	v1%3A175082502684218239
guest_id_ads	v1%3A175082502684218239
guest_id_marketing	v1%3A175082502684218239
personalization_id	"v1_Ov2OfpDxxIZSaCUS4DEONQ=="

Banner & Button Visibility

Over the entire page load, roughly 85 to 90% of websites tested lacked or did not display a visible cookie banner with a user consent mechanism. While it is possible that due to Brave's cookie banner blocked by default (Brave Software, 2022), it showcases a wider lack of compliance strategies used by websites targeting or catering to citizens from Nigeria. Amongst the few websites that had banners visible, many lacked critical user consent mechanisms, usually a 'reject' button was not present.

Figure 7: Example of a Lack of a 'Reject' Button



Special Cases

The notable outlier in this dataset was bbc.com which instead of a cookie notice, the site displayed a privacy update pop-up upon entry, as seen in Appendix F. However, this did not serve an adequate cookie banner as it did not offer any options for a user to select 'accept' or 'reject' non-essential cookies. This can be seen in the image below.

Table 3: Summary of Cookie Consent Compliance for Nigerian Websites using Brave (shields ON)

Compliance Level	***Number of Sites (#)***	***Percentage (%)***
Fully Compliant	2	4%

Partially Compliant	1	2%
Non-Compliant	47	94%

B. Brave browser with shields OFF

Overview

In this configuration, the Brave browser had its shields 'OFF', allowing all scripts and cookie notices to load naturally. The findings from this setup revealed a significant lack of compliance with NDPA, 2023, with only three websites meeting the full compliance standards for Nigeria. The remaining forty-seven websites showcased major legal and ethical shortfalls, including but not limited to: deployment of pre-consent tracking technologies, deceptive banner interfaces, and limited user choice mechanisms.

General Compliance Findings

Unlike the prior configuration using Brave with shields 'ON', this configuration exposed the more natural behaviours of these websites transparently, due to the software's cookie banner blocking by default feature being disabled. The three fully compliant websites: *flashscore.com.ng, temu.com,* and *msn.com* provided users with clear consent notices and interfaces that allowed for both acceptance or rejection of non-essential cookies, thus adhering to NDPA standards. The remaining forty-seven websites provided insufficient levels of compliance due to: 'accept only' buttons with no visible 'reject' option for cookies; implied consent mechanisms in which cookies were placed from just using the website; and consent being bundled in with the acceptance of the Terms of Service, contravening NDPA Section 34(1)'s freely given consent rule.

Pre-Consent Tracking

During a ten-minute observation window per website loaded, it was revealed that cookies were frequently set prior to any consent being given by the user. In particular, the volume of cookies placed before consent was granted ranged from 0 to 200, with an average of approximately 21.80434783 cookies placed prior to consent. The most common purposes for these cookies seemed to be for advertising and analytics.

Figure 8: Examples of Cookies Deployed for Advertising & Analytics Purposes

wa_csrf	6uF4OsVL0z5yk3vHiZk9BT
wa_lang_pref	en
wa_ul	72de75fa-5b37-418b-9eb0-73...
personalization_id	"v1_1E7w25CUlgNxfs7uZYZsjQ...
device-id	bbfc8e9d-fe3c-423c-81bc-49...
locale	en
redirect_to_int	1
sb_country	ng
sb_fs_flag	false
sb_fs_id	d95618c4-acad-4f3d-a40a-9...

These observed results likely violate the NDPA's rules regarding the lawful and transparent processing of data prior to consent being given.

Post-Consent Tracking

After the ten-minute observation window, in cases where cookie banners were available, the volume of observable cookies loaded after consent increased significantly. Post-consent tracking ranged from 0 to 603 cookies, with an average of 35.51111111 cookies per site. This sharp increase in tracking after consent suggests that non-essential cookies were technically disabled until consent was acquired, but the legality of this setup is to be questioned when consent was obtained using deceptive or one-sided tactics. These cookies often were placed for the purpose of cross-site profiling and data aggregation, causing further scrutiny to be placed on the suitability of these consent frameworks.

Banner & Button Visibility

Only 8 of the 50 websites (16%) loaded, displayed a visible banner cookie notice or pop-up, while the remaining 42 of the 50 websites (84%) lacked a visible cookie notice. Of the 8 websites, just 3 sites (37.5%) provided users with the option to explicitly 'reject' the use of cookies during their session. The remaining 5 websites instead employed unethical tactics such as 'accept-only', as seen in Appendix E or 'consent to cookie use from using the website' as a form of "consent" as seen in Figure 9 below.

Figure 9: Example of Implied Consent through Continued Use of the Site

Special Cases

A noteworthy outlier was yahoo.com, as this site recorded an unusually high volume of cookies and utilisation of aggressive third-party tracking technologies. Furthermore, prolonged loading of the site resulted in noticeable device slowdown over the observation period. Combined with

the absence of a cookie notice, this site raises serious concerns over compliance with the NDPA and general data ethics.

Table 4: Summary of Cookie Consent Compliance for Nigerian Websites using Brave (shields OFF)

Compliance Level	***Number of Sites (#)***	***Percentage (%)***
Fully Compliant	3	6%
Partially Compliant	0	0%
Non-Compliant	47	94%

C. Google Chrome (Default settings)

Overview

Using Google Chrome in its default configuration offered an insight into the real-world browsing experience of the average African user, due to this browser being the most used browsing software in the region (SOAX, 2025), and it does not come with native tracking protection like Brave. The results of this configuration provide a stark picture of further non-compliance with NDPA, 2023, particularly in relation to cookie consent mechanisms. Of the 50 websites, only five displayed full compliance, while the overwhelming remaining forty-five websites failed to meet the NDPA's consent requirements.

General Compliance Findings

The five websites that displayed full compliance were: *flashscore.com.ng, temu.com, msn.com, google.com and solixdepin.net*. In the case of solixdepin.net, this site provided no cookie notice but deployed 0 cookies throughout the entire observation period, thus complying with the NDPA, 2023. The rest of these sites provided cookie notices with a visible 'reject' button and did not load non-essential cookies until clear, affirmative consent was granted. In contrast, the forty-five non-compliant websites either; lacked a cookie banner, bundled consent alongside the Terms of Service, **or simply placed non-essential cookies regardless of the user's consent option. Previously partially compliant websites such as: livescore.com, jumia.com.ng and bing.com did present users with a cookie banner, but failed to include an

option to reject cookies or utilised dark patterns, that nudged users towards accepting the notice without providing an alternative option.

Pre-Consent Tracking

Before any consent, cookies were frequently set, directly violating NDPA requirements. The volume of cookies deployed prior to consent ranged from 0 to 1,160, with an average of approximately 71.42222222 cookies per site. Noticeably, yahoo.com and legit.ng demonstrated particularly egregious behaviour, with over 800 cookies loaded without any visible request for user consent. The vast volume of these cookies raises concerns about the ethical implications of mass surveillance and potential data selling conducted without a user's knowledge.

Post-Consent Tracking

After consent was provided, where possible, the number of cookies drastically increased on many sites, with the post-consent range spanning from 0 to 1,235 cookies. An approximate average of 83.27272727 cookies per site was revealed. An example would be flashscore.com.ng which spiked from just two cookies before consent to over 280 cookies after user consent.

Banner & Button Visibility

Of the 50 sites tested, only 9 websites (18%) showcased a cookie notice or form of user consent mechanism. However, out of the 9 websites, just 4 (44.4%) included a clear option to reject cookies. These four sites were: *google.com*, flashscore.com.ng, *msn.com, and temu.com.* The remaining utilised coercive practices, for instance, pornhub.com and betking.com displayed banners that stated the continued use of the site was a form of user consent, despite this being explicitly non-compliant with NDPA regulations (see Appendix G).

Special Cases

A number of outliers within this dataset warrant specific mention, but in particular, globally recognised platforms such as: *facebook.com, youtube.com, x.com* and *instagram.com* did not present any cookie notices or options to control tracking. This is a troubling finding in light of their reach and influence across the world. Although, it is important to note that it is possible a cookie notice could be displayed after a user has created an account with these platforms before a notice is shown.

Table 5: Summary of Cookie Consent Compliance for Nigerian Websites using Google Chrome (Default Settings)

Compliance Level	***Number of Sites (#)***	***Percentage (%)***

Fully Compliant	5	10%
Partially Compliant	0	0%
Non-Compliant	50	90%

5.4.2 Ghana

A. Brave browser with shields ON

Overview

Promptly moving onto the Ghanaian dataset, the use of Brave with shields 'ON' revealed critical insights into cookie consent practices among high-traffic websites. This setup simulates a privacy-aware user's browsing experience where built-in protections automatically block trackers and third-party cookies by default (Brave Software, 2022). Despite these protections, the results showcased that the overwhelming majority of websites failed to meet the standards under Ghana's DPA, 2012. On the contrary, it is important to note that brave's shield's may have played a larger role in blocking significant volumes of tracking infrastructure and may have hindered the display of cookie banners. Nevertheless, out of the 50 websites tested, only three were fully compliant with adequate practices, while the remaining forty-seven were non-compliant.

General Compliance Findings

The three websites found to be fully-compliant were: chatgpt.com, piaproxy.com and google.com. These sites presented cookie banners (where Brave permitted them to load), offered users the ability to reject non-essential cookies, and only deployed cookies once consent was given. However, elements such as briefly flashing banners suggest that Brave active shields may have disabled scripts or technically suppressed user cookie notices, thus raising complexity about how many other websites are false non-compliant as a result of browser intervention or if it's due to inadequate website compliance.

The remaining forty-seven websites were deemed non-compliant according to the compliance checklist, primarily due to the complete absence of any visible user cookie notice, a failure to offer meaningful choice, or the deployment of cookies without legitimate user consent.

Pre-Consent Tracking

The number of cookies set before consent ranged from 0 to 20 cookies, (with the exception of some highly protected sites where Brave intervened and blocked upwards of 20 ads, trackers and more. Bing.com and microsoft.com placed 20 and 11 cookies respectively, despite no affirmative action being taken by the user. In other cases, cookie storage occurred in the background, without the user's knowledge, essentially undermining the legal requirement for prior and informed consent under GDPA, 2012. The average pre-consent cookie load across all 50 websites in this browser configuration was approximately 5.829787234 cookies.

Furthermore, Brave shields blocked a wide range of ads, trackers and more across various domains, including: 36 on microsoft.com; 17 on aliexpress.com; and 22 on openai.com These sidenotes showcase the widespread nature of tracking technologies and how platforms rely heavily on these third-party technologies to aggregate and process data before any interaction with the site has occurred.

Post-Consent Tracking

On websites that were fully compliant with GDPA, 2012, cookies loaded as expected — only after explicit user consent was granted. The post-consent cookie loading observable on these sites was more modest, ranging from 0 to 17 cookies. However, for the overwhelming number of non-compliant websites, post-consent is a more misleading title, as cookies were set on the user's device regardless of any consent procedure.

Other websites like bing.com, and amazon.com loaded additional tracking cookies without ever asking users for consent, which is a direct breach of user rights under Ghana's GDPA, 2012. Brave's shields further reinforce this as the shields blocked a further 16 additional ads, trackers and more, across both websites.

Banner & Button Visibility

Only 3 websites (6%) out of 50 sites visited, displayed a visible cookie banner or consent pop-up while using Brave with shields 'ON'. Of those, 2 of the 3 sites (66.7%) were: chatgpt.com and piaproxy.com which provided a visible 'reject' button and hindered tracking until a decision was made by the user. The other website, google.com, did not display a functional banner throughout the observation window, but instead the banner briefly flashed across the user's device. This was possible due to Brave's shield, but was considered compliant based on prior observations and cookie behaviour.

The remaining 47 of the 50 websites (94%) either failed to load a banner entirely, or combined tracking consent with other agreements like continued site use, without offering users any control over their preferred cookie settings. This behaviour falls short of Ghana's Data Protection Act's stipulations on informed and unambiguous consent.

Special Cases

Some outlier websites deserve individual mention. chatgpt.com was notable for its nuanced cookie control settings, with users able to explicitly reject non-essential cookies before interaction, which was a rare example of good practice within Ghana.

On the other hand, bing.com's cookie count heavily fluctuated throughout the entire observation window, and popular forum website reddit.com was unable to be viewed as it was blocked by local ISP or network security (see Appendix H). This may have been a result of using the VPN.

Table 6: Summary of Cookie Consent Compliance for Ghanaian Websites using Brave (shields ON)

Compliance Level	***Number of Sites (#)***	***Percentage (%)***
Fully Compliant	3	6%
Partially Compliant	0	0%
Non-Compliant	47	94%

B. Brave browser with shields OFF

Overview

Disabling Brave browser's default privacy protection features (shields 'OFF'), the experimental dataset revealed more compliance with GDPA, 2012, but still not a significant change. Compliance still remained relatively low, with only twelve websites tested being fully compliant with GDPA, 2012. The remaining websites showcased partial compliance or no compliance by failing to present any cookie notice, initiated prior tracking technologies or utilised deceptive techniques to secure user consent.

General Compliance Findings

With Brave's protective shield 'OFF', this configuration allowed for a more direct evaluation of whether websites were technically aligned with Ghana's data protection obligations. Just 12

out of the 50 websites (24%) tested were fully compliant with GDPA, 2012, displaying banners that featured clear information about cookie use and enabled users to decline non-essential cookies as easily as accepting them. Two additional websites (4%) displayed partial compliance, generally by offering consent mechanisms that had a visible reject button but still deployed non-essential tracking before clear consent had been registered. The remaining 36 of the 50 websites (72%) outright failed in presenting any form of cookie notice or function for users to exercise control, placing them in clear breach of Ghana's data protection requirements.

These sites typically engaged in immediate tracking upon visiting or concealed consent within broader terms and conditions, which does not satisfy the requirement for specific, informed, and freely given consent (Data Protection Act, 2012, ss. 20(1), 22, 23, 35(1)(b)).

Pre-Consent Tracking

During the ten-minute observational window, before any active user interaction or consent was given, the number of cookies placed varied widely across the sample. In several cases, the tracking activity was minimal or negligible. Approximately, an average of 39.08510638 cookies were set prior to consent. However, on the more extreme end, websites such as yahoo.com placed over 850 cookies before the user had a chance to engage with any notice or provide affirmative consent. Similar patterns were observed on ghanaweb.com, where cookies continued to be placed in a seemingly infinite loop, as a result of scrolling background ad scripts. The most common purposes of these pre-consent cookies included session management, third-party advertising, behavioural profiling, and cross-site user tracking.

Post-Consent Tracking

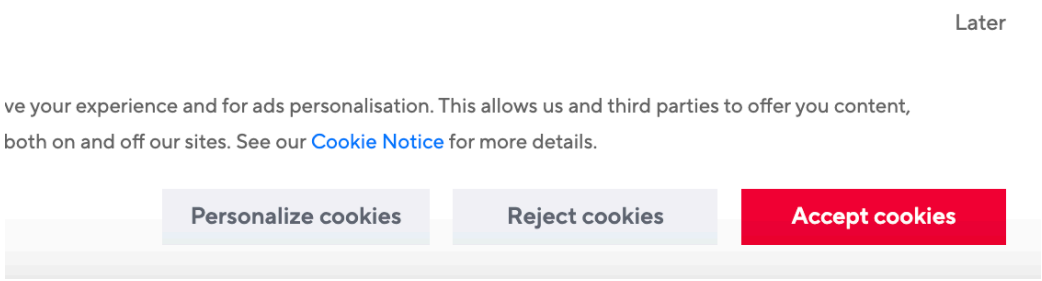
After the initial observation window, in cases where a cookie notice or consent could be granted, the volume of cookies set continued to rise significantly, with approximately 48.4 cookies set per website. For example, on msn.com the total number of cookies rose from forty-two to fifty-four following consent. Similarly, canva.com initiated cookie placement prior to consent, with cookies increasing from eight to forty-three post-consent. Although these increases were not inherently problematic when preceded by valid consent, the trend across most websites tested showcased a worrying pattern of intensified tracking activity, regardless of whether the user had meaningfully opted in or not. This phenomenon raises questions about the integrity and sincerity of consent mechanisms and whether users are fully informed about the breadth of data collection that follows their interactions.

Banner & Button Visibility

In spite of the removal of Brave's cookie banner blocking by default, banner visibility still remained fairly limited. Only 17 of the 50 websites displayed a form of cookie notice, which out of these websites, 13 of the 17 sites provided users with a visible 'reject' button to refuse non-essential tracking. In some instances where banners were present, aliexpress.com employed some design-based manipulation such as a brightly coloured 'accept' button

contrasted against a less noticeable reject button, as seen in Figure 10 and included in Appendix I for reference.

Figure 10: Example of Colour Manipulation on 'Reject' Button

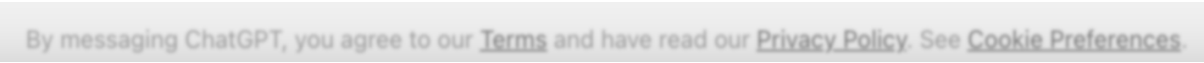


Another noticeable instance was, in deepseek.com whereby users were provided with an option to 'refuse non-essential' cookies. As this is not technically a 'reject' button, it was categorised as being partially compliant with Ghana's DPA, 2012.

Special Cases

Nevertheless, some websites exhibited problematic behaviours. For instance, yahoo.com not only placed hundreds of cookies without consent but also triggered noticeable performance degradation on the test device, presumably due to the volume and complexity of its background ad scripts. A particularly flagrant example was during the testing of chatgpt.com, where a singular message at the bottom of the interface read that "by messaging chatgpt, you agree to our Terms and have read our privacy policy. see cookie preferences", as seen in Figure 11 below and included in Appendix J for reference.

Figure 11: Example of ChatGPT.com's Implied Consent



This approach does not meet the legal standards or requirements of Ghana's DPA, 2012 or even widely recognised international frameworks like the GDPR.

Table 7: Summary of Cookie Consent Compliance for Ghanaian Websites using Brave (shields OFF)

Compliance Level	***Number of Sites (#)***	***Percentage (%)***
Fully Compliant	12	24%

Partially Compliant	2	4%
Non-Compliant	36	72%

C. Google Chrome (default settings)

Overview

In this last browser configuration, Google Chrome was utilised with its default settings, and this dataset revealed similar results to the previous configuration (Brave with shields 'OFF') with improved yet relatively low cookie consent compliance levels. Without the same native privacy protection as Brave, Google Chrome allowed for full usage of tracking technologies and consent banners by organisations. Despite this fact, only a handful of websites met Ghana's data protection regulations, with an overwhelming majority showcasing a continued failure of being non-compliant with GDPA, 2012.

General Compliance Findings

Of the fourteen sites that were fully compliant with GDPA, 2012, they include: google.com, msn.com, band.us, tempail.com, audiomack.com, spotify.com, and flashscore.com.gh. These websites presented explicit banners with a clearly visible 'reject' button and only placed cookies after consent was given. Although some websites such as livescore.com and deepseek.com had cookie banners, they showed no visible reject button and utilised dark patterns such as implied consent from continued use of the website and 'accept only' buttons. Non-compliant websites did not display any form of cookie notice for providing users with unambiguous and informed consent. In fact, they typically began tracking immediately after the sites were visited without any visible links or privacy notices for users to interact with.

Pre-Consent Tracking

Nevertheless, the results revealed a significantly high volume of cookie placement prior to consent being given. In particular, ghanaweb.com placed a total of 335 cookies throughout the ten-minute observation period, audiomack.com placed 376 cookies in the same timeframe. Approximately, 43.34042553 cookies were placed per site. In stark contrast, fully compliant sites deferred any cookie placement until consent was granted, or loaded the bare minimum session cookies for the websites essential functions.

Post-Consent Tracking

Post-consent, there was a notable yet unsurprising rise in cookie volumes across most sites. Approximately, 60.53191489 cookies were set per site tested. Audiomack.com rose from 376 to 433 cookies, canva.com from 9 to 41 cookies and msn.com from 23 to 30 cookies. Although these increases are not problematic when they have legally complied with Ghana's DPA, their intensity of the tracking technologies placed requires further exploration and exploration into the malicious activities that come with users accepting third-party cookies.

Banner & Button Visibility

Out of the total sample of only 47 sites fully loaded (3 sites server address could either not be found or had DNS resolution issues), only 18 sites (38.20%) displayed any form of cookie banner. Among these 18, only 14 provided users with both an 'accept' and 'reject' option, thus meeting the basic requirements for a valid consent notice/interface. The remaining 4 banners utilised deceptive dark patterns such as: an 'accept only option'; combining cookie consent with the TOS; and user interface obfuscation to hide the 'reject' button. For further reference of the user interface obfuscation, refer to Appendix I.

Special Cases

Specific websites demonstrated notable anomalies. Repeatedly yahoo.com showed extreme cookie volumes, reaching up to 712 cookies set post-consent, which resulted in a significant decline of the host device's ability to operate. Deepseek.com allowed only binary choices between "accept all" or "necessary only," lacking granularity. Pornhub.com displayed a notice that consent was implied through site use, which is inconsistent and non-compliant with Ghana's DPA. Meanwhile, several platforms such as microsoftonline.com, 808ball.com, and moviebox.ng failed to load altogether, and were thus excluded from cookie analysis.

Table 8: Summary of Cookie Consent Compliance for Ghanaian Websites using Google Chrome (Default Settings)

Compliance Level	***Number of Sites (#)***	***Percentage (%)***
Fully Compliant	14	28%
Partially Compliant	1	2%
Non-Compliant	35	70%

5.5 Comparative Compliance Scores

Table 9: Comparative Cookie Consent Compliance Rates Across Nigerian and Ghanaian Websites (n=150 browser–website observations per country)

Country	***% Fully Compliant***	***% Partially Compliant***	***% Non-Compliant***
Nigeria	6.67% (10/150)	0.66% (1/150)	91.33% (137/150)
Ghana	15.33% (23/150)	2.00% (3/150)	80.67% (121/150)

The comparative compliance analysis shows a strikingly low level of adherence to cookie consent obligations in both Nigeria and Ghana, no matter the browser settings. This section provides a summary of compliance scores across three different browser setups: Brave with shields on, Brave with shields off, and Google Chrome with its default settings. The aim here is to see if the technological environment affects how websites handle cookie consent banners and mechanisms, as well as to assess overall regional compliance with national and international data protection laws like the NDPA in Nigeria, the upcoming Ghanaian Data Protection Act, and the GDPR.

In Nigeria, finding fully compliant websites was quite rare across all configurations. Only two websites managed to achieve full compliance with Brave shields enabled, and three did so with shields disabled. When using Google Chrome, that number crept up to five. Partial compliance was almost non-existent, with just a few websites offering consent banners but missing reject buttons, which clearly violates lawful consent standards. The overwhelming majority of websites, over 90% in every browser configuration, were deemed to be non-compliant with both legislation frameworks across Nigeria and Ghana. These sites either didn't display a banner, employed coercive designs known as "dark patterns," or placed cookies before securing meaningful consent. This widespread issue indicates a general disregard by data controllers for NDPA obligations or a lack of awareness among site operators regarding current compliance requirements.

Ghana showed trends that were strikingly similar to those in Nigeria. Just like in Nigeria, only a handful of websites managed to meet the full legal requirements across the three different browser setups. In the Brave Shields ON scenario, a mere two websites were fully compliant. When the shields were turned off, that number jumped to ten. Under Google Chrome, eleven websites achieved full compliance. Just like in Nigeria, the number of partially compliant sites was quite limited, with over 85% of websites in Ghana ultimately falling short of compliance.

Interestingly, a few platforms did see an improvement in compliance when using Chrome—likely because this browser is less aggressive in blocking scripts compared to Brave, which allowed websites to load their banners more consistently. However, the quality of these banners often left much to be desired when examined closely.

The slightly higher full compliance rate in Ghana might indicate either regional differences in web development practices or varying levels of exposure to international legal standards. Nevertheless, both countries exhibit significant shortcomings in providing users with lawful, informed, and freely given consent. These findings echo concerns highlighted in global privacy research, which suggests that low and middle income countries are especially at risk of inadequate digital rights enforcement due to a mix of legal uncertainty, insufficient enforcement infrastructure, and technological disparities.

Chapter 6: Discussion

This chapter critically analyses the results of the experiment performed in Chapter 5, connecting the results to the legal frameworks discussed in *Chapter 3: Legal Framework Analysis* and existing literature in *Chapter 2: Literature Review*. It evaluates the level of compliance that websites adhere to in each country, investigates the underlying reasons for observed patterns, and reflects on broader issues for user privacy and digital governance in West Africa and developing regions. Furthermore, cross-nation comparisons are made to spotlight structural challenges, specific website behaviours, and browser specific dynamics.

6.1 General Observations and Trends

Across the 100 websites tested, the most dominant trend was a persistent, pervasive lack of compliance with each nation's data protection regulations. Even in the two countries with comprehensive legal frameworks (Nigeria and Ghana), a noticeable lack of enforcement enabled ineffective technical implementation of cookie consent protocols.

6.1.1 Pre-Consent Tracking as the Default

Results of the experiment confirmed widespread pre-consent cookie placement when a user visited a website, regardless of cookie preferences. This default, is a clear violation of two laws in both jurisdictions this research surrounds; Nigeria's Data Protection Act, 2023 (Federal Republic of Nigeria Official Gazette, 2023), and Ghana's Data Protection Act, 2012 (Data Protection Act, 2012). For the NDPA, 2023, relevant violations include sections 24(1)(a-b), 25(1)(a), 26(3), 26(6), 26(7)(a), 27(1), (36(1), and 35(1). Similarly, relevant violations for the GDPA, 2012, include sections 17, 18(1), 20(1), 23, 35(1)(b) and 39(1).

Furthermore, the results strongly highlighted that in almost all jurisdictions tested, pre-consent tracking occurred in over 90% of cases. This pattern reflects a more prominent, deeper issue - that technical non-compliance is the norm and standard, not the exception, even when sufficient legislation is in place. The gap between law and reality raises growing concerns over

enforcement capabilities, digital literacy and the lack thereof among citizens, and the influence of major platforms that fail to localise their compliance efforts.

6.1.2 Cookie Banner Design and Dark Patterns

For the few cookie notices that existed, their consent interfaces were often designed to encourage user acceptance rather than support meaningful user choice due to the various dark patterns observed. The scarcity of reject buttons on first-layer banners effectively violated the NDPA and GDPA, which each have multiple sections underlining the need for users to provide consent to the data collection practices utilised by websites. Only a small percentage of websites such as temu.com, flashscore.com.ng and msn.com, provided users with a balanced interface. For full reference, example screenshots have been included in Appendix K.

Unsurprisingly, the presence of further dark patterns, such as “accept-only” (jumia.com.ng - make a link to appendix), “accepting privacy policy combined with TOS” (1xbet.ng , chatgpt.com), or in some extreme cases, “consent to cookie use just from using the website” (betking.com). These various dark patterns suggest intentional design choices to bypass regulatory inspection/investigation, aligning with prior findings that emphasise that weaponisation of interface design to subvert data protection obligations (Nouwens et al., 2020) does occur.

6.2 Summary of Key Findings

This study took an in-depth look at how compliant high-traffic websites in Nigeria and Ghana are following cookie consent rules laid out in each nation’s respective data protection laws; Nigeria’s Data Protection Act (NDPA, 2023) and Ghana’s Data Protection Act (GDPA, 2012) as well as internationally recognised standards like the GDPR. By testing 100 websites (50 from each country) across three different browser setups: Brave with Shields ‘ON’; Brave with Shields ‘OFF’; and Google Chrome (default settings), the study uncovered some serious patterns of non-compliance in both countries, which could have significant consequences for digital rights and lawful data processing.

Across all browser setups, the practice of placing cookies before consent was alarmingly common, even on sites that claimed to adhere to explicit consent frameworks. While the average number of cookies varied by browser (ranging from about 5.6 with Brave Shields ON to over 71 with Chrome), third-party tracking scripts were often activated before users had a chance to interact, violating the fundamental principle of informed consent. This is particularly concerning since consent should be obtained before any data processing occurs, as highlighted in Recital 32 of the GDPR and Section 34(1) of Nigeria’s NDPA. The prevalence of pre-consent tracking indicates a systemic neglect or lack of awareness regarding consent requirements by website operators, especially in areas where enforcement is weaker.

- The visibility and functionality of consent banners were among the most glaring shortcomings. Less than one-third of the websites tested displayed any kind of consent banner. For those that did, many were missing a clear or functional "Reject" button,

instead relying on manipulative design tactics ("dark patterns") like ‘accept-only’ options, embedding consent within terms of service, or assuming consent based on site usage. These practices fall short of the standards for freely given, specific, and informed consent mandated by all major data protection frameworks (European Data Protection Board, 2020; ICO, 2022).

Geographically, Ghana has slightly outperformed Nigeria in compliance, especially regarding the Brave Shields OFF and Chrome settings. Ghana achieved a compliance rate of 28% in Chrome, while Nigeria lagged behind at just 10%. This gap might be due to varying levels of exposure to international standards, the impact of globally hosted platforms, or differences in how enforcement is visible. Still, non-compliance was the prevailing trend in both countries, with over 80% of websites in each failing to meet basic legal requirements.

Some platforms such as google.com, chatgpt.com, and msn.com, consistently showcased best practices across all settings, utilizing delayed cookie placement, detailed consent mechanisms, and user-friendly banner interfaces. On the flip side, sites such as yahoo.com and ghanaweb.com stood out as significant outliers, with cookie counts soaring to 700–800 before any user interaction, often lacking visible banners or user controls.

To sum it all up, here are the main takeaways:

- Pre-consent tracking was almost everywhere, breaching the legal need for prior consent.

- The visibility of consent banners was shockingly low: Only 26 out of 100 sites offered meaningful banners with options to reject.

- Browser settings played a role in perceived compliance, with Brave blocking many banners, while Chrome exposed serious tracking issues.

- Dark patterns were prevalent, including "accept-only" banners, consent hidden in terms of service, and confusing reject button designs.

- Ghana had a slight edge over Nigeria in compliance rates, but both fell short of what’s considered acceptable.

- High-traffic global platforms weren’t necessarily more compliant, as sites like youtube.com, x.com, and amazon.com often failed to show banners in most tests.

- Cookie volumes spiked significantly after consent, indicating that while some banners functioned technically, they raised concerns about transparency and the purpose of data collection.

Together, these findings highlight serious gaps in how cookie consent is being handled, even on the most popular websites in the region. They also point to an urgent need for better

regulatory oversight, improved design standards, and improved public awareness within the digital landscape in West Africa.

6.3 Interpretation of Results

The empirical findings portrayed in this study highlight a profound yet consistent divide between the legislative power and intent of data protection laws in Nigeria and Ghana and their real-world practicality in emerging digital environments. Both Nigeria's Data Protection Act (NDPA, 2023) and Ghana's Data Protection Act (GDPA, 2012) embrace and draw upon core principles from the GDPR, including but not limited to: the centrality of information; freely given, and explicit user informed consent for data processing. However, the actual practices displayed by the countries most visited websites falls significantly short of these legal standards.

In Nigeria, the NDPA defines consent as a "freely given, specific, informed and unambiguous indication of the data subject's wishes" (Section 65, NDPA ,2023; Section 34(1), NDPA, 2023). However, across all three browser configurations, more than 91% of websites failed to provide even the minimum legal conditions for valid user consent. Consistent use of coercive consent notices, implied consent through continued browsing, and the complete absence of cookie notices were recurrent. The default, particularly across the mainstream browser (Google Chrome), revealed how users were routinely subjected to pre-consent tracking, which is in direct violation of NDPA principles in respect to lawful and transparent data processing.

In a similar situation, Ghana's GDPA, 2012 also places an obligation on data controllers to ensure that data subjects are informed about "the nature of the data being collected" and the "purpose for which the data is required for collection" (Data Protection Act, 2012, ss. 27(2), 35(1)). Despite this, only 28% of tested websites using Google Chrome provided a cookie banner to users with a visible 'reject' option. This absence of meaningful choice ruminates on an erosion of the user's autonomy and agency, which are fundamental pillars of data protection law globally (Ausloos, 2018; Brkan, 2019).

The wide disparity between legislative frameworks and digital practice appears to be representative of a broader issue of regulatory fragility across developing economies. As Bryant (2021) highlights, limited resources of data protection authorities across many African nations has resulted in limited investigatory ability, weak sanctioning powers and low public visibility. In such environments, compliance often becomes subjective, especially for international platforms with little motivation to abide by domestic legal obligations (Bryant, 2021). This is supported by the near-universal non-compliance observed by major global platforms such as youtube.com, x.com and facebook.com, all of which failed to display basic user consent notices across the three tests.

Moreover, the findings imply a problematic reliance on the superficial appearance of compliance without actual informed user consent. In several instances throughout the research, cookie notices were presented but lacked reject buttons, or displayed misleading colour schemes. These practices align with what Nouwens et al., (2020) and Utz et al., (2019)

have labelled as “dark patterns” — design strategies with the intention of nudging users toward consent.

On an important note, browser configurations played an unremarkable role in the observable compliance. For instance, Brave’s Shields ‘ON’, offered significantly greater privacy to users but obscured non-compliant behaviour by blocking banners altogether. Contrarily, Chrome’s permissiveness exposed more raw tracking behaviours, to reveal the full extent of websites’ non-compliance, although there was an overall increase in the number of websites found to be fully-compliant. This may have been a result of Brave’s blocking that prevented some websites from fully rendering their cookie notices.

Be that as it may, the raw tracking behaviours revealed using Google Chrome underscores the complexities between technical environments, emerging digital economies and regulatory effectiveness, raising the need for future legal standards to consider and incorporate how browser architecture influences both enforcement and user experience.

Nevertheless, the findings also give rise to a deeper reflection on legal transplantation and diffusion. As both Nigeria and Ghana have been inspired and adopted GDPR-inspired principles (Ekpo, Okokon and Akpakpan, 2024; Spirkl, 2024), yet lack the level of enforcement required that supports the GDPR’s success in the EU. Consequently, a compliance gap is left, so while laws are in place, the absence of powerful deterrents or user empowerment mechanisms limits their real-world feasibility. The issue thus, is not simply just legal drafting, but more of an emphasis should be placed on the maturity, resource availability and political will.

In this regard, the study reinforces longstanding concerns within regulatory and development literature that digital rights in developing nations remain unpredictable, not only due to legal gaps but also due to the institutional shortfalls and uneven power distribution between regulators and multinational tech firms (Hackfort, 2021). Although in Hackfort’s research, the direct focus is on industrialised contexts, the analysis of the underlying power structures and legal deficiencies provides valuable insights into the broader global landscape and its implications for digital rights, including in digitally emerging nations, where these issues have been acknowledged as requiring further research.

Nevertheless, it is likely that without coordinated regional enforcement or strong interoperable enforcement tools, the status quo is likely to persist.

In summary, while Nigeria and Ghana have robust legislative frameworks on paper, this study highlights the poor transition into actual digital practices. The overwhelming lack of compliance, especially among popular platforms, underscores the urgent need for stronger institutions, innovative regulations, and increased public accountability. Without these crucial changes, the right to data privacy risks becoming nominal rather than actionable for millions of users in West Africa.

6.4 The Role of Browser Technologies

Browser settings and technologies play a role in protecting and facilitating users' exposure to cookies and shaping the visibility of consent mechanisms. The choice of browser alongside its default settings, had a noticeable effect on both the volume of cookies deployed and the form of cookie banners.

Brave browser with its shields 'ON', provided the most privacy protected experience. Its blocking-by-default (Brave Software, 2022) of trackers, third-party scripts and cookie banners prevented many websites visited from displaying consent notices entirely. While this served the interests of user privacy and enhanced the browsing experience, it did complicate and obstruct the analysis of legal compliance, as websites were 'technically' prevented from exhibiting their consent mechanisms. As a result, this raises a challenge on how legal compliance can be measured accurately, if the user interface is altered by the privacy tool itself. Although this specific configuration simulates a privacy-conscious user, it does conceal whether the website would have been compliant with domestic legislative frameworks in a less restrictive context.

On the contrary, turning Brave shields 'OFF' provided a clearer lens for websites to be assessed for their legal compliance. In this experimental environment, there was noticeably improved and more consistent cookie notice rendering, allowing the true design patterns and cookie mechanisms employed by website operators to be exposed. Despite this more permissive setup, overall compliance remained critically low across both jurisdictions, therefore implying that browser suppression alone, is not the main driver of non-compliance.

However, the browser with the most implications for user privacy was Google Chrome (Default Settings). As the most dominant browser across Africa (SOAX, 2025), holding 76.37% of the market share (StatCounter Global Stats, 2025), it provided a meaningful simulation for the average user experience of individuals living in Nigeria and Ghana. In direct contrast to Brave, Google Chrome offers no default tracking protections. Consequently, some websites deployed the highest volume of cookies, both before and after consent was obtained. In addition, cookie notices on Chrome often lacked 'reject' buttons or used dark patterns to influence user informed consent, calling attention to the fact that the most dominant browser in the region is inherently less privacy-protective for users (Ul Haque, Khan and Fahim, 2023), which may amplify online risks in low-enforcement regions.

The browser-dependent variables challenge assumptions in data protection laws that users visit and interact with websites under informed and transparent conditions. There is further discussion to be had about browser behaviour in digital rights assessments.

6.5 Regional Challenges in Enforcement and Awareness

It is imperative to consider the other challenges faced in West Africa to enforce these data protection laws. In Nigeria, the Nigeria Data Protection Commission (NDPC), although legally empowered, does continue to face critical challenges in resource allocation, staffing, and rapid technological growth (Nigeria Data Protection Commission, 2025). The combination of these

challenges allows the institutional fragility to contribute to the widespread liberties that website operators take for granted, as observed in this study, where over 90% of websites failed to meet the basic legal thresholds for valid cookie consent.

Although, it would be inaccurate to characterise the NDPC as entirely ineffective, there have been a couple of instances in which the NDPC has effectively asserted its regulatory authority when adequately mobilised. On a domestic level, a high-profile enforcement case involved Multichoice Nigeria, who in early 2025 was fined ₦766million for violating the NDPA for unauthorised actions. These violations included the unauthorised processing of personal data; illegal cross-border transfers of personal data; and intrusive and disproportionate data processing (Camillus Eboh, 2025; Anuku, 2025) that infringed on the rights of Nigerian citizens. On an international level, the NDPC made headlines in July 2024, after a joint investigation by the NDPA and the Federal Competition and Consumer Protection Commission (FCCPC), issued Meta a $220million administrative fine for discriminatory practices against Nigerian users due to their failure "to provide Nigerians the opportunity to self-determine or otherwise withhold consent to the gathering of their data" (Broersma, 2024).

These enforcement actions against organisations showcase a positive evolution for Nigeria's enforcement authority, signalling a willingness of regulators to hold domestic and multinational organisations accountable. Crucially, these actions demonstrate that Nigeria's legislative frameworks are not just symbolic, but that with sufficient support and resources, it has the potential to serve as a robust authority for safeguarding citizens' data privacy.

In Ghana, the situation is more opaque. While the GDPA, 2012 is still in effect, Ghana's Data Protection Commission (GDPC) has yet to impose any visible sanctions or regulatory fines for non-compliance in this area. As a result, a perception of legal dormancy may have been created, in which website operators face little to no meaningful consequences (Foe-Ahorney, 2024) for failing to comply with Ghana's Data Protection Act, 2012. This instantiates what Grattet and Jenness (2008) discuss as the risk of laws becoming primarily symbolic rather than operational, particularly in instances whereby there is a lack of corresponding 'activation' through robust 'agency and community processes'. As a result, these studies suggest that compliance can thus become a discretionary act, rather than a legally obligated one.

The enforcement void in both Nigeria and Ghana is further exacerbated by low levels of awareness and digital literacy. As Ha et al., (2006) observed nearly two decades ago, internet users often possess a limited understanding of what cookies are and their impact on privacy. Nearly two decades later, this issue remains largely unresolved in West Africa, particularly amongst everyday users.

While modest progress has been made in governmental education efforts, it remains narrowly focused. In Nigeria, the NDPC launched its Virtual Private Academy to enable users "at all levels to understand and apply data privacy principles in practical ways, fostering a culture of responsibility and compliance across sectors."(Nigeria Data Protection Commission, 2025). For further reference, see Appendix L. Whereas Ghanaian organisations such as *One Million Coders* offer data protection courses, for users to become certified data protection officers (One Million Coders, 2025), as seen in Appendix M for further reference.

However, both these programs are clearly more targeted for individuals working within organisations, or those seeking to up-skill for improved employment opportunities, and not for the average user residing in these countries. Without targeted public-facing campaigns or civic engagement strategies, individuals are left ill-equipped to exercise their rights (Solano et al., 2022) under NDPA or GDPA, but may also be unaware that such rights exist.

Consequently, this knowledge gap further weakens the societal pressure necessary to hold digital platforms and website operators accountable (Gawer and Srnicek, 2021). In growing environments where legal enforcement and public digital literacy is low, the compounding effect may be the quiet erosion of data protection rights in an individual's daily life.

6.6 Platform Accountability and Global Influence

One of the most striking patterns emerging in the data from this study is the disproportionate non-compliance of globally recognised technology firms operating in West Africa. Popular websites such as Meta (Facebook, Instagram, Whatsapp), Amazon, ByteDance (TikTok), X (formerly Twitter), and Youtube have repeatedly failed to meet the basic legislative standards by failing to offer lawful consent notices or delay cookie placement until valid user consent was obtained. These same organisations, however, display different behaviour in the European Union, by offering granular cookie controls, and meaningful opt-out mechanisms to EU-based users, to comply with the GDPR.

This double standard underscores a reality in which data governance is a tiered regime of compliance, in which platform behaviour varies depending on the jurisdiction it is in, rather than the universal adherence to global standards (Helberger, Pierson and Poell, 2017). While it is clear these firms can comply with frameworks like the GDPR, they appear to minimise their compliance efforts in jurisdictions perceived to have weaker regulatory oversight or enforcement capacity. (Greenleaf, 2021; (Bygrave, 2017).

This issue thus is not merely one of neglect but of material inequality. In the absence of credible sanctions, multinationals are able to operate below legal standards, exploiting the gaps in legal capacity across jurisdictions to optimise their surveillance and monetisation practices (Kwet, 2019).

Moreover, the failure of dominant global platforms to respect local laws sends an accepted message: that West African regulatory regimes can be ignored without consequence. As a result, this not only erodes the legitimacy of national data protection frameworks but also weakens public trust in the enforceability of digital individual rights. For laws such as the NDPA or GDPA to have a tremendous effect, they must be backed not just by national ambition but by the necessary political will and international support that compel compliance regardless of user location (Spirkl, 2024).

6.7 Limitations of the Study

Although this study adopted a systematic and replicable approach to assess the level of cookie compliance across high-traffic websites in Nigeria and Ghana, it is important to not overlook but consider careful consideration.

Firstly, using the Brave browser with Shields 'ON' was great for simulating a privacy-focused user experience, but it might have skewed the visibility results a bit. Brave's privacy features, such as the cookie banner blocking by default feature, may have unintentionally suppressed parts of the cookie interface that would otherwise have been observable under standard browsing conditions. As a result, some sites that were marked as non-compliant might actually have compliant banners that were just obscured by the browser. While this setup offered valuable insights into how users experience privacy in real-world settings, it might not have fully captured the actual rates of banner deployment.

Secondly, the ten-minute observation window for each website visited, while consistent throughout the tests, has its own time-related limitations. Some websites might delay cookie deployments using asynchronous scripts, slow loading pages, or consent-based triggers. It leaves room for the potentiality of other cookies set after the observation period were missed. As a result, it could potentially lead to an underestimation of the full tracking activities, particularly for websites with complex loading or background processes.

A third limitation of this study is its dependence on geolocation simulation through a VPN, to replicate user access from Nigerian and Ghanaian IP addresses (specifically Lagos and Accra). While this method is useful for mimicking user access from Nigerian and Ghanaian IP addresses, it may fail to capture the full range of real-world access conditions citizens of these nations may face. This includes factors such as localised content delivery, ISP-specific scripting, or the mobile-first interfaces that are often seen in African digital environments. Consequently, behaviours related to banners or cookie placements that are more optimised for mobile browsers or particular ISPs might not have been fully visible in the controlled desktop-based environment.

Furthermore, the reliance on VPNs meant that the study of smaller countries i.e Sierra Leone and Cameroon, could not be done due to the lack of servers in those regions. Future work can include these regions, but it remains dependent on the VPNs server list.

Additionally, this research placed an emphasis on client-side tracking technologies, mainly through browser-based cookie storage and banner visibility. It did not employ deep-packet inspection (DPI), server-side analysis, or network-level monitoring. Due to this, increasingly advanced tracking methods (fingerprinting, cookie syncing, or cross-domain script injection) were not part of the study. This creates a blind spot regarding the full extent of unlawful data processing that might be occurring beyond observable cookie behaviours.

Finally, the research was cross-sectional, meaning that each website was examined and tested at a particular point in time. However, compliance behaviours may change due to external, unpredictable factors including: site updates; A/B testing; or shifts in regulatory

awareness. For the future, a more longitudinal design could provide a clearer, more accurate result of trends in cookie compliance over time.

Chapter 7: Conclusions & Future Work

This dissertation aimed to evaluate the real-world implementation of cookie consent practices and compliance levels across two major West African countries, Nigeria and Ghana, within the context of their respective data protection frameworks and international standards like the GDPR. By testing 100 high-traffic websites through three browser configurations (Brave shields 'ON', Brave shields 'OFF', and Google Chrome), this research provided a large-scale comparative audit of compliance in the region.

The results presented a clear and worrying pattern, in which the vast majority of websites failed to meet even the minimum legal requirements for valid user consent. The experiment revealed that over 90% of the tested websites in Nigeria, and over 80% in Ghana, deployed tracking technologies on the browser prior to obtaining informed or explicit user consent. These failures were persistent across all three browser configurations, though the protective features of Brave with shields 'ON' did reduce observable cookie volumes.

While Nigeria and Ghana have taken steps to adopt and incorporate GDPR-inspired frameworks, the data demonstrates that a profound gap between legislation and implementation does exist. In both countries, users are often exposed to intrusive tracking without meaningful options for refusal, and the corresponding regulatory authorities lack the technical and institutional ability to effectively enforce compliance. This issue was especially severe with foreign platforms that often applied significantly lower compliance standards for West African users.

From a methodological standpoint, this study also highlighted the importance and role of browser environments as a variable to be considered in compliance research. Brave, Google Chrome, and other browsers offer different privacy experiences for their users, and thus legal standards may want to evolve to acknowledge this complexity. In addition, the study identified a concerning lack of user awareness and digital literacy that limited the practical enforcement of data rights, even where legal protections exist.

7.2 Directions for Future Work

Future work should prioritise a number of key extensions. Geographical expansion should be considered, as incorporating additional West African nations such as Sierra Leone, Cameroon, and Senegal can be achieved through more direct local collaboration to bypass VPN restrictions. Additionally, given the dominance of mobile browsing in West Africa (Porter et al., 2012), subsequent studies should aim to examine cookie and potential SDK tracking within mobile browsers and apps, using real devices or through an emulation tool.

Nevertheless, further exploration of the cookies set can be achieved by server-side and deep packet-inspection. Integrating and utilising tools such as Wireshark would enable deeper

inspection into potential encrypted and non-visible tracking behaviours that were not reflected or found in the browser developer tools.

7.3 Final Reflections

This dissertation contributes to a growing field of empirical studies that explores and investigates the realities of digital rights of users in West Africa. Its findings demonstrate a fundamental imbalance between legal frameworks and practical reality, accelerated by various unique challenges such as regional enforcement gaps, low user awareness and global platform indifference. Until these issues are addressed, digital protections on paper will only continue to be undermined, leading to a situation in which consent becomes performative, rather than meaningful.

Bibliography

Abebe, R., Aruleba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S.L. and Sadagopan, S. (2021). Narratives and Counternarratives on Data Sharing in Africa. *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. doi:https://doi.org/10.1145/3442188.3445897.

Ajala, O.A., Arinze, C.A., Ofodile, O.C., Okoye, C.C. and Daraojimba, O.D. (2024). Reviewing advancements in privacy-enhancing technologies for big data analytics in an era of increased surveillance. *World Journal of Advanced Engineering Technology and Sciences*, [online] 11(1), pp.294–300. doi:https://doi.org/10.30574/wjaets.2024.11.1.0060.

AliExpress (2018). *AliExpress - Affordable Chinese Stores & Free Shipping - Online Shopping*. [online] AliExpress. Available at: https://www.aliexpress.com/ [Accessed 8 Sep. 2025].

Aloamaka, P.C. (2023). *View of DATA PROTECTION AND PRIVACY CHALLENGES IN NIGERIA: LESSONS FROM OTHER JURISDICTIONS*. [online] Ucc.edu.gh. Available at: https://journal.ucc.edu.gh/index.php/ucclj/article/view/1259/640 [Accessed 29 Apr. 2025].

Amasah, E., Odoi, R.N. and Arthur, E. (2022). *Reasonable Expectations of Privacy in the Digital Age: To What Extent Does Ghanaian Law Protect Individuals' Expectations in Cyberspace?* [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225869.

Anuku, W. (2025). *Multichoice Nigeria fined over N766m for violating NDP Act*. [online] Daily Post Nigeria. Available at: https://dailypost.ng/2025/07/06/multichoice-nigeria-fined-over-n766m-for-violating-ndp-act/ [Accessed 6 Sep. 2025].

Aseri, A.M. (2020). The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy. *Journal of Theoretical and Applied Information*, [online] 98(04), p.4. Available at: https://www.researchgate.net/profile/Abdulah-Aseri/publication/344243565_The_Implication_of_the_European_Union.

Ausloos, J. (2018). *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society?* (Dissertation presented in partial fulfilment of the requirements for the degree of Doctor in Laws, KU Leuven Faculty of Law).

Baako, I., Umar, S. and Gidisu, P. (2019). Privacy and Security Concerns in Electronic Commerce Websites in Ghana: A Survey Study. *International Journal of Computer Network and Information Security*, [online] 11(10), pp.19–25. doi:https://doi.org/10.5815/ijcnis.2019.10.03.

Bassey, M., Etefia, V. and Ebong, V. (2024). ECONOMIC COMMUNITY OF WEST AFRICAN STATES (ECOWAS) AND SUB-REGIONAL INTEGRATION IN WEST AFRICA. *European Journal of Political Science Studies*, [online] 7(2). Available at: https://oapub.org/soc/index.php/EJPSS/article/view/1772/2345 [Accessed 7 Sep. 2025].

BBC. (2025). *BBC - Home*. [online] Available at: https://www.bbc.co.uk/ [Accessed 8 Sep. 2025].

Bollinger, D. (2021). ETH Library Analyzing Cookies Compliance with the GDPR. [online] doi:https://doi.org/10.3929/ethz-b-000477333.

Boraine, A. and Doris, N.L. (2019). *The Fight against Cybercrime in Cameroon*. [online] *International Journal of Computer*. Available at: https://core.ac.uk/download/pdf/270221593.pdf.

Borberg, I.M., Hougaard, R., Rafnsson, W. and Kulyk, O. (2022). 'So I Sold My Soul': Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions. *Proceedings 2022 Symposium on Usable Security*. doi:https://doi.org/10.14722/usec.2022.23026.

Brave Software (2022). *Blocking annoying and privacy-harming cookie consent banners*. [online] Brave. Available at: https://brave.com/privacy-updates/21-blocking-cookie-notices/ [Accessed 28 Aug. 2025].

Brkan, M. (2019). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, [online] 20(6), pp.864–883. doi:https://doi.org/10.1017/glj.2019.66.

Broersma, M. (2024). *Nigeria Fines Meta $220m Over Privacy Infringements*. [online] Silicon UK. Available at: https://www.silicon.co.uk/e-regulation/legal/nigeria-whatsapp-meta-privacy-fine-572313 [Accessed 6 Sep. 2025].

Bryant, J. (2021). *Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights*. [online] Available at: https://law.stanford.edu/wp-content/uploads/2021/05/BryantAfricaInTheInformationAge.pdf.

Bygrave, L.A. (2017). Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements. *Oslo Law Review*, [online] 4(2), pp.105–120. doi:https://doi.org/10.18261/issn.2387-3299-2017-02-03.

Cahn, A., Alfeld, S., Barford, P. and Muthukrishnan, S. (2016). An Empirical Study of Web Cookies. *Proceedings of the 25th International Conference on World Wide Web - WWW '16*. [online] doi:https://doi.org/10.1145/2872427.2882991.

Camillus Eboh (2025). *Nigerian agency fines Multichoice 766 million naira for data privacy breaches*. [online] Reuters. Available at: https://www.reuters.com/sustainability/boards-policy-regulation/nigerian-agency-fines-multichoice-766-million-naira-data-privacy-breaches-2025-07-07/ [Accessed 6 Sep. 2025].

Cetin, M.B. (2024). *Evaluating the Effects of Digital Privacy Regulations on User Trust*. [online] arXiv.org. Available at: https://arxiv.org/abs/2409.02614 [Accessed 29 Apr. 2025].

Cha, S.-C., Hsu, T.-Y., Xiang, Y. and Yeh, K.-H. (2019). Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal*, [online] 6(2), pp.2159–2187. doi:https://doi.org/10.1109/jiot.2018.2878658.

ChatGPT (2025). *ChatGPT*. [online] ChatGPT. Available at: https://chatgpt.com/ [Accessed 8 Sep. 2025].

Chester, J. (2012). Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the 'Big Data' Era. *Springer eBooks*, [online] pp.53–77. doi:https://doi.org/10.1007/978-94-007-2903-2_4.

Data Protection Act (2012). *Data Protection Act, 2012 Section ARRANGEMENT OF SECTIONS Data Protection Commission*. [online] Available at: https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf.

Data Protection Africa (2022). *Cameroon | Fact Sheet | Data Protection Africa*. [online] Data Protection Africa | ALT Advisory. Available at: https://dataprotection.africa/cameroon/ [Accessed 29 Apr. 2025].

Data Protection Africa (2022). *Sierra Leone Fact Sheet | Data Protection Africa*. [online] Data Protection Africa | ALT Advisory. Available at: https://dataprotection.africa/sierra-leone/#:~:text=DPA legislation%3A Sierra Leone currently,processed by telecommunications network operators.&text=Personal data is not defined [Accessed 29 Apr. 2025].

Data Protection Africa (2023). *Nigeria | Data Protection Fact Sheet*. [online] Data Protection Africa | ALT Advisory. Available at: https://dataprotection.africa/nigeria/ [Accessed 29 Apr. 2025].

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T. (2019). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *Proceedings 2019 Network and Distributed System Security Symposium*. [online] doi:https://doi.org/10.14722/ndss.2019.23378.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T. (2019). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *arXiv (Cornell University)*. [online] doi:https://doi.org/10.14722/ndss.2019.23378.

Economic Community of West African States (2010). *THIRTY-SEVENTH SESSION OF THE AUTHORITY OF HEADS OF STATE AND GOVERNMENT*. [online] Available at: https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf.

Ekpo, O., Okokon, A. and Akpakpan, M. (2024). Data protection in the digital age: A comparative analysis of Nigeria's NDPA and the EU's GDPR. *Proceedings of the 13th International Conference on Information & Communication Technologies and Development*, pp.48–56. doi:https://doi.org/10.1145/3700794.3700799.

EUR-Lex (2002). *Directive - 2002/58 - EN - eprivacy directive - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng [Accessed 7 Sep. 2025].

EUR-Lex (2016). *L_2016119EN.01000101.xml*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1807-1-1 [Accessed 7 Sep. 2025].

Europa.eu. (2019). *CURIA - Documents*. [online] Available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=6E44D9829D2D3D40E1DB8E3FED571250?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8196213 [Accessed 27 Aug. 2025].

European Commission. (2024). *Data protection explained*. [online] Available at: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en#how-is-personal-data-protected [Accessed 26 Aug. 2025].

European Commission. (2024). *What data can we process and under which conditions?* [online] Available at: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/principles-gdpr/overview-principles/what-data-can-we-process-and-under-which-conditions_en [Accessed 26 Aug. 2025].

European Commission. (2024). *When is consent valid?* [online] Available at: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en [Accessed 7 Sep. 2025].

European Data Protection Board (2019). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | European Data Protection Board*. [online] Europa.eu. Available at: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en [Accessed 28 Aug. 2025].

European Data Protection Supervisor. (2025). *E*. [online] Available at: https://www.edps.europa.eu/data-protection/data-protection/glossary/e_en#e-privacy_directive2009-136-ec [Accessed 27 Aug. 2025].

Federal Republic of Nigeria Official Gazette (2023). *Federal Republic of Nigeria Official Gazette*. [online] Available at: https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf.

Flashscore (2025). *Flashscore.com.ng: Live Football Scores, Livescore - EPL, La Liga, Champions League*. [online] Flashscore.com.ng. Available at: https://www.flashscore.com.ng/ [Accessed 8 Sep. 2025].

Foe-Ahorney, S. (2024). Does the Law Protect the Privacy of Ghanaians on the Internet? An Exploratory Study. *ResearchGate*, [online] pp.111–124. doi:https://doi.org/10.1515/9783110797909-008.

Gawer, A. and Srnicek, N. (2021). *Online Platforms: Economic and Societal Effects*. [online] King's College London. Available at: https://kclpure.kcl.ac.uk/portal/en/publications/online-platforms-economic-and-societal-effects [Accessed 7 Sep. 2025].

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, [online] 59(6), pp.703–705. doi:https://doi.org/10.2501/ijmr-2017-050.

Government of Sierra Leone (2006) *The Telecommunications Act, 2006 (Act No. 9 of 2006)*. Freetown: Government Printing Department. Available at: https://www.sierra-leone.org/Laws/2006-9s.pdf

Government of Sierra Leone (2013) *The Right to Access Information Act, 2013*. Freetown: Government Printing Department. Available at: https://www.sierra-leone.org/Laws/2013-02.pdf

Grattet, R. and Jenness, V. (2008). Transforming Symbolic Law into Organizational Action: Hate Crime Policy and Law Enforcement Practice. *Social Forces*, 87(1), pp.501–527. doi:https://doi.org/10.1353/sof.0.0122.

Greenleaf, G. (2021). *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348 [Accessed 6 Aug. 2025].

Ha, V., Inkpen, K., Al Shaar, F. and Hdeib, L. (2006). An examination of user perception and misconception of internet cookies. *CHI '06 Extended Abstracts on Human Factors in Computing Systems*, [online] pp.833–838. doi:https://doi.org/10.1145/1125451.1125615.

Hackfort, S. (2021). Patterns of Inequalities in Digital Agriculture: A Systematic Literature Review. *Sustainability*, [online] 13(22), pp.12345–12345. doi:https://doi.org/10.3390/su132212345.

Harding, W.T., Reed, A.J. and Gray, R.L. (2001). Cookies and Web Bugs: What They are and How They Work Together. *Information Systems Management*, 18(3), pp.17–24. doi:https://doi.org/10.1201/1078/43196.18.3.20010601/31286.3.

Harper, S., Mehrnezhad, M. and Leach, M. (2023). Security and privacy of pet technologies: actual risks vs user perception. *Frontiers in the Internet of Things*, [online] 2. doi:https://doi.org/10.3389/friot.2023.1281464.

Helberger, N., Pierson, J. and Poell, T. (2017). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, [online] 34(1), pp.1–14. doi:https://doi.org/10.1080/01972243.2017.1391913.

InfoCuria Case-law (2019). *CURIA - Documents*. [online] Europa.eu. Available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=6E44D9829D2D3D40E1DB8E3FED571250?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8196213 [Accessed 27 Aug. 2025].

Izuogu, C.E. (2019). Mitigating Privacy Risks of Cookie-Fried Web-Surfers in Nigeria. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.3877428.

Jeffries, R. (1993). The state, structural adjustment and good government in Africa. *The Journal of Commonwealth & Comparative Politics*, 31(1), pp.20–35. doi:https://doi.org/10.1080/14662049308447646.

Jumia (2025). *Jumia Nigeria | Online Shopping for Electronics, Fashion, Home, Beauty & Sport*. [online] Jumia Nigeria. Available at: https://www.jumia.com.ng/ [Accessed 8 Sep. 2025].

Kanu, J.S., Vandi, M.A., Bangura, B., Draper, K., Gorina, Y., Foster, M.A., Harding, J.D., Ikoona, E.N., Amara Jambai, Mohamed, Kaitibi, D., Moffett, D.B., Singh, T. and Redd, J.T. (2024). Promoting Awareness of Data Confidentiality and Security During the COVID-19 Pandemic in a Low-Income Country—Sierra Leone. *Public health reviews*, [online] 45. doi:https://doi.org/10.3389/phrs.2024.1607540.

Koch, R. (2019). *Cookies, the GDPR, and the ePrivacy Directive - GDPR.eu*. [online] GDPR.eu. Available at: https://gdpr.eu/cookies/ [Accessed 29 Apr. 2025].

Kretschmer, M., Pennekamp, J. and Wehrle, K. (2021). Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Transactions on the Web*, 15(4), pp.1–42. doi:https://doi.org/10.1145/3466722.

Kretschmer, M., Pennekamp, J. and Wehrle, K. (2021). Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Transactions on the Web*, [online] 15(4), pp.1–42. doi:https://doi.org/10.1145/3466722.

Kuaban, G.S., Nkemeni, V., Nwobodo, O.J., Czekalski, P. and Mieyeville, F. (2024). Internet of Things Adoption in Technology Ecosystems within the Central African Region: The Case of Silicon Mountain. *Future Internet*, [online] 16(10), pp.376–376. doi:https://doi.org/10.3390/fi16100376.

Kulyk, O., Hilt, A., Gerber, N. and Volkamer, M. (2018). 'This Website Uses Cookies': Users' Perceptions and Reactions to the Cookie Disclaimer. *Proceedings 3rd European Workshop on Usable Security*. [online] doi:https://doi.org/10.14722/eurousec.2018.23012.

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, [online] 60(4), pp.3–26. doi:https://doi.org/10.1177/0306396818823172.

Lewis, P.M. (1996). Economic Reform and Political Transition in Africa The Quest for a Politics of Development. *World Politics*, [online] 49(1), pp.92–129. doi:https://doi.org/10.1353/wp.1996.0021.

Linden, T., Khandelwal, R., Harkous, H. and Fawaz, K. (2020). The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(1), pp.47–64. doi:https://doi.org/10.2478/popets-2020-0004.

Lukman Adebisi Abdulrauf (2020). Giving 'teeth' to the African Union towards advancing compliance with data privacy norms. *Information & Communications Technology Law*, [online] 30(2), pp.87–107. doi:https://doi.org/10.1080/13600834.2021.1849953.

Machuletz, D. and Böhme, R. (2020). Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, [online] 2020(2), pp.481–498. doi:https://doi.org/10.2478/popets-2020-0037.

Matte, C., Bielova, N. and Santos, C. (2019). *Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*. [online] arXiv.org. Available at: https://arxiv.org/abs/1911.09964 [Accessed 29 Apr. 2025].

Mehrnezhad, M. (2020). A Cross-Platform Evaluation of Privacy Notices and Tracking Practices. [online] pp.97–106. doi:https://doi.org/10.1109/eurospw51379.2020.00023.

Miyazaki, A.D. (2008). Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *Journal of Public Policy & Marketing*, [online] 27(1), pp.19–33. doi:https://doi.org/10.1509/jppm.27.1.19.

MSN (2025). *MSN*. [online] Msn.com. Available at: https://www.msn.com/en-gb [Accessed 8 Sep. 2025].

Nigeria Data Protection Commission (2025). *NDPC -International Journal of Data Privacy and Protection i*. [online] Available at: https://www.aluko-oyebode.com/wp-content/uploads/2025/02/NDPC-International-Journal-of-Data-Privacy-and-Protection.pdf.

Nigeria Data Protection Commission (2025). *Virtual Privacy Academy – Nigeria Data Protection Commission*. [online] Ndpc.gov.ng. Available at: https://ndpc.gov.ng/virtual-privacy-academy/ [Accessed 8 Sep. 2025].

Nigeria Data Protection Commission (2025). *Virtual Privacy Academy – Nigeria Data Protection Commission*. [online] Ndpc.gov.ng. Available at: https://ndpc.gov.ng/virtual-privacy-academy/ [Accessed 6 Sep. 2025].

NiTDA (2019). *NIGERIA DATA PROTECTION REGULATION 2019*. [online] Available at: https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf.

Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *arXiv (Cornell University)*, [online] pp.1–13. doi:https://doi.org/10.1145/3313831.3376321.

Nwaeze, A.C., Zavarsky, P. and Ruhl, R. (2017). Compliance evaluation of information privacy protection in e-government systems in Anglophone West Africa using ISO/IEC 29100:2011. *2017 Twelfth International Conference on Digital Information Management (ICDIM)*. [online] doi:https://doi.org/10.1109/icdim.2017.8244644.

Nwosu, C. (2022). Should One Accept the Cookies? Exploring the Privacy Concerns in Digital Advertising in Nigeria. *SSRN Electronic Journal*. [online] doi:https://doi.org/10.2139/ssrn.4262747.

Ochinanwata, C., Igwe, P.A. and Radicic, D. (2023). The institutional impact on the digital platform ecosystem and innovation. *International Journal of Entrepreneurial Behavior & Research*, [online] 30(2/3), pp.687–708. doi:https://doi.org/10.1108/ijebr-01-2023-0015.

One Million Coders (2025). *Data Protection Course Details*. [online] Onemillioncoders.gov.gh. Available at: https://onemillioncoders.gov.gh/certified-dpf-course [Accessed 8 Sep. 2025].

One Million Coders (2025). *Data Protection Course Details*. [online] Onemillioncoders.gov.gh. Available at: https://onemillioncoders.gov.gh/certified-dpf-course [Accessed 6 Sep. 2025].

One Million Coders (2025). *One Million Coders - Ghana*. [online] Onemillioncoders.gov.gh. Available at: https://onemillioncoders.gov.gh/ [Accessed 8 Sep. 2025].

Orji, U.J. (2017). Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act. *International Data Privacy Law*, [online] 7(3), pp.179–189. doi:https://doi.org/10.1093/idpl/ipx013.

Pornhub.com (2019). *Free Porn Videos & Sex Movies - Porno, XXX, Porn Tube | Pornhub*. [online] Pornhub.com. Available at: https://www.pornhub.com/.

Porter, G., Hampshire, K., Abane, A., Munthali, A., Robson, E., Mashiri, M. and Tanle, A. (2012). Youth, mobility and mobile phones in Africa: findings from a three-country study. *Information Technology for Development*, [online] 18(2), pp.145–162. doi:https://doi.org/10.1080/02681102.2011.643210.

Prinsloo, P. and Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology*, [online] 53(4), pp.894–913. doi:https://doi.org/10.1111/bjet.13226.

Reddit (2005). *Reddit*. [online] Reddit. Available at: https://www.reddit.com/.

Semrush (2025). *Most Visited Websites in Nigeria 2025 | Trending Websites*. [online] Semrush. Available at: https://www.semrush.com/trending-websites/ng/all [Accessed 8 Sep. 2025].

SOAX. (2025). *Browser market share: The most popular browsers of 2024*. [online] Soax.com. Available at: https://soax.com/research/browser-market-share [Accessed 7 Sep. 2025].

Solano, J.L., Martin, A., Ohai, F., Souza, S. de and Taylor, L. (2022). Digital disruption or crisis capitalism?: Technology, power and the pandemic. *Tilburg University Research Portal*. [online] doi:https://doi.org/10.26116/gdj-euaifund.

Spirkl, C. (2024). Data Laws Around the Globe – Insights, Frictions and Opportunities. Highlights from the African Data Protection Laws Conference in Accra, Ghana, 13-15 September 2022 and Comparative Data Law Conference in Munich, Germany, 7-8 December 2023. *GRUR International*, [online] 73(9), pp.865–871. doi:https://doi.org/10.1093/grurint/ikae093.

Statista (2025). *Total population Ghana 2030| Statista*. [online] Statista. Available at: https://www.statista.com/statistics/447474/total-population-of-ghana/#statisticContainer [Accessed 8 Sep. 2025].

Strycharz, J., Smit, E., Natali Helberger and Guda van Noort (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior*, [online] 120, pp.106750–106750. doi:https://doi.org/10.1016/j.chb.2021.106750.

Svärd, P. (2016). Freedom of information laws and information access. *Information Development*, [online] 33(2), pp.190–198. doi:https://doi.org/10.1177/0266666916642829.

Tchao, E., Diawuo, K.-G., Aggor, C. and Kotey, S. (2017). Ghanaian Consumers" Online Privacy Concerns: Causes and its Effects on E-Commerce Adoption. *IJACSA) International Journal of Advanced Computer Science and Applications*, [online] 8(11). Available at: https://arxiv.org/pdf/1801.01086.

temu (2022). *Temu United Kingdom | Explore the Latest Clothing, Beauty, Home, Jewelry & More*. [online] temu. Available at: https://www.temu.com/ [Accessed 8 Sep. 2025].

Trusov, M., Ma, L. and Jamal, Z. (2016). Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting on JSTOR. *Jstor.org*. [online] doi:https://doi.org/10.2307/44012162.

Turner, E.C. and Dasgupta, S. (2003). Privacy on the Web: an Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. *Information Systems Management*, 20(1), pp.8–18. doi:https://doi.org/10.1201/1078/43203.20.1.20031201/40079.2.

Ul Haque, E., Khan, M.M.H. and Fahim, M.A.A. (2023). The Nuanced Nature of Trust and Privacy Control Adoption in the Context of Google. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, [online] pp.1–23. doi:https://doi.org/10.1145/3544548.3581387.

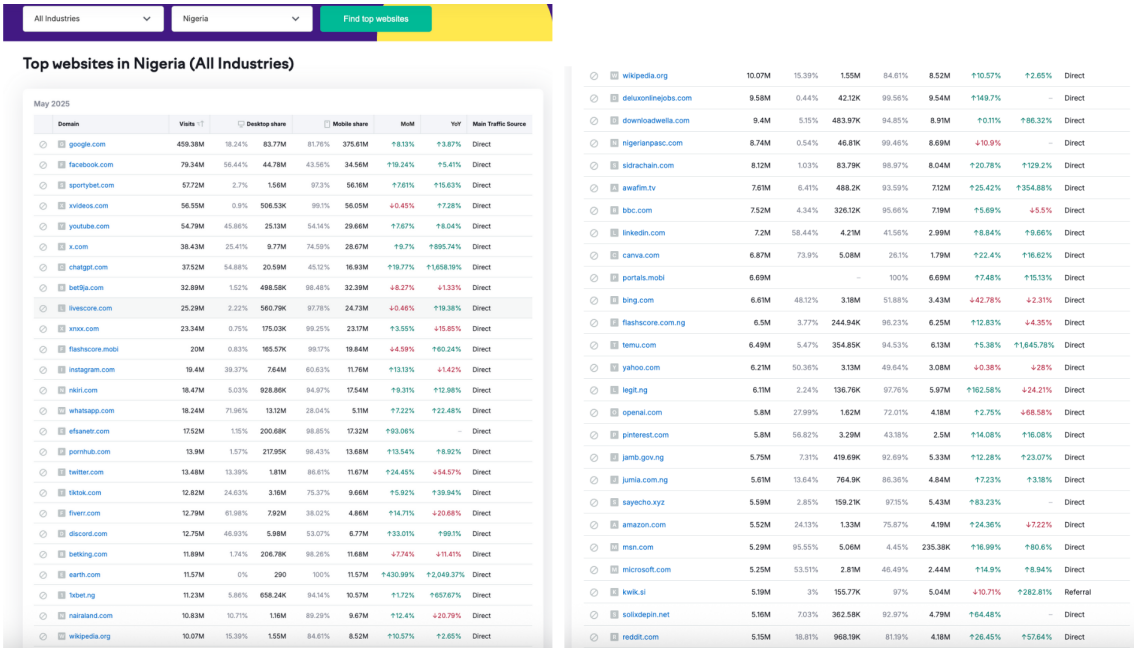
Utz, C., Degeling, M., Fahl, S., Schaub, F. and Holz, T. (2019). (Un)informed Consent. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, [online] pp.973–990. doi:https://doi.org/10.1145/3319535.3354212.

Virtual Privacy Academy (2025). *Welcome Back !* [online] Virtualprivacyacademy.ng. Available at: https://learn.virtualprivacyacademy.ng/ [Accessed 8 Sep. 2025].

World Bank Group (2021). *World Bank Open Data*. [online] World Bank Open Data. Available at: https://data.worldbank.org/country/nigeria [Accessed 8 Sep. 2025].

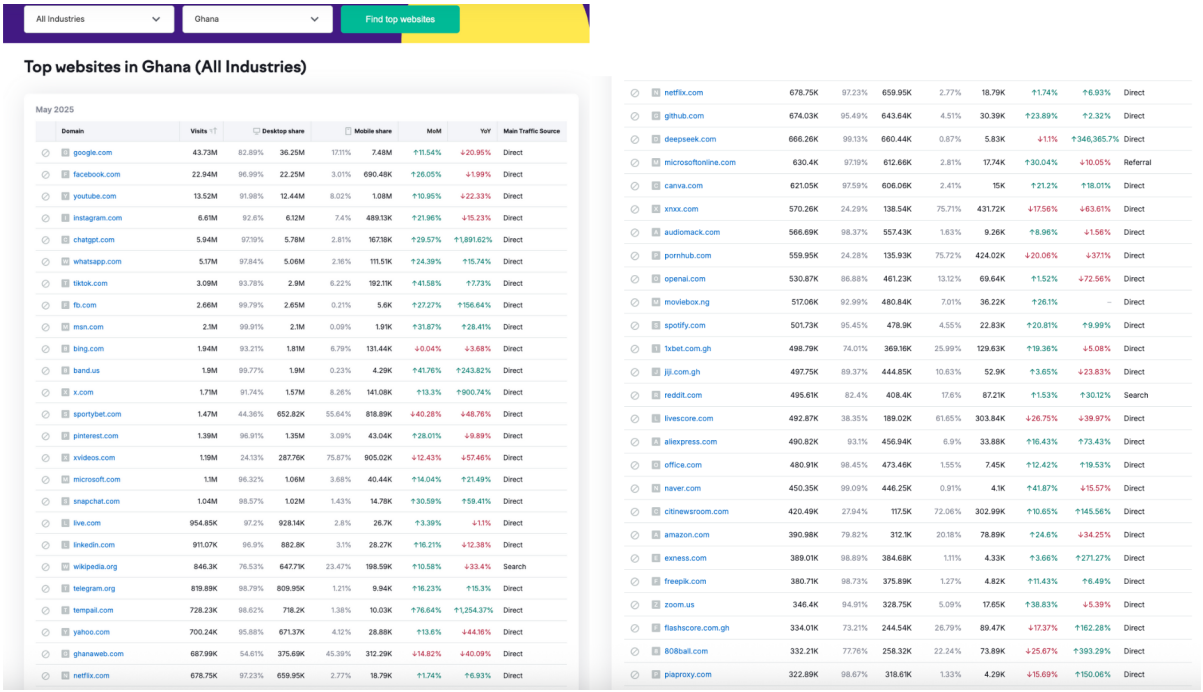
Appendices

Appendix A: Top 50 websites in Nigeria
Screenshot from Semrush (2025), captured by author

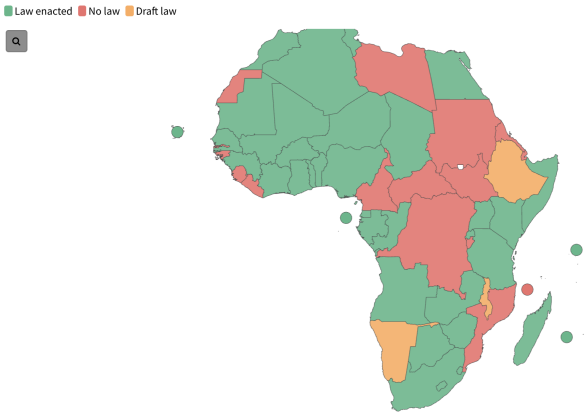


	Domain	Visits	Desktop share		Mobile share		MoM	YoY	Main Traffic Source
	google.com	459.38M	18.24%	83.77M	81.76%	375.61M	↑8.13%	↑3.87%	Direct
	facebook.com	79.34M	56.44%	44.78M	43.56%	34.56M	↑19.24%	↑5.41%	Direct
	sportybet.com	57.72M	2.7%	1.56M	97.3%	56.16M	↑7.61%	↑15.63%	Direct
	xvideos.com	56.55M	0.9%	506.53K	99.1%	56.05M	↓0.45%	↑7.28%	Direct
	youtube.com	54.79M	45.86%	25.13M	54.14%	29.66M	↑7.67%	↑8.04%	Direct
	x.com	38.43M	25.41%	9.77M	74.59%	28.67M	↑9.7%	↑895.74%	Direct
	chatgpt.com	37.52M	54.88%	20.59M	45.12%	16.93M	↑19.77%	↑1,658.19%	Direct
	bet9ja.com	32.89M	1.52%	498.58K	98.48%	32.39M	↓8.27%	↓1.33%	Direct
	livescore.com	25.29M	2.22%	560.79K	97.78%	24.73M	↓0.46%	↑19.38%	Direct
	xnxx.com	23.34M	0.75%	175.03K	99.25%	23.17M	↑3.55%	↓15.85%	Direct
	flashscore.mobi	20M	0.83%	165.57K	99.17%	19.84M	↓4.59%	↑60.24%	Direct
	instagram.com	19.4M	39.37%	7.64M	60.63%	11.76M	↑13.13%	↓1.42%	Direct
	nkiri.com	18.47M	5.03%	928.86K	94.97%	17.54M	↑9.31%	↑12.98%	Direct
	whatsapp.com	18.24M	71.96%	13.12M	28.04%	5.11M	↑7.22%	↑22.48%	Direct
	efsanetr.com	17.52M	1.15%	200.68K	98.85%	17.32M	↑93.06%	–	Direct
	pornhub.com	13.9M	1.57%	217.95K	98.43%	13.68M	↑13.54%	↑8.92%	Direct
	twitter.com	13.48M	13.39%	1.81M	86.61%	11.67M	↑24.45%	↓54.57%	Direct
	tiktok.com	12.82M	24.63%	3.16M	75.37%	9.66M	↑5.92%	↑39.94%	Direct
	fiverr.com	12.79M	61.98%	7.92M	38.02%	4.86M	↑14.71%	↓20.68%	Direct
	discord.com	12.75M	46.93%	5.98M	53.07%	6.77M	↑33.01%	↑99.1%	Direct
	betking.com	11.89M	1.74%	206.78K	98.26%	11.68M	↓7.74%	↓11.41%	Direct
	earth.com	11.57M	0%	290	100%	11.57M	↑430.99%	↑2,049.37%	Direct
	1xbet.ng	11.23M	5.86%	658.24K	94.14%	10.57M	↑1.72%	↑657.67%	Direct
	nairaland.com	10.83M	10.71%	1.16M	89.29%	9.67M	↑12.4%	↓20.79%	Direct
	wikipedia.org	10.07M	15.39%	1.55M	84.61%	8.52M	↑10.57%	↑2.65%	Direct
	deluxonlinejobs.com	9.58M	0.44%	42.12K	99.56%	9.54M	↑149.7%	–	Direct
	downloadwella.com	9.4M	5.15%	483.97K	94.85%	8.91M	↑0.11%	↑86.32%	Direct
	nigerianpasc.com	8.74M	0.54%	46.81K	99.46%	8.69M	↓10.9%	–	Direct
	sidrachain.com	8.12M	1.03%	83.79K	98.97%	8.04M	↑20.78%	↑129.2%	Direct
	awafim.tv	7.61M	6.41%	488.2K	93.59%	7.12M	↑25.42%	↑354.88%	Direct
	bbc.com	7.52M	4.34%	326.12K	95.66%	7.19M	↑5.69%	↓5.5%	Direct
	linkedin.com	7.2M	58.44%	4.21M	41.56%	2.99M	↑8.84%	↑9.66%	Direct
	canva.com	6.87M	73.9%	5.08M	26.1%	1.79M	↑22.4%	↑16.62%	Direct
	portals.mobi	6.69M		–	100%	6.69M	↑7.48%	↑15.13%	Direct
	bing.com	6.61M	48.12%	3.18M	51.88%	3.43M	↓42.78%	↓2.31%	Direct
	flashscore.com.ng	6.5M	3.77%	244.94K	96.23%	6.25M	↑12.83%	↓4.35%	Direct
	temu.com	6.49M	5.47%	354.85K	94.53%	6.13M	↑5.38%	↑1,645.78%	Direct
	yahoo.com	6.21M	50.36%	3.13M	49.64%	3.08M	↓0.38%	↓28%	Direct
	legit.ng	6.11M	2.24%	136.76K	97.76%	5.97M	↑162.58%	↓24.21%	Direct
	openai.com	5.8M	27.99%	1.62M	72.01%	4.18M	↑2.75%	↓68.58%	Direct
	pinterest.com	5.8M	56.82%	3.29M	43.18%	2.5M	↑14.08%	↑16.08%	Direct
	jamb.gov.ng	5.75M	7.31%	419.69K	92.69%	5.33M	↑12.28%	↑23.07%	Direct
	jumia.com.ng	5.61M	13.64%	764.9K	86.36%	4.84M	↑7.23%	↑3.18%	Direct
	sayecho.xyz	5.59M	2.85%	159.21K	97.15%	5.43M	↑83.23%	–	Direct
	amazon.com	5.52M	24.13%	1.33M	75.87%	4.19M	↑24.36%	↓7.22%	Direct
	msn.com	5.29M	95.55%	5.06M	4.45%	235.38K	↑16.99%	↑80.6%	Direct
	microsoft.com	5.25M	53.51%	2.81M	46.49%	2.44M	↑14.9%	↑8.94%	Direct
	kwik.si	5.19M	3%	155.77K	97%	5.04M	↓10.71%	↑282.81%	Referral
	solixdepin.net	5.16M	7.03%	362.58K	92.97%	4.79M	↑64.48%	–	Direct
	reddit.com	5.15M	18.81%	968.19K	81.19%	4.18M	↑26.45%	↑57.64%	Direct

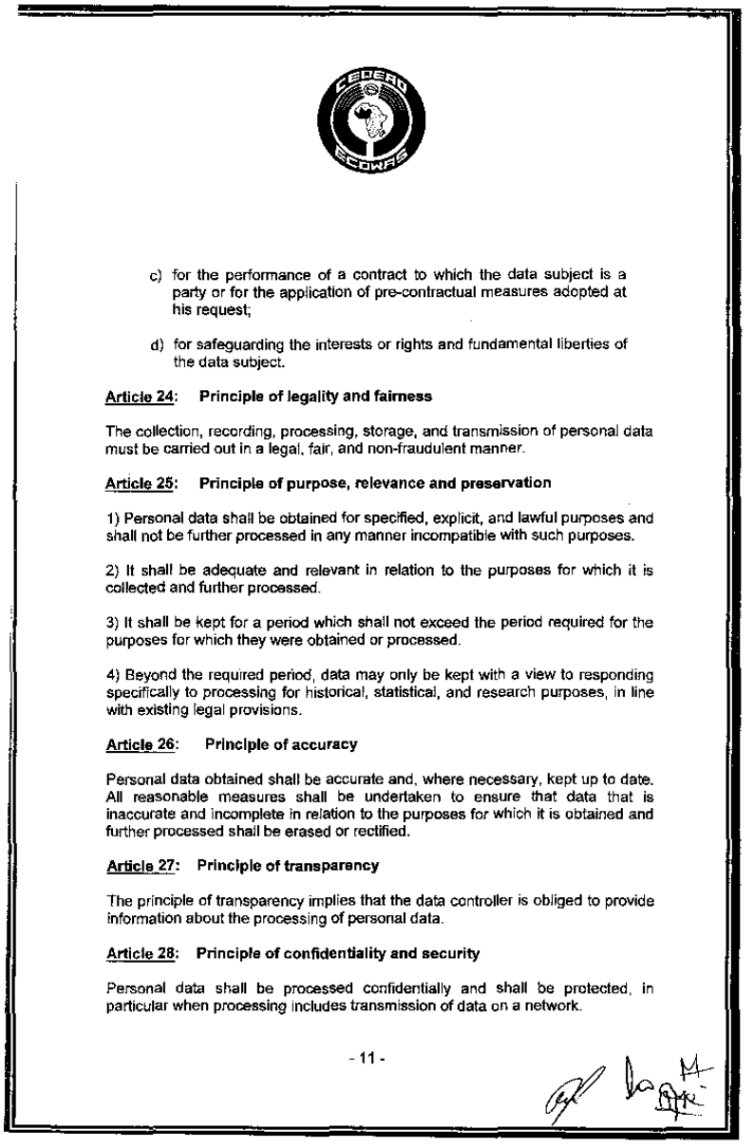
Appendix B: Top 50 websites in Ghana
Screenshot from Semrush (2025), captured by author



Appendix C: Data Protection Africa's Map of African countries have legislation in green or no legislation in red.
Screenshot from Data Protection Africa (2024), captured by author



Appendix D: ECOWAS Supplementary Act with similar subject rights to the GDPR.
Screenshot from Economic Community of West African States (2010), captured by author



c) for the performance of a contract to which the data subject is a party or for the application of pre-contractual measures adopted at his request;

d) for safeguarding the interests or rights and fundamental liberties of the data subject.

Article 24: Principle of legality and fairness

The collection, recording, processing, storage, and transmission of personal data must be carried out in a legal, fair, and non-fraudulent manner.

Article 25: Principle of purpose, relevance and preservation

1) Personal data shall be obtained for specified, explicit, and lawful purposes and shall not be further processed in any manner incompatible with such purposes.

2) It shall be adequate and relevant in relation to the purposes for which it is collected and further processed.

3) It shall be kept for a period which shall not exceed the period required for the purposes for which they were obtained or processed.

4) Beyond the required period, data may only be kept with a view to responding specifically to processing for historical, statistical, and research purposes, in line with existing legal provisions.

Article 26: Principle of accuracy

Personal data obtained shall be accurate and, where necessary, kept up to date. All reasonable measures shall be undertaken to ensure that data that is inaccurate and incomplete in relation to the purposes for which it is obtained and further processed shall be erased or rectified.

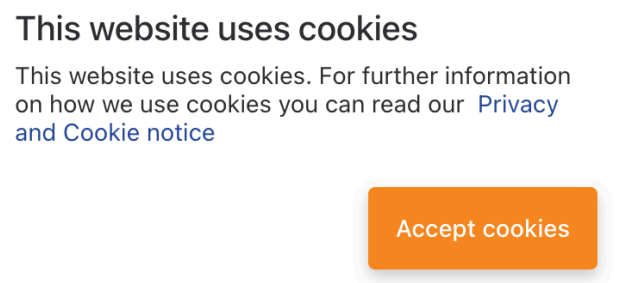
Article 27: Principle of transparency

The principle of transparency implies that the data controller is obliged to provide information about the processing of personal data.

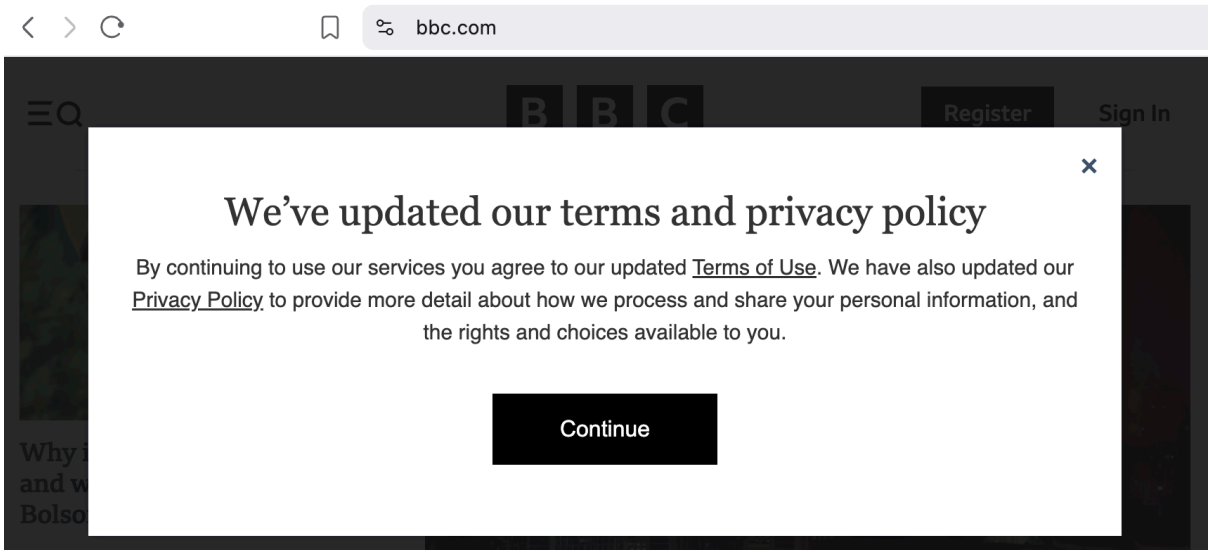
Article 28: Principle of confidentiality and security

Personal data shall be processed confidentially and shall be protected, in particular when processing includes transmission of data on a network.

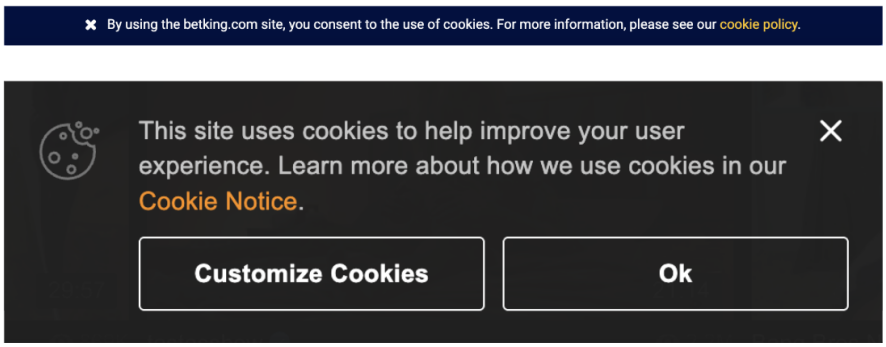
Appendix E: *Example of 'Accept' only Dark Pattern Used*
*Screenshot from jumia.com.ng (*2025*) captured by author*



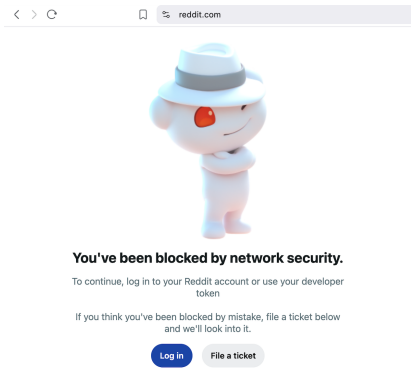
Appendix F: bbc.com's Privacy Pop-Up Notice
*Screenshot from bbc.com (*2025*) captured by author*



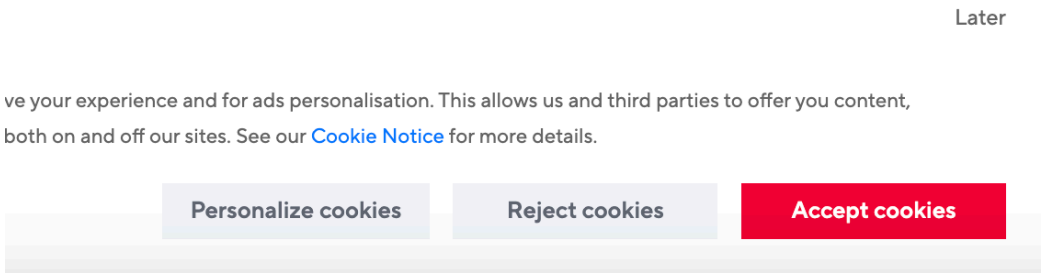
Appendix G: Examples of Implied Consent from Continued Use of the Website
*Screenshot from betking.com (*2025*) and Pornhub.com (2019) captured by author*



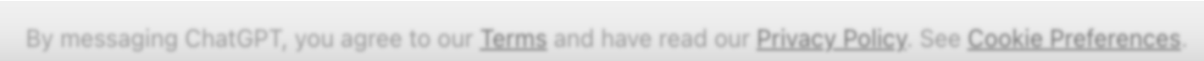
Appendix H: Inaccessible Reddit.com due to being blocked by local ISP or Network Security
*Screenshot from reddit.com (*2005*) captured by author*



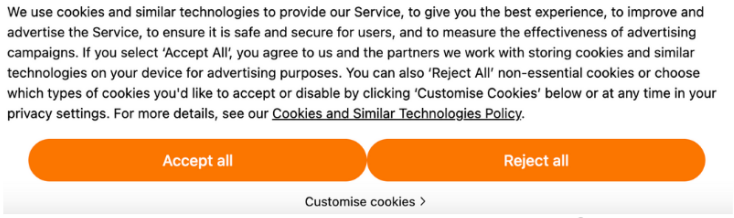
Appendix I: Example of Colour Manipulation on ‘Reject’ Button
Screenshot from AliExpress.com (2018) captured by author



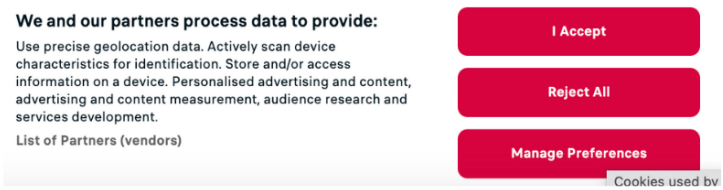
Appendix J: Example of ChatGPT.com’s Implied Consent
Screenshot from chatgpt.com (2025) captured by author



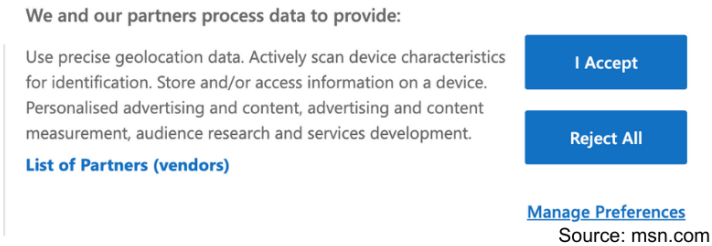
Appendix K: Example of Balanced Interfaces provided by temu.com, flashscore.com.ng and msn.com
Screenshots from temu.com (2022), flashscore.com.ng (2025), and msn.com (2025) captured by author



Source: temu.com



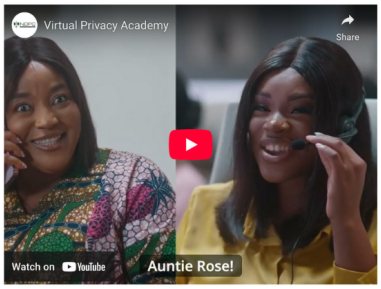
Source: flashscore.com.ng



Source: msn.com

Appendix L: Nigeria's Virtual Privacy Academy

Screenshots from Nigeria Data Protection Commission (2025) and Virtual Private Academy (2025) captured by author

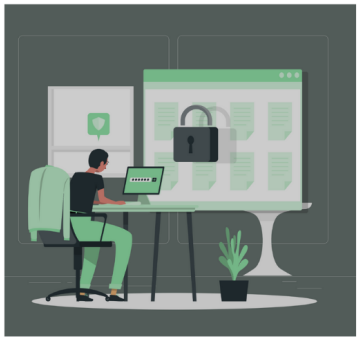


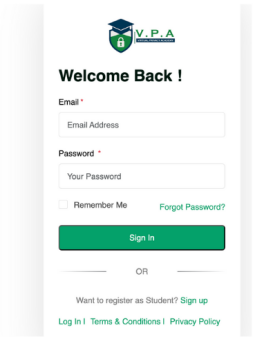
// capacity-building at NDPC

VIRTUAL PRIVACY ACADEMY

As part of our continued commitment to deepening data protection awareness and capacity-building, we're proud to introduce the **Virtual Privacy Academy**.

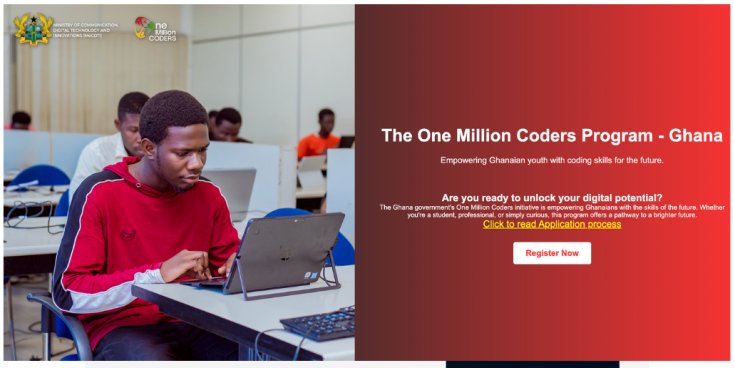
This innovative virtual learning platform, accessible at **https://learn.virtualprivacyacademy.ng**, is designed to bring data protection to life. The academy goes beyond theory by weaving real-life scenarios into compelling, relatable stories that illustrate the impact and importance of data protection in everyday life. It's a dynamic tool that empowers learners at all levels to understand and apply data privacy principles in practical ways, fostering a culture of responsibility and compliance across sectors.

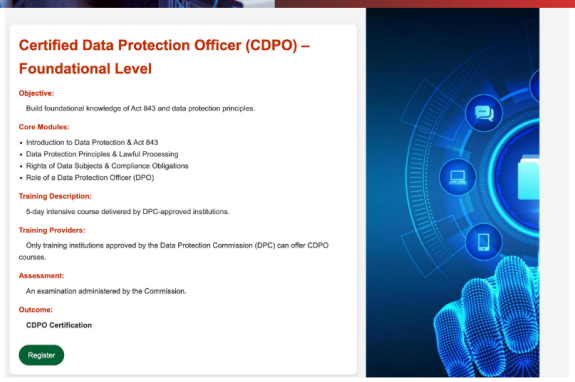




Appendix M: Data Protection Course Offered by One Million Coders

Screenshots from One Million Coders (2025) and One Million Coders (2025) captured by author





Certified Data Protection Officer (CDPO) – Foundational Level

Objective:

Build foundational knowledge of Act 843 and data protection principles.

Core Modules:

- Introduction to Data Protection & Act 843
- Data Protection Principles & Lawful Processing
- Rights of Data Subjects & Compliance Obligations
- Role of a Data Protection Officer (DPO)

Training Description:

5-day intensive course delivered by DPC-approved institutions.

Training Providers:

Only training institutions approved by the Data Protection Commission (DPC) can offer CDPO courses.

Assessment:

An examination administered by the Commission.

Outcome:

CDPO Certification

Register