

LIBRARY AND INFORMATION POLICY AND THE CHALLENGES OF DATA PRIVACY, SECURITY, AND SURVEILLANCE IN DIGITAL LIBRARIES

Okiemute Patience AKPEVWOGHO

Library, Southern Delta University, Ozoro, Nigeria

Email: okiteworld@gmail.com

akpevwoghoop@sdu.edu.ng

ORCID: <https://orcid.org/0009-0008-7963-5813>

Edith Ijeoma OSHIOKPU

Department of Library and Information Science

Southern Delta University, Ozoro

Email: oshiokpuei@sdu.ng; ijeomaoshiokpuedith@gmail.com

ORCID: <https://orcid.org/0009-0007-5291-7469>

&

Rose Oborakpororo UKUAME,

Email: roseukuame@gmail.com

Abstract

This study investigated library and information policy, data privacy, challenges in the implementation of library policies, and security and surveillance in digital libraries in selected Federal University libraries in Nigeria. A quantitative cross-sectional survey design was used in the study. The study employed a structured questionnaire, and questionnaires were returned by 287 respondents (95.7%) of the 300 questionnaires distributed, which were used in the analysis. To answer the research questions, descriptive statistics was used, and to test the hypotheses at the 0.05 level of significance, regression analysis was used. The results showed that library and information policies meant for addressing data privacy had a positive general perception that they were sufficient. Data privacy practices were also shown to increase users' trust, information-seeking behaviour and intellectual freedom too. But there were institutional, technological and human capacity issues that hindered implementation of the policy. The results also showed that security measures positively enhanced the users' confidence in the digital library services, while excessive security might make some information resources not easily accessible for users. Results of the hypothesis tests showed that policy adequacy, data privacy, implementation, and security and surveillance outcomes had statistically significant associations. It is recommended that digital library governance should be an integrated process that encompasses the development of a strong privacy policy, formation of a capability to implement the policy, security measures, and clear, proportionate surveillance. It advises periodic policy reviews, capacity building for staff, enhanced infrastructure for cybersecurity, transparency in data governance, and the implementation of clear safeguards to reduce the potential for excessive user monitoring.

Keywords: Library and Information Policy; Digital Libraries; Data Privacy; Information Security; Security and Surveillance.

INTRODUCTION

Academic libraries have experienced a fast-paced digital transformation, which has brought about significant changes in the acquisition, organization, storage, access and dissemination of information resources. Nowadays, digital library platforms can be leveraged to make scholarly materials, E-databases, institutional repositories, and other technology-mediated information services available remotely, thereby increasing their accessibility and usefulness to academic library services (Onunka et al., 2023; Agboke & Oladokun, 2024; Hussain, 2023). The personalisation of services, information discovery, and operational efficiency have also been improved by the use of emerging technologies such as artificial intelligence, cloud computing, big data analytics and automated library systems (Garoufallou & Gaitanou, 2021; Jha, 2023; Bawack & Bawack, 2026). But these advances have also led to the generation of a larger and more complex amount of personal, transactional and behavioural information in digital library environments (Ocks & Salubi, 2024; Ikwanusi et al., 2023; Sebastian, 2023).

As reliance on digital infrastructures continues to increase, so has the worry over data privacy and personal information protection. As digital libraries gradually become the primary source of information for users, the governance of privacy becomes more vital to the efficient management of digital libraries (Katulic & Katulic, 2025; Kapadiya & Kapadiya, 2024; Saha, 2024). Results of academic library studies indicate that privacy and security vulnerabilities may be the potential exposure of weaknesses in institutional policies, cybersecurity infrastructure, staff awareness and data governance (Farid et al., 2025; Musa & Yelwa, 2025; Alouffi et al., 2021). When it comes to the ethical use of new technologies, the capacity of libraries to set up proper safeguards for user-collected information is now becoming more and more relevant (Ikwanusi et al., 2023; Ashiq, 2026; Bawack & Bawack, 2026). In addition to privacy, information security is now a crucial part of a digital library's governance. Digital resources, information systems and user accounts need to be secured against unauthorised access, cyber threats, data loss and any other technological compromise (Alouffi et al., 2021; Saha, 2024; Katulic & Katulic, 2025). Meanwhile, digital library systems are increasingly offering ways to track users' behaviors and activities with authentication records, system logs, usage statistics and other forms of digital tracking. While this monitoring can contribute to the security of the system, it can also raise privacy and trust issues if it is too intrusive or inadequately controlled, or if it infringes upon users' intellectual freedoms (Sebastian, 2023; Ocks & Salubi, 2024; Kapadiya & Kapadiya, 2024). Effective library and information policies that can reconcile the challenges of new technologies with new information access, privacy protection, security considerations, and responsible surveillance are clearly important. The current literature shows that various factors such as institutional capacity, technology, and human aspects still hinder the implementation of comprehensive information security policies in academic libraries (Farid et al., 2025; Musa & Yelwa, 2025; Ashiq et al., 2021). These issues are especially relevant in Nigeria's academic libraries amid the rapidly evolving landscape of digital technologies, with their policies being implemented and the security capabilities of institutions potentially differing (Agboke & Oladokun, 2024; Onunka et al., 2023; Bolasco, 2023).

Therefore, it is important to study library and information policy not only from the point of data privacy, but also from the point of security measures and surveillance mechanisms that exist in digital library environments. This study therefore investigates the Library and Information Policy and problems of Data Privacy, Security and Surveillance in digital libraries, especially the effectiveness of Policies, Privacy Practices, Challenges and the Security and Surveillance necessary to protect digital resources, user information and in monitoring the activities in digital library, with particular emphasis on the digital library and information policy and the challenges of data privacy, security and surveillance in digital libraries.

Aim and Objectives of the Study

Aim of the Study

The aim of this study is to examine library and information policy and the challenges of data privacy, security and surveillance in digital libraries.

Objectives of the Study

The specific objectives are to:

1. Examine the adequacy of existing library and information policies in addressing data privacy challenges within digital library environments.
2. Assess data privacy practices and their influence on users' trust, information seeking behaviour and intellectual freedom in digital libraries.
3. Examine the challenges affecting the implementation of library and information policies in digital libraries.
4. Assess the security and surveillance measures adopted in digital libraries, including the mechanisms used to protect digital resources and user information and monitor digital library activities.

Research Questions

The study seeks to answer the following research questions:

1. To what extent do existing library and information policies adequately address data privacy challenges in digital libraries?
2. What is the influence of data privacy practices on users' trust, information-seeking behaviour, and intellectual freedom in digital libraries?
3. What challenges affect the implementation of library and information policies in digital libraries?
4. What security and surveillance measures are adopted in digital libraries to protect digital resources and user information and monitor digital library activities?

Research Hypotheses

The following null hypotheses will be tested:

- H₀₁: Existing library and information policies have no significant effect on addressing data privacy challenges in digital libraries.
- H₀₂: Data privacy practices have no significant influence on users' trust, information-seeking behaviour and intellectual freedom in digital libraries.
- H₀₃: Library and information policy implementation has no significant relationship with the effective management of challenges affecting digital library services.
- H₀₄: Security and surveillance measures have no significant influence on users' trust, information-seeking behaviour and intellectual freedom in digital libraries.

LITERATURE REVIEW

Conceptual Review

Library and Information Policy in Digital Libraries

A digital library policy that addresses the library and information environment, library and information policy in digital libraries.

Library and information policy is the institutional principles and procedures for the management, access, use, and protection of information resources (Farid et al., 2025; Onunka et al., 2023; Agboke & Oladokun, 2024). It has become more important in the context of digital libraries due to the creation, processing and storage of large volumes of data related to usage by both users and institutions in digital libraries (Garoufallou & Gaitanou, 2021; Bawack & Bawack, 2026). Responsibilities for information governance, privacy, access control and appropriate use of technology should be clearly defined in the policy, and equitable access to digital resources should be supported (Ashiq et al., 2021; Farid et al., 2025). But the advent of artificial intelligence, cloud computing, and other emerging technologies continually present new capabilities and dangers, which are threatening traditional policy arrangements (Jha, 2023; Hussain, 2023; Ashiq, 2026). However, the effectiveness of the policy depends on institutional commitment, staff capacity, technological

facilities, and continual review (Farid et al., 2025; Bolasco, 2023; Musa & Yelwa, 2025).

Data Privacy in Digital Libraries

Data privacy issues regarding confidentiality and security of the data from unauthorized access, disclosure, and misuse (Katulic & Katulic, 2025; Kapadiya & Kapadiya, 2024; Saha, 2024). Digital libraries rely on registered and authenticated users as sources of information via their access to electronic resources and interaction with library services, and privacy is an integral aspect of good library management (Ocks & Salubi, 2024; Ikwuanusi et al., 2023; Sebastian, 2023). Good practice examples encompass transparency in the use of data collection, controlled data access, responsible handling and protection of personal information (Kapadiya & Kapadiya, 2024; Katulic & Katulic, 2025). Inadequate privacy measures can impact users' trust and willingness to access information freely (Kapadiya & Kapadiya, 2024; Ocks & Salubi, 2024). The privacy paradox underscores the impact of users' apparent privacy concerns while they are still willing to share information when they believe that digital services are beneficial to them, highlighting the need for clear governance (Ocks & Salubi, 2024; Ikwuanusi et al., 2023).

Security Measures in Digital Libraries

Information security refers to technical and organisational measures for protecting digital resources and systems against unauthorised access, disruption, loss and cyber threats (Alouffi et al., 2021; Saha, 2024; Katulic & Katulic, 2025). The protection of resources and user information in a digital library can be achieved by using authentication, access controls, secure information-management practices and other mechanisms (Farid et al., 2025; Katulic & Katulic, 2025; Musa & Yelwa, 2025). Cloud-based environments add to the risks as services and information can rely on interconnected or external infrastructure (Alouffi et al., 2021; Garoufallou & Gaitanou, 2021). Thus, security needs to be both technological and institutional, with responsibilities and procedures established in the institutional policies for the protection of information assets (Farid et al., 2025; Saha, 2024).

Surveillance in Digital Libraries

Surveillance is the process of keeping an eye on or tracking a user's online behavior for security, administration and service management (Kapadiya & Kapadiya, 2024; Ocks & Salubi, 2024; Sebastian, 2023). Digital systems can create records of authentication, resources accessed and patterns of activities which allow libraries to track and monitor system use and identify potentially inappropriate activities (Bawack & Bawack, 2026; Garoufallou & Gaitanou, 2021). Monitoring can be used to assist security, but it must be based on principles of transparency, proportionality and appropriate governance (Kapadiya & Kapadiya, 2024; Ocks & Salubi, 2024). Overuse or over-regulation of surveillance can affect the privacy, trust, and intellectual freedom of users, as they may be deterred from seeking certain sensitive or controversial information (Kapadiya & Kapadiya, 2024; Ocks & Salubi, 2024; Sebastian, 2023). Security and surveillance are thus analytically separate, security is about ensuring security of systems and resources, while surveillance is about observing or monitoring what is going on within a system (Saha, 2024; Kapadiya & Kapadiya, 2024).

Users' Trust, Information-Seeking Behaviour, and Intellectual Freedom

Perception of responsible management and digital activity protection from misuse of users' personal information, and digital activity protection from misuse (Kapadiya & Kapadiya, 2024; Saha, 2024; Ocks & Salubi, 2024) have an impact on users' trust in digital libraries. Proper privacy and security measures can foster trust and promote sustained user interaction with digital information systems, while insufficient security measures can lead to lack of trust and less use of the systems (Musa & Yelwa, 2025; Katulic & Katulic, 2025). Information-seeking behaviour can also be affected by monitoring practices if the users feel monitored (Kapadiya & Kapadiya, 2024; Sebastian, 2023). This means that libraries should create a space where the users can read the material in an appropriate way without any unnecessary monitoring and interference in the reading process (Ashiq et al., 2021; Onunka et al., 2023).

Theoretical Review

Communication Privacy Management Theory

The Communication Privacy Management Theory, created by Sandra Petronio, details the ways personal information is regulated and managed by individuals and how individuals expect those who have access to it to do so responsibly. The theory has significant implications for digital libraries as people input their personal information and create digital records of their behavior when using electronic resources and services (Kapadiya & Kapadiya, 2024; Ocks & Salubi, 2024). Users should therefore reasonably be able to anticipate that libraries will create clear policies in relation to collecting, storing, accessing, and sharing information that they collect about the user (Ikwuanusi et al., 2023; Saha, 2024). Failure to meet these expectations can inflict a lack of trust and impact on information-seeking behavior (Kapadiya & Kapadiya, 2024; Ocks & Salubi, 2024). The theory also sheds light on issues related to surveillance, as it needs to be transparent and securely monitored to avoid intruding into users' boundaries of privacy (Sebastian, 2023; Kapadiya & Kapadiya, 2024). Therefore, it is a suitable basis to consider the balancing of security needs of the institution, privacy, and intellectual freedom in library policy.

Empirical Review

Farid et al. (2025), in a systematic review of digital information-security management policies in academic libraries, found that policy implementation remained inconsistent because of limited institutional commitment, inadequate staff awareness, and weak assessment mechanisms. Musa and Yelwa (2025) similarly identified inadequate cybersecurity infrastructure, limited privacy awareness, and weak institutional policies as major challenges in tertiary-institution digital libraries in Zamfara State. These findings establish the importance of policy implementation and institutional capacity within the Nigerian context.

Ocks and Salubi (2024) examined the privacy paradox in library information services and found that users could continue providing personal information despite privacy concerns, highlighting the importance of transparency and effective data governance. Kapadiya and Kapadiya (2024) emphasised the protection of user information and the implications of monitoring for privacy and trust, while Ikwuanusi et al. (2023) argued that ethical AI practices can strengthen privacy protection when supported by appropriate governance mechanisms.

Katulic and Katulic (2025) demonstrated the importance of personal-data protection within academic library service platforms, while Alouffi et al. (2021) identified security threats and mitigation requirements associated with cloud computing. Collectively, these studies establish substantial evidence on privacy, security and policy, but provide comparatively limited empirical attention to the specific security measures and surveillance mechanisms operating within digital libraries and their implications for users.

Synthesis and Gap in Literature

The literature has identified how library policy, privacy and security/surveillance issues are interconnected in the process of digital transformation (Onunka et al., 2023; Garoufallou & Gaitanou, 2021; Agboke & Oladokun, 2024). Privacy protection, cybersecurity, and ethical policies and technology adoption have been studied by previous researchers (Farid et al., 2025; Musa & Yelwa, 2025; Ikwuanusi et al., 2023). However, privacy and security are often studied as a single entity, and surveillance is considered a secondary phenomenon compared to privacy and security (Kapadiya & Kapadiya, 2024; Ocks & Salubi, 2024; Sebastian, 2023). The weak empirical linkage of library and information policy, data privacy, security, and surveillance mechanisms as three components of digital library governance within Nigerian academic libraries is the major gap, as mentioned in Musa & Yelwa (2025); Agboke & Oladokun (2024); Farid et al. (2025). This study seeks to fill this void by considering security and surveillance as an analytical goal in its own right, and by investigating how it affects users' trust, information-seeking behaviour, and intellectual freedom. This differentiated approach offers a solid foundation for comprehending the balance between safeguarding systems and resources and preserving users' privacy and freedom of information access in a digital library without over-constricting users' rights (Kapadiya & Kapadiya, 2024; Ocks & Salubi, 2024; Saha, 2024).

METHODOLOGY

This study was conducted using a quantitative approach with cross sectional survey design in the study, which aimed to find out the library and information policy, data privacy, policy implementation challenges, security and surveillance measures in digital libraries. The study targeted selected Federal University libraries in Nigeria, between which registered library users and professional librarians were targeted. The study population consisted of 1,200 respondents, and the sample size was determined by Taro Yamane's formula at 0.05 level of precision, which gave 300 respondents. Stratified random sampling was employed in proportionate sampling to ensure representativeness of the identified groups of respondents. Data was collected by a structured questionnaire with closed ended items on 5 point Likert scale. The instrument included questions concerning library and information policy, data privacy, implementation problems and security and surveillance, and the latter was analyzed separately. The reliability of the instruments was measured with Cronbach's Alpha, where the minimum value that was accepted was 0.70. The responses were summarised using descriptive statistics and tested the stated hypotheses using multiple regression analysis at the 0.05 level of significance. This analysis was carried out with the 287 questionnaires that were returned of 300 questionnaires distributed.

RESULT

Presentation of Results

In total, 300 questionnaires were given to the respondents who were chosen from the study area. Of these, 287 questionnaires (95.7%) were properly completed and returned, 8 questionnaires (2.7%) were partially filled and 5 questionnaires (1.6%) were withdrawn by the respondents. Thus, 287 questionnaires were used as data for the analysis.

Data Analysis

Table 1: Socio Demographic Characteristics of Respondents (N = 287)

Variable	Category	Frequency	Percentage (%)
Gender	Male	156	54.4
	Female	131	45.6
Age	Below 20 years	26	9.1
	20 to 29 years	118	41.1
	30 to 39 years	81	28.2
	40 to 49 years	42	14.6
	50 years and above	20	7.0
Status	Undergraduate Student	102	35.5
	Postgraduate Student	70	24.4
	Academic Staff	40	13.9
	Librarian	58	20.2
	Others	17	5.9
Educational Qualification	Diploma	28	9.8
	Bachelor's Degree	121	42.2
	Master's Degree	93	32.4
	Doctorate	33	11.5
	Others	12	4.2
Digital Library Usage	Daily	94	32.8
	Weekly	97	33.8
	Monthly	49	17.1
	Occasionally	32	11.1
	Rarely	15	5.2

The data presented in the table reveals that there was a relatively even gender distribution with 156 respondents (54.4%) being male and 131 (45.6%) female. As far as age is concerned, the

most numerous group was those aged between 20 and 29 years (41.1%), while the next group of respondents was aged between 30 and 39 years (28.2%). A total of 26 (9.1%) and 42 (14.6%) respondents were below 20 and 40–49 years, respectively, and 20 (7.0%) were 50 years old and over. In terms of status, the largest group was undergraduate students (102 or 35.5%), then postgraduate students (70 or 24.4%) and then librarians (58 or 20.2%). The academic staff category received the highest number of responses (40, 13.9%), and another 17 respondents (5.9%) were in other categories. As regards educational qualifications, the highest number of respondents were those with a bachelor's degree (121, 42.2%), followed by those holding a masters degree (93, 32.4%). 33 (11.5%) respondents had doctorates; 28 (9.8%) had diplomas; and 12 (4.2%) had other qualifications. In terms of frequency of using the digital library, 97 (33.8%) respondents used the digital library weekly, and 94 (32.8%) respondents used the digital library daily. 49 respondents used digital library services monthly (17.1%), 32 respondents used digital library services occasionally (11.1), and 15 respondents used digital library services rarely (5.2%).

ANSWERING RESEARCH QUESTIONS

Research Question One

To what extent do existing library and information policies adequately address data privacy challenges in digital libraries?

Table 6: Adequacy of Library and Information Policies in Addressing Data Privacy Challenges (N = 287)

S/N	Questionnaire Items	SA n (%)	A n (%)	U n (%)	D n (%)	SD n (%)	M	SD	Decision
1	My library has clear policies for protecting users' personal information.	109 (38.0)	116 (40.4)	22 (7.7)	28 (9.8)	12 (4.2)	3.98	1.11	Agree
2	Library staff follow established rules when handling users' personal data.	98 (34.1)	121 (42.2)	27 (9.4)	29 (10.1)	12 (4.2)	3.92	1.10	Agree
3	The digital library clearly explains how users' information is collected and used.	93 (32.4)	126 (43.9)	23 (8.0)	31 (10.8)	14 (4.9)	3.88	1.13	Agree
4	Existing library policies adequately protect users from unauthorised access.	101 (35.2)	118 (41.1)	25 (8.7)	30 (10.5)	13 (4.5)	3.92	1.12	Agree
5	Current policies effectively regulate monitoring of	87 (30.3)	123 (42.9)	31 (10.8)	34 (11.8)	12 (4.2)	3.83	1.11	Agree

	users' activities.								
	Grand Mean						3.91	1.11	Agree

Decision rule: Mean ≥ 3.00 = Agree; Mean < 3.00 = Disagree.

The general perception of the library and information policies' level of effectiveness in meeting data privacy issues is also favourable as indicated in Table 6. There was an overall agreement (grand mean = 3.91, meaning ranged from 3.83 to 3.98). Clear policies protecting users' personal information had the highest mean score (3.98), and the lowest mean score (3.83) was for the effectiveness of policies in regulating users' monitoring. The results also indicate that respondents are aware of the existence of institutional privacy provisions, although there is a comparatively lower number of respondents in relation to the points of regulation of monitoring, suggesting an area of increased policy clarity and governance.

Research Question Two

What is the influence of data privacy practices on users' trust, information-seeking behaviour and intellectual freedom in digital libraries?

Table 7: Data Privacy Practices, Users' Trust, Information-Seeking Behaviour and Intellectual Freedom (N = 287)

S/N	Questionnaire Items	SA	A	U	D	SD	M	SD	Decision
1	I trust the digital library because my personal information is protected.	105 (36.6)	119 (41.5)	24 (8.4)	27 (9.4)	12 (4.2)	3.97	1.10	Agree
2	I feel free to search for information without fear of misuse of my activities.	96 (33.4)	124 (43.2)	25 (8.7)	29 (10.1)	13 (4.5)	3.91	1.11	Agree
3	Good privacy practices encourage me to use the digital library more frequently.	101 (35.2)	121 (42.2)	23 (8.0)	29 (10.1)	13 (4.5)	3.93	1.12	Agree
4	I am more willing to use digital library resources when I know my personal information is protected.	108 (37.6)	117 (40.8)	21 (7.3)	29 (10.1)	12 (4.2)	3.98	1.11	Agree
5	Privacy protection encourages me to explore information resources freely.	94 (32.8)	126 (43.9)	26 (9.1)	28 (9.8)	13 (4.5)	3.91	1.10	Agree
	Grand Mean						3.94	1.11	Agree

From Table 7, it can be seen that the users' perception of the relationship between data privacy practices and trust, information-seeking behaviour and intellectual freedom is positive. The range of the items was from 3.91 to 3.98, with a grand mean of 3.94. The mean (3.98) was the

highest for users' willingness to use digital library resources if their personal information was protected. The findings indicated that privacy protection is linked to higher confidence in digital library services and the conditions are conducive to users' search and exploration of information.

Research Question Three

What challenges affect the implementation of library and information policies in digital libraries?

Table 8: Challenges Affecting the Implementation of Library and Information Policies (N = 287)

S/N	Questionnaire Items	SA	A	U	D	SD	M	SD	Decision
1	Inadequate funding affects the implementation of library and information policies.	111 (38.7)	116 (40.4)	21 (7.3)	27 (9.4)	12 (4.2)	4.00	1.10	Agree
2	Inadequate cybersecurity infrastructure makes policy implementation difficult.	105 (36.6)	122 (42.5)	23 (8.0)	25 (8.7)	12 (4.2)	3.99	1.08	Agree
3	Lack of staff training affects compliance with information policies.	98 (34.1)	126 (43.9)	24 (8.4)	27 (9.4)	12 (4.2)	3.94	1.09	Agree
4	Limited user awareness of data privacy requirements affects policy implementation.	101 (35.2)	119 (41.5)	25 (8.7)	29 (10.1)	13 (4.5)	3.93	1.12	Agree
5	Existing policies are not reviewed regularly to reflect technological changes.	94 (32.8)	121 (42.2)	29 (10.1)	30 (10.5)	13 (4.5)	3.88	1.12	Agree
6	Rapid technological changes make existing policies difficult to implement.	107 (37.3)	118 (41.1)	22 (7.7)	28 (9.8)	12 (4.2)	3.98	1.10	Agree
	Grand Mean						3.95	1.10	Agree

Table 8 reveals substantial challenges affecting policy implementation, with item means ranging from **3.88 to 4.00** and a grand mean of **3.95**. Inadequate funding recorded the highest mean (4.00), closely followed by inadequate cybersecurity infrastructure (3.99) and rapid technological change (3.98). These findings indicate that implementation challenges extend

beyond policy formulation to financial resources, technological infrastructure, staff competence, user awareness, and the capacity to continuously adapt policies to technological developments.

Research Question Four

What security and surveillance measures are adopted in digital libraries to protect digital resources and user information and monitor digital library activities?

Table 9: Security and Surveillance Measures in Digital Libraries (N = 287)

Dimension	Questionnaire Items	SA	A	U	D	SD	M	SD	Decision
Security	Strong security measures increase my confidence in digital library services.	112 (39.0)	119 (41.5)	20 (7.0)	25 (8.7)	11 (3.8)	4.03	1.08	Agree
Security	Existing security measures adequately protect digital resources from unauthorised access.	103 (35.9)	121 (42.2)	24 (8.4)	27 (9.4)	12 (4.2)	3.96	1.09	Agree
Security	Security measures protect users' personal information from unauthorised access.	106 (36.9)	118 (41.1)	25 (8.7)	27 (9.4)	11 (3.8)	3.98	1.09	Agree
Surveillance	Current policies effectively regulate monitoring of users' activities.	87 (30.3)	123 (42.9)	31 (10.8)	34 (11.8)	12 (4.2)	3.83	1.11	Agree
Surveillance	Digital library systems monitor users' access activities.	91 (31.7)	119 (41.5)	30 (10.5)	34 (11.8)	13 (4.5)	3.84	1.13	Agree
Surveillance	Excessive monitoring discourages me from using some digital library	105 (36.6)	117 (40.8)	24 (8.4)	28 (9.8)	13 (4.5)	3.95	1.12	Agree

	resources.								
	Security Grand Mean						3.99	1.09	Agree
	Surveillance Grand Mean						3.87	1.12	Agree

The survey results in table 9 clearly show a difference between respondents' perceptions of security and surveillance. The grand mean for the three security items was 3.99, suggesting a high level of agreement that security measures are effective at protecting resources and user information, and increase confidence in the digital library services. The most frequent individual mean (4.03) was related to confidence in the security measures.

The results for the surveillance items yielded a slightly lower, but still favorable, grand mean of 3.87. All the respondents agreed that digital library systems track access activity, and that current policies govern the tracking. The mean on the statement "Some resources are used less because of excessive monitoring" is of special interest, however, because it is equal to 3.95. It means that even when perceived as institutionally controlled, surveillance has a potential behavioural effect.

The results thus suggest that security and surveillance should be considered analytical dimensions separately. Security is seen as protection and a boost to confidence, while over-surveillance can create a situation of limiting information use. This distinction is the one that is at the heart of the study's contribution.

TEST OF RESEARCH HYPOTHESES

The hypotheses were tested at the **0.05 level of significance** using regression analysis. The null hypothesis was rejected where $p < .05$ and retained where $p \geq .05$. The four hypotheses correspond directly to the four research objectives.

Table 10: Summary of Regression Tests of Research Hypotheses

Hypothesis	Test	R	R ²	Adjusted R ²	F	p-value	Decision
H₀₁: Library and information policies have no significant effect on addressing data privacy challenges in digital libraries.	Regression	0.714	0.510	0.508	296.42	< .001	Rejected
H₀₂: Data privacy practices have no significant influence on users' trust, information-seeking behaviour and intellectual freedom.	Regression	0.768	0.590	0.586	135.76	< .001	Rejected
H₀₃: Challenges affecting the implementation of library and information policies have no significant effect on the effective implementation of such policies in digital libraries.	Regression	0.681	0.464	0.460	61.12	< .001	Rejected

H₀₄: Security and surveillance measures have no significant influence on users' trust, information-seeking behaviour and intellectual freedom.	Regression	0.739	0.546	0.543	113.61	< .001	Rejected
--	------------	-------	-------	-------	--------	--------	-----------------

Results of the regressions have shown that there are statistically significant relationships in each of the four hypothesised relationships. The results indicate that data privacy outcomes are not due to chance ($R^2 = .510$, $p < .001$); library and information policy explains 51.0% of the variance in data privacy outcomes. The same situation occurs with H₀₂, which explains 59.0% of the variance with data privacy practices and users' trust, information-seeking behaviour and intellectual freedom ($R^2 = .590$, $p < .001$).

The model is statistically significant ($R^2 = .464$, $p < .001$) so the identified implementation challenges are significantly related to policy implementation outcomes and H₀₃ is rejected. Lastly, H₀₄ is rejected, and security and surveillance account for 54.6% of the variance in users' trust, information-seeking behaviour and intellectual freedom ($R^2 = .546$, $p < .001$).

The results overall show that policy adequacy, data privacy, implementation conditions, security and surveillance are important aspects of digital library governance. Most importantly, the strong H₀₄ supports empirical grounds for including an objective for Security and Surveillance in the fourth objective instead of simply being a part of data privacy.

DISCUSSION OF FINDINGS

The results highlight the need to take care of the intersection of policy sufficiency, data protection, capacity to implement, and the security and surveillance model to make digital libraries effective. The overall impression of the current privacy policies and security protections was favorable, indicating that effective institutional policies and security precautions could help to build user trust and confidence that they are able to trust the digital library resources. This is consistent with the values of effective governance of privacy and information security in digital library contexts that Farid et al. (2025), Kapadiya and Kapadiya (2024), and Saha (2024) have highlighted. But the implementation challenges remain and include infrastructure, staff competence, funding and technological changes (Agboke & Oladokun, 2024; Bolasco, 2023; Musa & Yelwa, 2025). Importantly, the findings indicate that security and surveillance do not go hand in hand: while robust security provides increased confidence, over-monitoring can result in a decrease in information use. This discovery further underlines concerns for privacy, responsible data governance, and the ethical management of data in digitally mediated library services (Ocks & Salubi, 2024; Ikwuanusi et al., 2023; Katulic & Katulic, 2025).

CONCLUSION AND RECOMMENDATIONS

The study reveals that a comprehensive strategy for digital library governance calls for an integrated approach to library and information policy, data privacy, policy implementation, security and surveillance. The results show that in general, users' confidence and participation in digital library services are enhanced by existing privacy and security measures. But institutional, technological, and human-capacity limitations are present for implementing. The results also highlight the need to consider security and surveillance as separate, yet interrelated dimensions; appropriate security measures are essential to users and digital resources, but too much surveillance can deter users from seeking information and affect their trust. Therefore, the protection, monitoring, privacy, and intellectual freedom must be balanced in the framework of effective governance.

Recommendations

1. Digital libraries should regularly review and revise privacy and information policies to address the latest developments in technology, cybersecurity, and information protection needs.
2. Institutions should further improve security infrastructure by implementing appropriate security authentication, access control, data protection, system monitoring, and cybersecurity security measures.
3. Constant training of library staff on data privacy, cybersecurity, emerging technologies, and responsible information governance.
4. Surveillance practices shall be policy-governed, proportionate, and transparent. Users must understand the types of activities being monitored; why they are being monitored; how information is being collected, processed, and used.
5. Libraries need to create concrete safeguards to prevent over-monitoring, and security measures should not unduly limit users' information-seeking, their privacy, or their intellectual freedom.

REFERENCES

- Agboke, A. L., & Oladokun, B. D. (2024). Emerging technologies in academic libraries: prospects and challenges in Nigeria. *Communicate: Journal of Library and Information Science*, 26(2), 10-20.
- Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *Ieee Access*, 9, 57792-57807.
- Ashiq, M. (2026). Industry 5.0—the human centric solution and personalization: challenges and opportunities for libraries. *Library Hi Tech News*, 43(5), 16-19.
- Ashiq, M., Rehman, S. U., & Mujtaba, G. (2021). Future challenges and emerging role of academic libraries in Pakistan: A phenomenology approach. *Information Development*, 37(1), 158-173.
- Bawack, R., & Bawack, R. (2026). “Hey librarian, what can AI and analytics do for you”: a systematic literature review and sociotechnical perspective. *Aslib Journal of Information Management*, 78(4), 816-834.
- Bolasco, M. L. O. (2023). Librarians’ digital competencies: influence on their utilization of emerging educational technologies. *British Journal of Multidisciplinary and Advanced Studies*, 4(4), 75-87.
- Farid, G., Warraich, N. F., & Iftikhar, S. (2025). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, 51(4), 1000-1014.
- Garoufallou, E., & Gaitanou, P. (2021). Big data: opportunities and challenges in libraries, a systematic literature review. *College & Research Libraries*, 82(3), 410.
- Hossain, Z., Biswas, M. S., & Khan, G. (2026). AI literacy of library and information science students: A study of Bangladesh, India and Pakistan. *Journal of Librarianship and Information Science*, 58(1), 285-299.
- Hussain, A. (2023). Use of artificial intelligence in the library services: prospects and challenges. *Library Hi Tech News*, 40(2), 15-17.
- Ikwuanusi, U. F., Adepoju, P. A., & Odionu, C. S. (2023). Advancing ethical AI practices to solve data privacy issues in library systems. *International journal of multidisciplinary research updates*, 6(1), 033-044.
- Jha, S. K. (2023). Application of artificial intelligence in libraries and information centers services: prospects and challenges. *Library hi tech news*, 40(7), 1-5.
- Kapadiya, M. H., & Kapadiya, N. K. (2024). User Privacy in Digital Libraries: Challenges, Implications and Strategies for Safeguarding Information. *Indian Journal of Library Science Research & Information Technology*, 1(2), 37-45.
- Katulic, A., & Katulic, T. (2025). Ensuring security of personal data in library services platforms of academic libraries in the EU. *Digital library perspectives*, 41(3), 403-418.
- Musa, H., & Yelwa, A. S. (2025). Data Privacy and Security Challenges in Digital Libraries of Tertiary Institutions in Zamfara State. *FUGUS International Journal of Library and Information Science*, 2(2), 79-89.
- Ocks, Y., & Salubi, O. G. (2024). Privacy Paradox in Industry 4.0: A review of library information services and data protection. *South African Journal of Information Management*, 26(1), 1845.
- Onunka, O., Onunka, T., Fawole, A. A., Adeleke, I. J., & Daraojimba, C. (2023). Library and information services in the digital age: Opportunities and challenges. *Acta Informatica Malaysia*, 7(1), 113-121.
- Saha, R. (2024). Data privacy and cyber security in digital library perspective: Safe guarding user information. *International journal of scientific research in engineering and management*, 8(4).
- Sebastian, G. (2023). Privacy and data protection in ChatGPT and other AI chatbots: strategies for securing user information. *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)*, 15(1), 1-14.

Udo-Okon, T. N., Akpan, E. E., Fcicn, D. P., & Ap, P. P. G. D. C. A. (2024). The challenges of artificial intelligence in library management system. *Information science*, 6(1).