

Privacy Versus Personalization: Evaluating the Ethical Implications of Artificial Intelligence Chatbots in Nigerian Academic Libraries

Gilbert Paul Igboechesi (CLN)
Librarian, University of Jos, Nigeria

Thomas Akinbayo Adigun (PhD)
University Librarian, University of Uyo, Nigeria

doi: <https://doi.org/10.37745/ijliss.15/vol12n2117>

Published May 31, 2026

Citation: Igboechesi G.P. and Adigun T.A. (2026) Privacy Versus Personalization: Evaluating the Ethical Implications of Artificial Intelligence Chatbots in Nigerian Academic Libraries, *International Journal of Library and Information Science Studies*, 12(2),1-17

Abstract: *The growing integration of artificial intelligence (AI) chatbots into Nigerian academic libraries raises pressing questions about the balance between data-driven personalization and the protection of user privacy. This paper examines, through secondary sources, the ethical tensions generated when AI tools collect behavioural data from library users in a context where formal governance frameworks are largely absent. A gap analysis of privacy policies across Nigerian academic libraries reveals that existing frameworks are inadequate for regulating AI-specific data practices. Drawing on Privacy-by-Design principles, Nigerian data protection legislation, and international library ethics standards, the paper proposes a context-sensitive model for ethical AI deployment in Nigerian academic libraries. The study contends that personalization and privacy are not inherently incompatible, but that deliberate institutional design and transparent data governance are necessary conditions for reconciling them.*

Keywords: AI chatbots, academic libraries, Nigeria, data privacy, personalization, Privacy-by-Design, library ethics, data governance, intellectual freedom

INTRODUCTION

The rapid integration of artificial intelligence (AI) technologies into academic library services represents one of the most consequential transformations in the history of library and information science (LIS). Across institutions in the Global South, including Nigerian universities, AI-powered chatbots are increasingly deployed to support reference services, answer patron queries, and navigate large digital collections on behalf of users. These technologies carry significant promise:

they extend service availability beyond staffed hours, reduce research friction, and offer the prospect of personalized information support tailored to individual academic needs. At the same time, the data architectures that make AI personalization possible are built on the continuous collection, storage, and analysis of user behavioural data, a practice that sits in fundamental tension with the long-established privacy values of the library profession. Whether Nigerian academic libraries can harness the service benefits of AI chatbots without compromising their foundational commitment to patron confidentiality and intellectual freedom remains an open and urgent question. Understanding this tension requires examining both the technical architecture of AI systems and the normative frameworks that govern library practice in the Nigerian context. The sections that follow explore this problem through a review of existing scholarship, a gap analysis of current policy frameworks, and a proposed model for ethical AI governance in Nigerian academic libraries.

The concept of patron privacy has occupied a central place in library ethics for well over a century. Professional bodies such as the International Federation of Library Associations and Institutions (IFLA), the American Library Association (ALA), and the Nigerian Library Association (NLA) have consistently affirmed that the records of what a person reads, borrows, or researches belong to that individual and must be shielded from disclosure. This commitment reflects a deeper principle: that libraries are spaces where intellectual inquiry can proceed without surveillance or the fear of judgment, and that this freedom is a precondition for genuine scholarship. Nissenbaum (2010) theorized this dimension of information privacy through the concept of contextual integrity, arguing that privacy is violated not merely when data is collected, but when information flows depart from the norms of the context in which they were originally shared. A library patron who submits a query to a reference librarian does so within a relationship of professional confidentiality; when that same query is processed by an AI system, logged in a commercial cloud database, and potentially fed back into model training, the contextual expectations of privacy are disrupted in ways that have not yet been fully reckoned with in library practice. The legal landscape in Nigeria adds a further dimension to this ethical question, as both the Nigeria Data Protection Regulation (NDPR) of 2019 and the Nigeria Data Protection Act (NDPA) of 2023 establish formal obligations concerning data collection, consent, and retention that apply directly to the AI tools libraries are beginning to adopt. The extent to which existing library privacy policies in Nigeria are adequate to these legal and ethical demands is, at best, uncertain.

AI personalization systems do not function passively. They require ongoing access to behavioural data: the queries a user submits, the resources they select, the paths they follow through digital collections, and the frequency and timing of their library visits (Bhatt & Bhatt, 2022). This data, aggregated over time, allows AI systems to model user preferences and research trajectories with increasing precision, enabling the kind of anticipatory recommendation and tailored response that constitutes the core value proposition of AI-enhanced library services. Zuboff (2019) described this phenomenon as the generation of "behavioural surplus," meaning the data produced as a byproduct of service use that is extracted, analysed, and deployed for predictive modelling, often

without the explicit awareness or meaningful consent of the individuals whose behaviour generated it. In a commercial context, behavioural surplus is the foundational resource of the digital economy; in the library context, it represents a form of surveillance that sits uneasily alongside the profession's historical commitment to non-disclosure. The practical challenge for Nigerian academic libraries is that many of the AI tools they are adopting are commercial platforms developed by vendors whose business models assume, if not depend upon, access to this behavioural data. Without deliberate contractual and policy intervention, the adoption of commercial AI in Nigerian libraries risks importing surveillance architectures that undermine the very values these institutions are mandated to uphold.

The existing body of scholarship on AI ethics in libraries has grown substantially in recent years, though the preponderance of this literature has been developed in North American and European contexts (Breeding, 2021; Fernandez, 2022; Lund & Wang, 2023). The Nigerian academic library environment, with its distinctive regulatory, infrastructural, and socioeconomic characteristics, has received comparatively little systematic attention, representing a gap that this paper aims to begin addressing. Research on digital library development in Nigeria has documented the considerable strides made by institutions such as the University of Lagos, the University of Ibadan, Ahmadu Bello University, and Obafemi Awolowo University in building digital infrastructure and expanding electronic resource access (Okuonghae & Adeniran, 2020). However, this literature has largely focused on questions of access, adoption, and capacity, rather than on the ethical governance dimensions of digital and AI-enhanced services. A separate strand of research on data privacy awareness among Nigerian library users (Bello & Ariola, 2021; Okonkwo, 2022) suggests that while students are generally receptive to digital services, their understanding of how AI systems collect and use their data is limited, a finding with significant implications for the design of consent and transparency mechanisms. Taken together, these bodies of literature indicate that the Nigerian academic library sector is at an early but critical stage in negotiating the relationship between technological adoption and ethical governance, a stage at which the choices made now will shape the information rights of Nigerian scholars for years to come. The paper proceeds by first establishing the relevant literature on AI personalization, library privacy, and Privacy-by-Design, it then examines the current status of AI adoption in Nigerian academic libraries and conducts a gap analysis of existing privacy policy frameworks, the ethical implications of AI chatbot deployment are then discussed in depth and a Privacy-by-Design model tailored to the Nigerian academic library context is proposed; how libraries can negotiate this tension, what governance tools are available, and what an ethical model for AI deployment might look like in the Nigerian context are the questions this paper attempted to address. It is within this layered landscape of professional ethics, legal obligation, and technological change that this paper situates its inquiry.

Navigating the Ethics of Privacy and the Mechanisms of AI Personalization in Academic Libraries

The deployment of AI tools in academic libraries has been driven by a convergence of technological capability and institutional aspiration. Chatbot-based reference services, increasingly powered by large language models (LLMs) such as OpenAI's GPT series, have been positioned as scalable solutions to the challenge of providing high-quality reference support to large student populations with limited professional staffing (Bhatt & Bhatt, 2022). These systems promise round-the-clock service availability, rapid response to high query volumes, and, over time, the capacity to learn from prior interactions and surface resources that align with individual users' research interests. Lund and Wang (2023) examined the early implications of ChatGPT for academic libraries and found that while the technology demonstrated considerable potential for reference and instruction support, it also raised substantial questions about accuracy, bias, and the appropriate boundaries of AI autonomy in scholarly contexts. The personalization capabilities of AI library systems operate across several distinct dimensions: at the transactional level, chatbots learn from query history to refine the relevance of subsequent responses; at the behavioural level, AI systems can analyse users' navigation patterns within digital collections to model their research interests and proactively recommend resources; at the ambient level, IoT sensors can aggregate data about physical space usage to optimize service delivery and resource allocation. Each of these dimensions generates data, and the accumulation of data across all three produces a behavioural profile of individual library users that is both detailed and potentially sensitive. The implications of this profiling for patron privacy, intellectual freedom, and institutional trust are the central concern of this paper. Understanding how other scholars and professional bodies have theorized these implications provides the conceptual foundation for the analysis that follows.

Library privacy is not merely a procedural requirement; it is a foundational ethical commitment grounded in the relationship between information access and intellectual freedom. IFLA (2015) affirmed in its Internet Manifesto that the privacy of library users must be respected and that libraries have a responsibility to protect the personal data of the individuals they serve. The ALA (2019) has similarly asserted that privacy is essential to the exercise of free speech, free thought, and free association, and that library records are among the most sensitive categories of personal information precisely because they reveal the intellectual interests and inquiries of individuals who have sought information in a context of professional confidentiality. These international principles are directly relevant to Nigerian libraries, both because the NLA has subscribed to broadly similar professional norms and because Nigeria's own data protection legislation, specifically the NDPR issued by the National Information Technology Development Agency (NITDA) in 2019 and the NDPA enacted in 2023, establishes legal obligations regarding data collection, consent, and retention that apply to the AI tools libraries are beginning to deploy. The NDPR mandates that data collection be grounded in identified legal bases, that data subjects be informed of the purposes for which their data is collected, and that data not be retained beyond the period necessary for those purposes; the NDPA further strengthened this framework by establishing the Nigeria Data Protection Commission (NDPC) as an enforcement authority with investigative and sanctioning

powers. The translation of these legal obligations into library practice, however, remains largely incomplete: Nigerian academic libraries have not, as a matter of routine, conducted data protection impact assessments, appointed data protection officers, or developed AI-specific privacy policies that address the data practices of chatbot reference systems. This governance gap constitutes the central problem to which this paper responds. The theoretical frameworks available for analysing and addressing this gap are examined in the subsections that follow.

Contextual Integrity and the Privacy-Personalization Tension

Nissenbaum's (2010) theory of contextual integrity provides one of the most analytically powerful frameworks for understanding why AI personalization poses a distinctive challenge to library privacy, beyond what can be captured by simple notions of data disclosure or breach. The theory holds that privacy norms are context-specific: information flows appropriately when they conform to the norms governing the context in which information was originally shared, and inappropriately when they violate those norms, regardless of whether any formal legal threshold has been crossed. In the library context, a patron who poses a reference question to a librarian does so within a relationship governed by norms of professional confidentiality; those norms constitute the contextual expectations of the interaction. When the same query is processed by an AI system, retained in a commercial cloud database, and potentially used to train future model iterations, the contextual integrity of the original interaction is disrupted, even if no statute has been violated and even if the user has formally consented to terms of service that authorize these uses. This theoretical insight helps explain why the conventional informed consent model may be insufficient as a primary mechanism for protecting library user privacy in the AI context: consent to data collection does not restore contextual integrity if the flows generated by AI systems remain inconsistent with the normative expectations of library service. Acquisti, Brandimarte, and Loewenstein (2016) further complicated the consent framework by documenting what they termed the privacy paradox, the empirically robust finding that individuals who express strong preferences for privacy in the abstract routinely make choices that prioritize convenience over privacy protection in practice, particularly when privacy costs are diffuse and delayed while personalization benefits are immediate and salient. In the library context, this paradox suggests that students may readily engage with AI chatbot services whose data practices they would theoretically find objectionable if those practices were fully transparent, not because they do not value privacy but because the cognitive and practical barriers to exercising privacy-protective choices are high. Designing governance frameworks that protect privacy without requiring users to bear these cognitive and practical burdens is therefore a critical challenge for library AI ethics. The feminist and critical information studies literature offers additional analytical resources for this project, as examined next.

Noble (2018) and Eubanks (2018) have demonstrated through detailed empirical research that AI systems are not neutral technologies: they encode the assumptions, biases, and power relations embedded in their training data and design choices, and they reproduce those biases in their outputs in ways that systematically disadvantage already-marginalized groups. Noble (2018) documented

how commercial search engines have historically returned results that reinforce racial stereotypes and cultural hierarchies, while Eubanks (2018) showed how algorithmic decision-making systems deployed in social services contexts have imposed disproportionate burdens on economically disadvantaged populations. These findings have direct relevance to the Nigerian academic library context, where AI chatbot systems trained predominantly on English-language Western academic sources may systematically underserve students researching African intellectual traditions, indigenous knowledge systems, or Nigeria-specific policy and governance questions. The equity implications of this representational gap are significant: if AI personalization systems deliver demonstrably inferior service quality to students working within African scholarly frameworks, they reproduce and potentially entrench existing hierarchies within the academy, undermining the library's equity mandate. Gender disparities in digital technology access and use, which remain pronounced in Nigerian universities, add a further dimension to this equity concern (Adeyemi & Taiwo, 2023). These critical perspectives suggest that an adequate ethics framework for AI in Nigerian academic libraries must attend not only to individual privacy rights but also to the structural dimensions of AI-related harm, including representational exclusion and differential service quality. With these theoretical resources established, the next subsection turns to the Privacy-by-Design framework, which provides the normative and practical foundation for the governance model proposed in this paper.

Origin of Privacy-by-Design and Library Applications

Privacy-by-Design (PbD), a framework originally developed by Cavoukian (2009) during her tenure as Information and Privacy Commissioner of Ontario, proposes that privacy protections should be embedded into the design of information systems from the outset, rather than appended as compliance measures after systems are built and deployed. The framework comprises seven foundational principles: proactive rather than reactive privacy protection; privacy as the default system setting; privacy embedded into system design; full functionality through positive-sum rather than zero-sum design; end-to-end security across the full lifecycle of data; visibility and transparency for all stakeholders; and respect for user privacy through user-centric design choices. The normative attraction of PbD for the library AI context lies in its rejection of the notion that privacy and functionality are necessarily in tension: properly designed systems, Cavoukian (2009) argued, can deliver their intended service benefits while simultaneously minimizing privacy risks, provided that privacy is treated as a design requirement rather than an afterthought. Applications of PbD principles to library technology contexts have been explored in the literature, with Fernandez (2022) proposing a PbD implementation framework for academic libraries that emphasized data minimization, algorithmic transparency, and user control, and Breeding (2021) identifying PbD-aligned practices in library technology procurement and vendor management. However, both of these contributions were developed for North American library environments, and their applicability to the Nigerian context is constrained by the significant differences in regulatory framework, technological infrastructure, institutional capacity, and socioeconomic context. The need for a contextually adapted PbD framework for Nigerian academic libraries, one that accounts for the specific governance challenges, resource constraints, and user characteristics

of this environment, is the animating concern of the latter sections of this paper. Before that model is presented, however, it is necessary to examine the current state of AI adoption in Nigerian academic libraries and to conduct a systematic gap analysis of existing privacy policy frameworks, as undertaken in the following section.

Status of AI Adoption in Nigerian Academic Libraries Context

Nigerian academic libraries occupy an ambiguous position in the landscape of global library AI adoption. They are sufficiently resourced in some leading federal universities to experiment with digital and AI-enhanced services, yet they operate under infrastructural, financial, and policy constraints that significantly complicate sustained and responsible technology adoption. The National Universities Commission (NUC) has progressively integrated digital resource development into its accreditation standards, creating institutional incentives for universities to invest in electronic databases, digital cataloguing systems, and increasingly, AI-enhanced reference services. Institutions including the University of Lagos, the University of Ibadan, Ahmadu Bello University, and Obafemi Awolowo University have made notable investments in digital library infrastructure, though the depth and consistency of implementation vary considerably across and within these institutions (Okuonghae & Adeniran, 2020). The COVID-19 pandemic served as a significant accelerant for digital library service adoption, compelling many Nigerian academic libraries to expand virtual reference capabilities rapidly and, in some instances, to experiment with chatbot-mediated reference services built on commercial AI platforms, often without systematic evaluation of the data governance implications of those platforms. The pandemic-driven urgency of digital service expansion compressed the deliberative processes that would ordinarily precede major technology adoption decisions, leaving data governance considerations subordinate to service continuity imperatives. At the time of this analysis, the majority of Nigerian academic libraries that have deployed or piloted AI chatbot services have done so through third-party commercial platforms rather than through bespoke institutional development, a pattern that introduces opacity into data governance arrangements since the data handling practices of commercial providers may not be fully visible to or controllable by the library institution. The governance implications of this reliance on commercial AI are examined in detail in the gap analysis that follows.

Gap Analysis of Existing Privacy Policy Frameworks

A review of publicly available privacy policies and institutional guidelines from a sample of Nigerian academic libraries reveals significant deficiencies in the capacity of existing frameworks to address the data governance demands of AI tools. The review examined policy documents from fifteen federal and state university libraries, assessing them against ten AI-relevant data governance criteria derived from the Nigeria Data Protection Regulation (NDPR), the Nigeria Data Protection Act (NDPA), and International Federation of Library Associations and Institutions' (IFLA) Data Protection Principles for Library Management Systems (IFLA, 2021). None of the fifteen institutions reviewed maintained a dedicated AI ethics policy for library services, and only three possessed any form of data protection policy that addressed digital and electronic service

data as distinct from physical circulation records; of these three, none had been updated since 2021 and none contained provisions relevant to the specific data practices of AI systems, including automated user profiling, third-party data sharing, or cross-system behavioural data aggregation.

Institution	Category	AI-Specific Consent	Data Minimisation	Retention Schedules	Algorithmic Accountability	Cross-Border Safeguards	DPIA Process	Data Protection Officer	User Rights (Access/Delete)	Vendor DPA Requirement	AI Ethics Policy
University of Lagos	Federal	X	X	X	X	X	X	X	X	X	X
University of Ibadan	Federal	X	X	X	X	X	X	X	X	X	X
Ahmadu Bello University	Federal	X	X	✓	X	X	X	X	✓	X	X
Obafemi Awolowo University	Federal	X	X	X	X	X	X	X	X	X	X
University of Nigeria, Nsukka	Federal	X	X	✓	X	X	X	X	X	X	X
University of Benin	Federal	X	X	X	X	X	X	X	X	X	X
University of Port Harcourt	Federal	X	X	X	X	X	X	X	X	X	X
Bayero University, Kano	Federal	X	X	X	X	X	X	X	X	X	X
Lagos State University	State	X	X	✓	X	X	X	X	✓	X	X
Ekiti State University	State	X	X	X	X	X	X	X	X	X	X
Rivers State University	State	X	X	X	X	X	X	X	X	X	X
Enugu State University of Sci. & Tech.	State	X	X	X	X	X	X	X	X	X	X
Abia State University	State	X	X	X	X	X	X	X	X	X	X
Kaduna State University	State	X	X	X	X	X	X	X	X	X	X
Imo State University	State	X	X	X	X	X	X	X	X	X	X
Total Libraries Meeting Criterion		0/15	0/15	3/15	0/15	0/15	0/15	0/15	2/15	0/15	0/15

Table 1 above presents a systematic evaluation of privacy policy provisions across fifteen Nigerian academic libraries, comprising eight federal university libraries and seven state university libraries. Each institution was assessed against ten AI-relevant data governance criteria derived from the Nigeria Data Protection Regulation (NDPR, 2019), the Nigeria Data Protection Act (NDPA, 2023), and the International Federation of Library Associations and Institutions (IFLA) Data Protection Principles for Library Management Systems (2021).

NOTE: The symbol ✓ denotes that a relevant provision was identified in the institution's publicly available policy documentation; X denotes the absence of such a provision. Institutions are listed in alphabetical order within each category.

DPA = Data Processing Agreement; DPIA = Data Protection Impact Assessment. Policy documents reviewed are those publicly available as at January 2026. The absence of a provision does not necessarily indicate non-compliance with the NDPR or NDPA; however, the absence of an explicit provision in publicly available documentation constitutes a governance transparency gap with material implications for patron trust and regulatory accountability. Source: Authors' gap analysis informed by NDPR (NITDA, 2019), NDPA (NDPC, 2023), and IFLA (2021).

Specific governance gaps identified through the analysis include the absence of AI-specific consent frameworks that adequately disclose the nature and extent of data collection by AI

reference tools, the lack of data minimization provisions requiring vendors to limit collection to what is strictly necessary for service delivery, the absence of specified data retention periods for AI-generated interaction logs, and the absence of any provisions for algorithmic accountability or audit of AI-generated recommendations for bias or accuracy (Adetimirin, 2021; Nwosu & Onyekachi, 2022). A further significant gap concerns cross-border data transfer: several commercial AI platforms used by Nigerian libraries process user data on servers located outside Nigeria, raising compliance questions under the NDPR's cross-border transfer provisions that existing library policies do not address. The root causes of these governance deficits are multiple, including resource constraints that limit policy development capacity, insufficient professional training in data governance among library staff, and the absence of sector-specific regulatory guidance from bodies such as the NLA or the Committee of University Librarians of Nigerian Universities (CULNU). These findings are consistent with broader evidence of a structural lag in sub-Saharan African academic libraries between technology adoption and governance framework development, a pattern documented by Nwosu and Onyekachi (2022) across multiple national contexts in the region. The user-side dimensions of this governance challenge, including awareness and attitudes among library patrons, are considered next.

User Awareness and Attitudes Toward AI and Privacy

An adequate understanding of the ethical landscape requires attention not only to institutional policy frameworks but also to the perspectives of library users whose data AI systems collect and whose intellectual freedom AI deployment may affect. Research on Nigerian university students' awareness of and attitudes toward AI data practices indicates that enthusiasm for digital library services coexists with limited understanding of how AI systems collect, store, and use behavioural data (Bello & Ariola, 2021). Many students engage with AI reference tools without awareness that their queries are retained in interaction logs, that their usage patterns may be analysed to generate behavioural profiles, or that their data may be shared with commercial third parties under the terms of service governing the platforms their libraries use. Okonkwo (2022) found that while students in federal universities in southeastern Nigeria expressed theoretical concern about data privacy, this concern rarely translated into privacy-protective behaviour in practice, a finding consistent with the privacy paradox documented by Acquisti et al. (2016) in other digital service contexts. Bello and Ariola (2021) similarly found that awareness of the data governance implications of AI-driven library services was substantially lower among students than awareness of the functional capabilities of those services, suggesting that information asymmetry between library institutions and their users is significant and consequential. The gender and socioeconomic dimensions of privacy attitudes in the Nigerian university context have been underexplored but are potentially significant: preliminary evidence reported by Adeyemi and Taiwo (2023) suggests that female students and students from lower socioeconomic backgrounds may exhibit greater risk-aversion concerning digital data sharing, reflecting broader patterns of vulnerability to data-enabled harm. These findings underscore the importance of designing AI governance frameworks that are responsive to the heterogeneous needs, awareness levels, and risk profiles of the diverse student populations that Nigerian academic libraries serve. With this understanding of the Nigerian context

established, the paper turns to a more detailed analysis of the specific ethical implications that AI chatbot deployment raises.

Ethical Implications of AI Chatbot Deployment in Nigerian Academic Libraries

Intellectual Freedom, Surveillance, and the Chilling Effect

One of the most consequential ethical risks associated with AI data collection in library contexts is the potential chilling effect on intellectual inquiry. The concept of the chilling effect, developed originally in First Amendment jurisprudence, describes the phenomenon in which awareness of surveillance deters individuals from engaging in lawful but sensitive expressive or associative activities, as researchers or inquirers self-censor their behavior to avoid scrutiny. Zimmer (2014) applied this framework to library contexts and found that patron awareness of data collection significantly reduces willingness to explore controversial, heterodox, or politically sensitive topics through library channels. In the Nigerian political environment, characterized by episodic restrictions on speech and expression, researchers working on sensitive issues such as governance, corruption, ethnic relations, or security sector reform may face meaningful risks if their research interests are exposed through inadequately governed AI data systems. An AI chatbot that retains detailed query logs indefinitely creates a potential vector for this kind of exposure, particularly where data security infrastructure is inadequate or where legal compulsion to disclose user data is possible under Nigeria's existing security legislation. Furthermore, AI chatbot interactions generate behavioural data that is qualitatively richer than traditional circulation records: they capture not only what a patron sought but how they articulated their informational need, what follow-up questions they pursued, and how they responded to different types of answers, producing a behavioural profile that is potentially far more revealing of a patron's intellectual interests and personal circumstances than any single circulation record. The implications of this richer surveillance capacity for intellectual freedom in Nigerian academic libraries have not yet been systematically examined in the library literature, making the chilling effect one of the most urgent research priorities identified by this analysis. The data security dimensions of this risk are considered in the next subsection.

Data Security Risks in Resource-Constrained Environments

The accumulation of sensitive patron behavioural data by AI systems in Nigerian academic libraries would be ethically concerning under any circumstances; it is especially so given the infrastructural constraints under which many of these libraries operate. Unreliable electricity supply, limited dedicated IT staffing, aging hardware, and budget pressures that compete with security investment are structural features of many Nigerian university library environments that create elevated vulnerability to data breaches and unauthorized data access. When AI systems aggregate behavioural profiles of library users on infrastructure that cannot be adequately secured, the risk that this data may be compromised, accessed by unauthorized parties, or retained beyond any legitimate service purpose is substantially elevated. The reliance on commercial AI platforms introduces additional data security considerations that are not always fully appreciated at the point

of procurement: third-party AI providers typically retain contractual rights to user interaction data for model training and service improvement purposes, and the data processing agreements governing these relationships are often written in technical legal language that library administrators are not trained to evaluate. This creates a fundamental opacity in data flows that is inconsistent with both the transparency principles of library ethics and the disclosure and consent requirements of the GDPR, and it places Nigerian academic libraries in the position of potentially facilitating data practices whose full scope and implications they cannot adequately assess or communicate to users. The equity dimensions of this situation, including the potential for AI systems to deliver differential service quality to different categories of users, are examined in the subsection that follows.

Algorithmic Bias and Equity in the Nigerian Academic Context

AI systems are not epistemically neutral: they reflect the assumptions, knowledge frameworks, and representational priorities embedded in their training data and the design choices made by their developers. Large language models such as those underpinning contemporary AI chatbot services are trained predominantly on English-language Western academic and popular sources, with the consequence that their capacity to respond effectively to queries in Nigerian languages, to engage with African scholarly traditions, or to surface Nigeria-specific academic resources is substantially less developed than their capacity within Anglophone Western academic frameworks (Noble, 2018). A postgraduate student in Nsukka researching the philosophical dimensions of Igbo oral traditions, or a student in Sokoto investigating indigenous governance systems in northern Nigeria, may receive qualitatively inferior AI-assisted reference support compared to a student pursuing a topic well-represented in the LLM's training corpus, not because their research questions are less rigorous but because the AI system's knowledge base is shaped by the representational priorities of its developers. These differential service outcomes reproduce and potentially entrench existing academic hierarchies that privilege certain knowledge traditions and research frameworks over others, undermining the library's mandate to provide equitable information access to all members of its community. Eubanks (2018) documented analogous equity effects in algorithmic systems deployed in social services contexts, finding that systems designed without explicit attention to the needs of marginalized populations systematically disadvantaged those populations in their operation. In Nigerian academic libraries, where gender disparities in digital technology access, ethnic and linguistic heterogeneity, and wide socioeconomic variation among students are all pronounced, the equity implications of algorithmically mediated service delivery are potentially significant. The dimensions of informed consent that intersect with these equity concerns are addressed next.

Informed Consent and User Autonomy

The principle of informed consent holds that individuals should freely agree, with full understanding, to uses of their personal information before that information is collected and processed. In the context of AI library service deployment, genuine informed consent would require that users understand what behavioural data is being collected through their interactions

with AI tools, for what purposes that data will be used, with whom it may be shared, for how long it will be retained, and how they can exercise rights of access, correction, and deletion. Acquisti et al. (2016) have demonstrated that even where consent mechanisms formally exist, they routinely fail to produce genuinely informed consent in digital service contexts, because the cognitive demands of processing complex terms of service documents exceed what most users can reasonably be expected to invest, and because the power asymmetry between service providers and users makes consent that is formally voluntary practically coerced when the alternative is forfeiting access to a service for which no adequate substitute exists. In Nigerian academic libraries, where the institutional library may represent a student's primary or sole access point to quality academic resources, this coercive dimension of consent is particularly acute: a student who must accept the data practices of an AI reference service as a condition of accessing library resources is not exercising free consent in any meaningful sense. The rights of data subjects established under the GDPR, including rights of access to their data, correction of inaccurate data, and deletion of data no longer necessary for its original purpose, are rarely implemented in practice in existing AI library deployments. Designing consent and data rights mechanisms that are genuinely meaningful for Nigerian library users, rather than formally compliant but practically inaccessible, is one of the central challenges addressed by the governance model proposed in the following section.

A Privacy-by-Design Model for Ethical AI Implementation in Nigerian Academic Libraries

Principles of the Proposed Model

The Privacy-by-Design model proposed in this paper adapts Cavoukian's (2009) foundational framework to the specific regulatory, infrastructural, and socioeconomic context of Nigerian academic libraries, organized around five core principles: ethical proactivity, data sovereignty, transparent intelligence, inclusive design, and institutional accountability. Ethical proactivity requires that libraries anticipate and address privacy risks before AI systems are deployed, rather than responding reactively to breaches or harms after they occur; this demands, at a minimum, that a Data Protection Impact Assessment (DPIA), as mandated by the GDPR for high-risk data processing activities, be completed prior to any AI procurement or deployment decision, with the assessment process designed to be participatory, engaging library staff, student representatives, faculty, and data protection professionals. Data sovereignty refers to the principle that library user data should remain subject to meaningful institutional and user control, rather than being appropriated by commercial AI vendors; in practice, this requires negotiating data processing agreements with vendors that prohibit the use of patron interaction data for commercial model training without explicit user consent, require data processing within Nigerian jurisdiction where technically feasible, and establish data minimization and automatic deletion provisions. Transparent intelligence demands that AI systems explain themselves to users, to library staff, and to institutional governance bodies: user-facing chatbot interfaces should provide plain-language disclosures of data practices at the point of engagement, users should be able to access a comprehensible summary of their own data, and libraries should conduct and publish regular

algorithmic audits assessing AI system outputs for accuracy, bias, and consistency with library values. Inclusive design requires that AI systems deployed in Nigerian academic libraries be engineered to serve the full linguistic, cultural, and socioeconomic diversity of the Nigerian academic community, with explicit attention to multilingual accessibility, the integration of African scholarly resources into AI reference corpora, and the differential vulnerability of particular user groups (Adeyemi & Taiwo, 2023). Institutional accountability requires ongoing organizational commitment to these principles through designated Library Data Protection Officers, user advisory committees with genuine participatory rights in AI governance, and transparent mechanisms for reporting privacy concerns and data breaches to both institutional leadership and the Nigeria Data Protection Commission. These five principles, taken together, constitute a framework that goes substantially beyond current practice in Nigerian academic libraries while remaining grounded in the regulatory and operational realities of the Nigerian context.

Implementation Roadmap

The implementation of the proposed PbD model is most productively understood as a phased institutional process requiring sustained commitment rather than a single policy adoption event. In the first phase, covering approximately the first six months of implementation, institutions should conduct a comprehensive baseline audit of all AI tools currently in use and the data flows they generate; complete Data Protection Impact Assessments for all existing and proposed AI deployments; develop or substantially revise privacy policies to incorporate AI-specific provisions aligned with the NDPR and NDPA; and appoint a Library Data Protection Officer equipped with sufficient organizational authority and resources to perform this role effectively. In the second phase, covering approximately months seven through eighteen, libraries should negotiate revised data processing agreements with AI vendors to incorporate data minimization, retention limitation, and prohibition of commercial data use provisions; develop and deploy user-facing transparency tools including privacy dashboards and comprehensible consent interfaces; establish ongoing algorithmic audit processes with published results; and create user advisory committees with meaningful participation in AI governance decisions. In the third phase, spanning approximately months nineteen through thirty-six, libraries should achieve full PbD compliance across all AI systems; publish annual transparency reports covering AI data practices, audit findings, and complaint resolution outcomes; engage with the NLA and CULNU to develop sector-wide AI ethics standards and share implementation learning; and contribute, through these professional bodies, to the development of sector-specific regulatory guidance by the Nigeria Data Protection Commission. Cross-institutional collaboration throughout all phases is strongly recommended, given that shared infrastructure development and collective policy learning can substantially reduce the resource demands of PbD implementation for individual libraries operating under budget constraints. The vendor selection and procurement considerations that support this implementation are addressed in the following subsection.

Vendor Selection and Procurement Considerations

The procurement process for AI library services is one of the most practically significant sites of privacy governance, because the data governance characteristics of an AI system are largely determined at the vendor selection stage rather than through post-deployment policy intervention. Libraries should develop AI procurement criteria that assign substantial weight to vendor data governance practices alongside functional service capabilities, treating data governance as a threshold requirement rather than a secondary consideration. Key vendor criteria should include demonstrated commitment to data minimization and explicit prohibition of commercial use of library patron data; provision of complete, auditable, and non-negotiable data processing agreements that meet NDPR and NDPA requirements; technical capability to support data portability, patron access to their own data, and deletion on request; full transparency about training data composition and model development processes; and demonstrated compliance with applicable data protection frameworks. The potential of open-source AI tools deserves serious consideration as an alternative to commercial platforms, since open-source systems offer greater institutional transparency and control over data processing, at the cost of greater demands on technical capacity and infrastructure. Consortia approaches, in which multiple Nigerian university libraries collaborate on shared AI infrastructure development and governance, may make the open-source option viable at scale while distributing the technical and financial burden across institutions; such arrangements would also create opportunities for developing AI reference corpora that better reflect the Nigerian and African scholarly resources most relevant to the user communities of Nigerian academic libraries. The discussion in the following section situates these recommendations within the broader context of the paper's findings and their implications for LIS practice and professional culture in Nigeria.

DISCUSSION

The analysis presented in this paper illuminates a governance crisis in Nigerian academic libraries that, while not unique to the Nigerian context, carries particular urgency given the scale of the sector and the specific vulnerabilities of Nigerian library users. As AI technologies are adopted at increasing pace, driven by digitization mandates, competitive pressures, and the demonstrated service benefits of AI personalization, the ethical and legal frameworks necessary to govern their data practices have not developed at a commensurate pace. The gap analysis of privacy policies across fifteen Nigerian academic libraries found not a single institution with a dedicated AI ethics policy for library services, and existing data protection provisions were consistently found to be inadequate for addressing the distinctive data practices of AI systems. This finding is consistent with the broader pattern documented by Nwosu and Onyekachi (2022) across sub-Saharan African academic library contexts and reflects structural conditions, including resource constraints, insufficient professional training in data governance, and the absence of sector-specific regulatory guidance, that will require coordinated responses at both institutional and sectoral levels. The Privacy-by-Design framework proposed in this paper represents one approach to closing this governance gap, but its successful implementation will depend critically on a parallel transformation in professional culture within Nigerian LIS: privacy must come to be understood

not as a compliance burden imposed from without but as a core professional value as fundamental to librarianship as intellectual freedom, equitable access, and service excellence, and this understanding must be reflected in LIS curricula, continuing professional development programs, and the institutional priorities of university librarians. The argument of this paper is emphatically not that AI personalization should be rejected by Nigerian academic libraries: the genuine service benefits of AI tools, expanded access, reduced research friction, extended service hours, and the potential to reach students who would not otherwise seek reference support, are real and significant, particularly in a context of constrained library staffing. The argument is, rather, that these benefits should not be purchased at the cost of patron privacy and intellectual freedom, and that the Privacy-by-Design model proposed here offers a practical pathway for realizing the service benefits of AI while preserving the ethical commitments that define the library profession.

Looking beyond individual institutional action, there is a compelling case for collective response among Nigerian academic libraries, professional associations, and regulatory bodies. The NLA and CULNU are positioned to play a significant coordinating role by developing sector-wide AI ethics standards, providing model policy frameworks that individual libraries can adapt, and advocating with the Nigeria Data Protection Commission for the development of sector-specific regulatory guidance for academic libraries. International partnerships with library associations in the Global North, facilitated through frameworks such as IFLA's global data protection advocacy program, offer opportunities to draw on established expertise while developing contextually appropriate solutions that reflect Nigerian legal frameworks, institutional realities, and user needs. The findings of this paper also point to a clear research agenda for the Nigerian LIS community: empirical measurement of the chilling effect associated with AI surveillance in Nigerian library contexts, evaluation of the implementation feasibility and effectiveness of PbD frameworks through pilot studies in partner institutions, and cross-national comparative research on AI ethics policy in academic libraries across sub-Saharan Africa would all contribute substantially to the evidence base available to practitioners and policymakers. The analysis presented here, grounded in secondary sources and policy document review, establishes the conceptual and empirical foundations for this future research while offering practical governance recommendations that libraries can begin acting upon within their current resource and regulatory environments. The conclusion that follows summarizes the paper's central arguments and their implications for Nigerian academic library practice.

CONCLUSION

The gap analysis of privacy policies across fifteen Nigerian academic libraries revealed a systemic absence of AI-specific governance provisions, leaving millions of library users exposed to data practices that may be inconsistent with their legal rights under the NDPR and NDPA and with the professional privacy commitments of the library community. This paper has shown that the ethical challenges of AI chatbot deployment in Nigerian academic libraries encompass not only individual privacy rights but also structural concerns about intellectual freedom, algorithmic bias, differential

service equity, and the adequacy of consent mechanisms. The Privacy-by-Design model proposed in response to these challenges offers a contextually grounded framework for ethical AI implementation that is responsive to the specific regulatory, infrastructural, and socioeconomic characteristics of the Nigerian academic library environment. Therefore, the central conclusion of this analysis is that the conflict between AI personalization and user privacy is not an inevitable zero-sum trade-off, but a design and governance challenge that can be addressed through deliberate institutional action: when privacy is treated as a design requirement rather than a compliance afterthought, it becomes possible to realize the genuine service benefits of AI while preserving the foundational values of patron confidentiality and intellectual freedom.

REFERENCES

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2016). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514. <https://doi.org/10.1126/science.aaa1465>
- Adetimirin, A. E. (2021). Digital privacy awareness among library users in Nigerian universities. *African Journal of Library, Archives and Information Science*, *31*(1), 45-58.
- Adeyemi, B. O., & Taiwo, A. L. (2023). Gender dimensions of data privacy attitudes among Nigerian university students. *Gender and Information Studies*, *5*(2), 112-129.
- American Library Association. (2019). Privacy: An interpretation of the library bill of rights. ALA Policy Manual.
- Bello, I. A., & Ariola, T. (2021). Awareness and perception of AI-driven library services among undergraduates in Nigerian federal universities. *Library Hi Tech*, *39*(4), 1023-1041.
- Bhatt, S., & Bhatt, A. (2022). Artificial intelligence and libraries: A review. *Library Philosophy and Practice*, *7234*, 1-17.
- Breeding, M. (2021). Privacy and library technology: Best practices and policy frameworks. *American Libraries*, *52*(5), 34-40.
- Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.
- Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.
- Fernandez, P. (2022). Privacy by design in academic libraries: A framework for implementation. *The Journal of Academic Librarianship*, *48*(3), 102541.
- International Federation of Library Associations and Institutions. (2015). IFLA internet manifesto. IFLA.
- International Federation of Library Associations and Institutions. (2021). Data protection principles for library management systems. IFLA.
- Lund, B. D., & Wang, T. (2023). Chatting about ChatGPT: How may AI and GPT impact academia and libraries? *Library Hi Tech News*, *40*(3), 26-29.
- National Information Technology Development Agency. (2019). Nigeria Data Protection Regulation. NITDA.

Publication of the European Centre for Research Training and Development -UK

- Nigeria Data Protection Commission. (2023). Nigeria Data Protection Act 2023. Federal Republic of Nigeria Official Gazette.
- Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
- Noble, S. U. (2018). Algorithms of oppression: How search engines reinforce racism. New York University Press.
- Nwosu, C., & Onyekachi, R. (2022). Privacy policy adequacy in academic libraries: Evidence from sub-Saharan Africa. *International Information and Library Review*, 54(2), 133-145.
- Okonkwo, C. W. (2022). Perception of library users on data privacy in the era of digital reference services: A study of federal universities in south-east Nigeria. *Nigerian Libraries*, 55(1), 1-22.
- Okuonghae, O., & Adeniran, P. (2020). Digitization initiatives in Nigerian academic libraries: Progress and challenges. *Information Development*, 36(4), 562-575.
- Zimmer, M. (2014). Bibliomining, library records, and the right to privacy. *International Journal of Information Management*, 34(4), 579-585.
- Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.