International Journal of Research in Library Science (IJRLS)

ISSN: 2455-104X

DOI: 10.26761/IJRLS.12.1.2026.2059

Volume 12, Issue 1 (January-March) 2026, Page: 281-292, Paper ID: IJRLS-2059

Protecting library user privacy

Dr. Vrushali Rane

Deputy Librarian, SNDT Women's University, BMK Knowledge Resource Centre, Mumbai, Maharashtra, India

libraryjuhu@sndt.ac.in; vrushrrane@gmail.com

ABSTRACT

This paper addresses the pressing issue of library user data privacy amidst the influence of information technology. It emphasizes the need for libraries to protect user data and explores strategies for doing so in a digital access environment.

The study conducted an online survey of libraries, collecting 342 responses to assess practices and perceptions regarding user data privacy. The survey focused on understanding the purpose of collecting personal information, awareness of associated risks, security measures employed, and the availability of privacy guidelines within institutions

.

Analysis revealed that 93% of libraries provided remote access, though not all shared user data. Most respondents demonstrated an understanding of the risks involved in utilizing personal information and highlighted security measures in place. However, 86% indicated a lack of privacy guidelines availability. Despite this, respondents provided insights into measures taken to maintain confidentiality and suggestions for positive user-library relationships.

This study contributes to the literature on library user data privacy by providing current practices and perceptions. By surveying libraries comprehensively, it identifies challenges and opportunities in safeguarding user data and gaps in privacy guidelines.

KEYWORDS: Library users; User Privacy; Authentication; Security Privacy Protection; User Security; Data Confidentiality; Data Protection; Personal Data.

INTRODUCTION

The libraries are now taking a holistic view of the library's collections, services and operations. Libraries are also taking advantage of emerging technologies to help users find information. With remote learning, cloud storage and digital access the focus is more on data privacy. As the way private information is shared, secured and damaged has increased. Libraries need to handle user personal information safely without causing any mishaps. The IFLA Code

of Ethics identifies respect for personal privacy, protection of personal data, and confidentiality in the relationship between the user and library as core principles.

The most challenging task for libraries is protecting user privacy. There are third parties involved in library activities to provide services. Libraries share user data with them which is stored on cloud or on an outside library server. As the services are mainly used by users on mobile devices the libraries need to make decisions on personal data management of users. The AMERICAN LIBRARY association code of ethics suggests to plan what kind of minimal user data to be collected, stored, shared and which data to be retained. Some guidelines to decide on user data are required to be prepared by the libraries to protect and maintain confidentiality. Libraries can also set rules with the third party or vendors before sharing user data to ensure privacy and quality service.

LITERATURE REVIEW

The literature review provides a comprehensive exploration of the complex aspects of data privacy and security concerns in libraries.

Kuzma investigated the web vulnerability challenges at European library web sites and how these issues can affect the data protection of their patrons. A web vulnerability testing tool was used to analyze 80 European library sites in four countries to determine how many security vulnerabilities each had and what were the most common types of problems. Analysis results from surveying the libraries show the majority have serious security flaws in their web applications. The research shows that despite country-specific laws mandating secure sites, system librarians have not implemented appropriate measures to secure their online information systems. Author suggests measures managerial processes such as performing periodic audits and risk assessments can help determine which systems are most vulnerable and concentrate on protecting those functions, as well as inspecting the systems to analyze potential problems. Technical approaches are the second method of diminishing these factors. These include ensuring updates and patches are promptly installed and having coders and designers implement safe coding practices to enhance their systems security and protect patron's data.

Devi surveyed the students of Manipur University to understand the usage and awareness of importance of social networking sites of academic nature. Among the users surveyed, 45% stated that there is a problem involved in the use of social networking sites mainly in the area of data security. Hence one needs to think twice before inclusion of personal data on social media.

Kritikos and Zimmer in their article 'Privacy Policies and Practices with Cloud-Based Services in Public Libraries: An Exploratory Case of Biblio Commons' found that public libraries are increasingly turning to cloud-based and Library 2.0 solutions to provide patrons more user-focused, interactive, and social platforms from which to explore and use library resources. These platforms such as BiblioCommons often rely on the collection and aggregation of patron data, and have the potential to disrupt long standing ethical norms within librarianship dedicated to protecting patron privacy. This article reports on the results of a pilot research study investigating how libraries are implementing third-party cloud computing services, how these implementations might impact patron privacy, and how libraries are responding to these concerns. The results of this research provide insights to guide the development of a set of best practices for future implementations of cloud-based Library 2.0 platforms in public library settings. The best practice came from the New York Public Library, who took additional steps to ensure

patrons were made aware of the new platform and the data sharing that might occur. Libraries are recommended to follow this example and provide direct and meaningful communication with patrons about what it means to create an account on the Biblio-Commons platform.

Marden described that the newly revised privacy policy approved by the New York Public Library's (NYPL) Program and policy committee in its September 2016 meeting provided the public with clear explanation of what information NYPL collects from the users, how NYPL uses that information, how users can manage the information NYPL collects about them (including methods of opting in and out of that collection) and when NYPL shares that information with the third parties.

Pekala pointed out that the emergence of a data economy has led to a new wave of online tracking and surveillance, in which multiple third parties collect and share user data during the discovery process making it much more difficult for the libraries to protect patron privacy. Users do their searches with web search engines, diminishing the library's control over privacy. Users expect their library discovery experience to be the same as web search engines. However, web search engines rely on a drastically different set of privacy standards, as they strive to create tailored, personalized search results based on user data. This paper explored the competing interests of privacy and user experience, and proposes possible strategies to address them in the future design of library discovery tools. An absolutely private discovery experience would mean that no user data is ever collected during the search process, whereas a completely personalized discovery experience would mean that all user data is collected and utilized to inform the design and features of the system. It is essential for library discovery tools to have built-in functionality that protects patron privacy to the greatest extent possible and enables the ethical use of patron data to improve user experience. The libraries need to address these requirements beyond establishing guidelines. Librarians need to engage in user experience research and design to discover and test the usefulness of possible intermediary solutions. Librarians must also become more educated as a profession on digital privacy issues and their ethical implications in order to educate patrons about their fundamental rights to privacy and empower them to make decisions about which discovery tools to use.

Yoose studied de-identification of Patron Data at Seattle Public Library for balancing privacy and strategic planning needs. The National Institute of Standards and Technology (NIST) USA divides Personally Identifiable Information (PII) into two categories. The first category, PII-1, is information that can directly identify a person, including name, birth date, address, and Social Security Number. The second category, PII-2, pertains to an individual's activities that can be linked back to that individual like medical, educational, financial, and employment information. In the context of libraries, the second category of PII includes the intellectual pursuits of the patron, including reference interactions, search queries, and circulation history. This kind of data, in sufficient enough quantities, can be used in certain circumstances to reverse engineer an identity. A famous example of re-identification using PII-2 data is the America Online release of search data in 2006. Even though the data was edited to remove some PII, the amount of PII-2 data present in the dataset enabled researchers to identify searchers by specific search patterns and queries. Since library patron data contains both categories of PII, libraries must consider the various risks regarding what data should be stored and used for operational use, along with the additional risks of having PII stored with third party vendors. If a library wants to perform analysis with regards to library collections and services, then they need

to construct a way to track unique data points without identifying unique individuals through PII disclosure (intentional or accidental). Anonymizing the data does not allow for this type of analysis, making it difficult to use the otherwise rich context that historical data would have provided. Outside of anonymization, another approach to consider for long-term analysis of 'unique data points' is the de-identification process which focuses on scrubbing particular PII data in a data set while at the same time keeping the data in a state where one can still track unique data points. With the removal or obfuscation of several PII-1 and PII-2 data points, one's ability to identify a particular individual in a data set is severely hampered, if not made impossible to do. De-identification is a viable option for protecting the privacy of individuals in particular datasets that are used to track behaviour or trends on an individual level. In practice, library patron data de-identification has its unique challenges and considerations. The case study of the Seattle Public Library shows how the library approached these challenges with the construction of their data warehouse.

Wu proposed an approach for the protection of user's book browsing behaviour in digital libraries whose practical significance is that it can ensure not only the security of behaviour privacy but also the availability (i.e. usability, accuracy and efficiency) of book services, making it easier to be integrated to an existing digital library platform. Besides, the basic idea of 'constructing dummies to cover up users' genuine book browsing requests' proposed in this paper also provides a new theoretical attempt to the protection of users' behaviour privacy in digital libraries. For this, the author has compared the methods such as encryption, identity authentication and access control that are not designed for digital libraries with this new approach for checking its suitability for checking the book browsing behaviour. The proposed framework includes constructing a group of ideal dummies for a user book browsing request which includes defining a privacy model to formulate the constraints that the ideal dummy request sequences should satisfy and then, based on the repository of book classification discussed an implementation algorithm of the privacy model followed by theoretical analysis of the security of the approach.
Thomchick and Nicolas-Rocca have thrown light on the security of user personal information. With the advent of IT, the confidentiality of data can be more secure using HTTPS as user data is very sensitive. To improve application security in libraries, implementation of HTTPS shall be beneficial.

Lamanna stated that libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information. He points out that all people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. As per the Patriot Act, libraries should stop collecting patron's reading habits. For this, Personally Identifiable Information (PII) is strictly necessary and libraries should check what information libraries really need to collect to offer the library cards. For example, date of birth or gender. If somebody is still collecting it, they need to keep it anonymous. Also CCTVs should only be set up where needed, taking great care to not to point them at patrons or staff computers. Also libraries need to make sure to follow the local CCTV footage retention laws and remove the footage as soon as time has expired. Libraries need to consider whether the presence of police or law enforcement personnel is actually necessary for the proper functioning in your library. Use of facial recognition technology where one's face is used to create a user profile has become ubiquitous and it is getting pushed back, libraries can initiate banning it. Libraries should ensure unlimited Wi Fi access to the users for emergencies for completing their work accessing online services, making sure WiFi is secure.

Maceli explores librarians' mental models or internalized understanding of the internet and how such knowledge is applied in their use and perception of Privacy Protection Technologies (PPT). He checked the librarian's familiarity with privacy related technical concepts like privacy settings, IP address, web browser plug-ins to block ads or tracking, incognito mode, cookies, encryption, proxy server, privacy protection search engine, virtual private network (VPN), Tor browser, secure sockets layer (SSL).

Nicolas-Rocca and Burkhard investigated how knowledge transferred within an online cyber security education has a positive effect on library employee information security practices and risk management practices in the libraries in the U.S.. Libraries in the United States handle sensitive patron information**,** including personally identifiable information and circulation records. With libraries providing services to millions of patrons across the U.S., it is important that they understand the importance of patron privacy and how to protect it. When library users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists. Therefore, it is imperative that libraries use extra care when handling patron personally identifiable information.

Katulić, Katulić and Grgić study found the relationship between the legal obligation of European libraries to ensure the transparent personal data processing and respect for user privacy. The paper highlights how libraries use privacy notices on websites to communicate with library users about the processing of personal data. Further it provides applicable transparency guidelines. The privacy policies and other privacy related documents were checked on the websites of 45 European national libraries. The analysis was done on the basis of the General Data Protection Regulation and the recommendations of the WP29/EDPB Transparency Guidelines. The findings suggest that European national libraries largely adhere to EU data protection standards. In total, 60% libraries use a separate privacy page, and 53% of the EU Member State national libraries websites managed to comply with publishing all necessary data protection information in a way recommended by the Guidelines, compared to 47% of non-Member State national libraries.

Together, these studies underscore the complex challenges and best practices in ensuring data privacy and security in library settings.

OBJECTIVES

- ✓ To understand the purpose of collecting personal information of the users
- ✓ To assess the risk factor involved in using personal information of the users
- ✓ To list out the measures taken for securing user data
- ✓ To check the availability of privacy guidelines

SCOPE OF THE STUDY

The scope of this research was to find out the measures taken by libraries in India to protect the personal data of users. It included how libraries handle user personal data when providing services internally as well as while involving third parties. It also tried to understand the security issues and risk factors involved in maintaining confidentiality. Other aspects related to user data privacy like policy guidelines, purpose of personal data collection were also studied. The study touches on the important aspect of user data privacy in this digital access environment.

RESEARCH METHODOLOGY

The survey method was used to understand the issues related to user privacy at the Indian libraries. For data collection questionnaire tool was employed. The questionnaire was prepared using google forms and sent digitally across all Indian libraries through ILOSc forum (Indian Librarians Online Study Circle) consisting of library professionals to get maximum responses. The questionnaire consisted of 18 questions which included 02 general questions, 09 multiple choice questions and 07 open ended questions. The questions were pilot tested and improved according to the suggestions. Total 367 responses were received. Out of it, 25 responses were not considered as the questionnaires were incomplete, there were duplicate responses etc. Thus a total 342 responses were analysed and presented in the following section.

DATA ANALYSIS AND INTERPRETATION

It was found from figure 1 that 89.5% had a remote access facility for accessing electronic resources while 8.8% didn't and 1.8% was not sure. This shows that the majority of the libraries are providing electronic resources to its users for study, teaching and research.

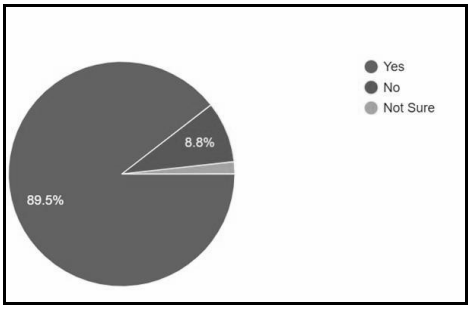

Figure 1: Availability of Remote Access to Access the Electronic Resources

From the Status of collecting personal information in Figure 2 it is found that 93% of the libraries collect personal information from the users to provide the services while 7% do not collect user personal information. It becomes necessary for the libraries to collect personal information of the users to provide facilities and services anytime and from anywhere.

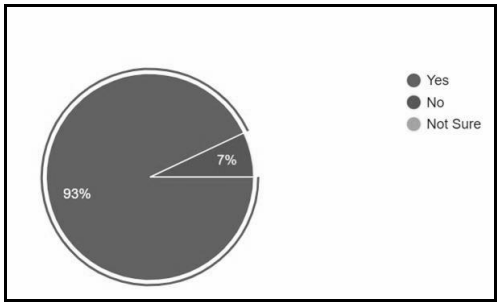

Figure 2: Status of collecting personal information

It was asked to the respondents to list out why the user information is collected and some of the major reasons received from the responses for collecting user personal information were -

Authentication or verification

- Call them for overdue reminders

- Contact them for informing them about library activities
- Create accounts for remote login
- Creating login, forget password options
- Feeding user data in Software
- For Circulation process, User Transactions, To send emails,
- Including in Nlist
- Library admin circulation purposes
- Library Dues
- Library Virtual Services
- Membership Creation
- Provide information about any new Library Services
- Provide information regarding resources for access
- Provide value added services
- Reach them in bulk
- Record for Students Connect
- Reminder for renewal, due date time, fine inform any notices , information etc.
- SDI, TOC
- Share current awareness service
- To generate e-certificates
- To get in touch with them in case of any discrepancy
- To register for NDL

It has become the need of the hour to incorporate user information in the library database to provide access to online resources. From the responses and as is seen in figure 3 it is found that 73.7% libraries are using user information to give them benefit of the e-resources available with the library while 26.3% are not collecting user information. This indicates that libraries may have other ways to provide online resources access to its users.

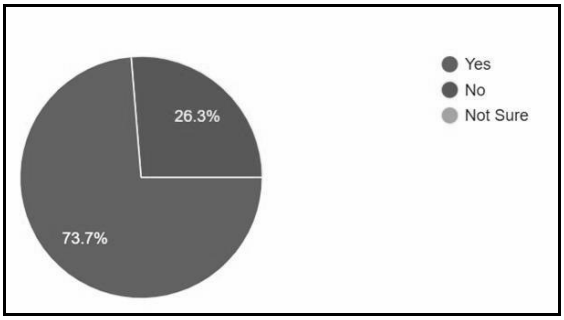

Figure 3: Use of user information in providing online access information about e-resources

Further it is noticed from figure 4 that 33.3% provide user data on OPAC, website or any discovery platform to access electronic resources while 66.7% don't provide user data on OPAC, website or any discovery platform may be due to security issues and have alternate solutions for access.

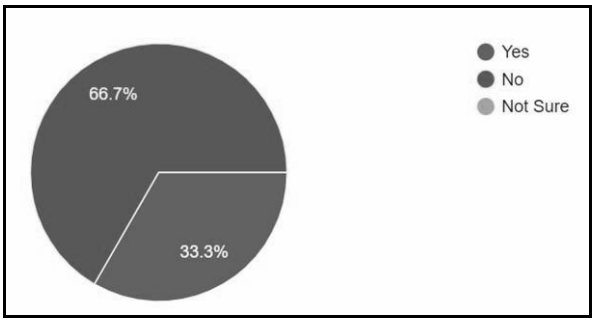

Figure 4: Availability of user data on OPAC, Website or Discovery Platform

In continuation, figure 5 indicates that 38.6% share user information with the third parties for providing online access to e-resources while 61.4% don't. This reveals that the remote access or use of discovery tools is still not popular among libraries. Few who share user data with third party are doing so for the benefit of users and help them to enhance knowledge from anywhere and anytime.

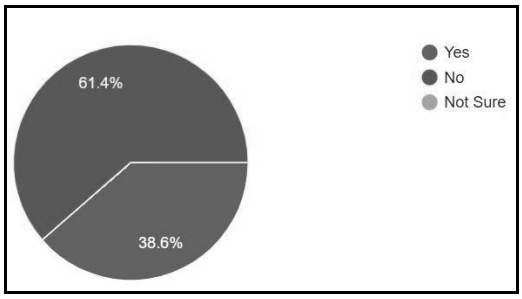

Figure 5: Sharing user information with the third parties for providing online access to e-resources

As seen from the above discussion, the majority of the libraries are not keen on sharing user personal information. Hence the respondents were asked whether they find risk involved in sharing user data and it was found from figure 6 that the 26.3% did not feel so. This indicates that these libraries are concerned about user personal data and are taking care to maintain privacy before sharing on any platform. It is further seen that 56.1% responded that there is risk involved and 17.5% are not sure about it.

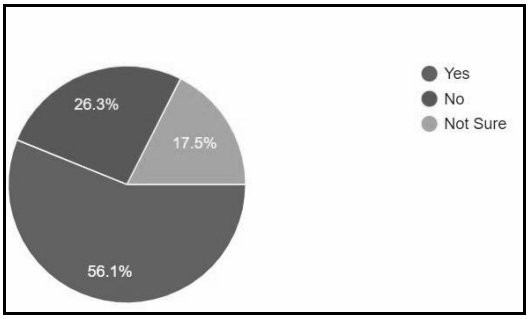

Figure 6: Opinion on risk involved in using user personal data which is vulnerable to theft

Due to majority responses on high risk involved in sharing user information, the risk faced or the risk likely to exist with user information were found as below -

- Breach of privacy
- Fraud calls
- Misuse of information
- Monetary fraud

- Online fraud
- Unethical activities
- Unwanted messages

To nullify the risk of sharing user information and at the same time to provide access to electronic resources remotely or use of other platforms for library services, security measures highlighted by some of the respondents are - Create E mail with registered domain

- Managing all data on own
- Share only with authenticate parties like INFLIBNET or NLIST
- Share with third party only with proper agreement

It was found from figure 7 that only 15.8% of the respondents delete user data after the user leaves the institution while 36.8% deactivate the user data. This is a good practice followed in order to ensure that there is no privacy breach of user data. However, 49.1% respondents are putting user data at risk as the data stays as it in their system. This could lead to any type of threat which should be thought of by the libraries.

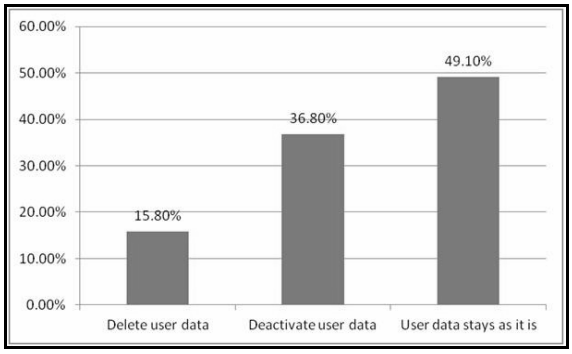

Figure 7: Status of user data when user becomes an alumni

It is necessary for the libraries to develop some rules in order to tackle user data safely. In view of this figure 8 indicates that 85.7% don't have guidelines, 8.9% have guidelines while 5.4% are not sure. Majority of the libraries need to think seriously about developing user privacy guidelines to keep user data safe and risk free. Those who have drafted guidelines have created Library Policy (Rules/Regulations) pamphlets for distribution among the students while the other has given remote access only through official / institutional email id and the same get deactivated at the end of the course period.

Looking at the criticality of maintaining privacy of user data, it becomes necessary for the libraries to prepare strong and robust user privacy policy or guidelines for the library. From figure 8 it is seen that, 8.9% of the respondents understand the need for the same which is why they have some rules set for user privacy. However larger libraries that is 85.7% do not have a user privacy policy while 5.4% are not sure. This calls for a major awareness among libraries to prepare and make available the user privacy policy.

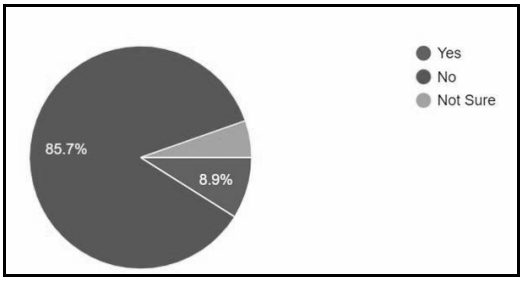

Figure 8: Availability of User Privacy Policy or Guidelines in the Library

Only having guidelines and not able to implement or sustain it is another issue. It was therefore found from the respondents that if they had a user privacy policy then whether they conduct a privacy audit? It was found that 5.3% responded are conducting the privacy audit while 86% do not do it and 8.8% are not sure about it.

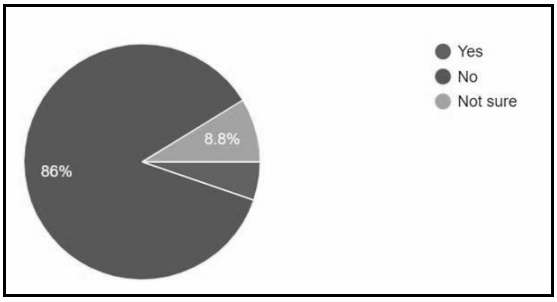

Figure 9: Privacy Audit Conducted

Measures taken to keep user data secured as received from responses are -

- Automatic suspension of official ids after user leave the institution
- Daily back-up of the software, Computer
- Data is stored in the ms word file format protected by password
- Data will not be shared with third party
- Deleting the data after the course time
- Library never disclosed the user's data to any other person or outside the organization or with external agencies or through any media
- Strictly informed library staff not to share/provide user data, especially mobile number, with anyone.
- To emphasize ethical values among library staff and instructions given to library staff for not sharing the user data
- User data access is provided only to the librarian or incharge of the circulation section (all staff cannot access) that helps in fixing the accountability.
- User Data Secured in College Office
- Users data on server and only Librarian have access right
- Using this data only for official purposes.
- How does library maintain the confidentiality of user personal data
- Answer to the queries only through the official desktop in the library.
- By giving unique number or library card number to all users
- Create safe user data files for concern course duration and then dissolve it permanently.
- Data displayed on admin login only.

- Follow ethical practices
- Only Librarian have access right and password protected
- Password Protected
- privacy policy is followed by staff
- User data is kept confidential
- User data is shared only with trusted third party
- Users data on server
- It was found that privacy awareness drives are not conducted for library staff and users. However, awareness practices are followed by college and library by always conducting awareness programmes regarding the security concern. Library staff is strictly instructed not to share the user data and keep it safe as it may lead to unnecessary intruding in the privacy of the users.

SUGGESTIONS

Important points that were highlighted from the study were -

- Institutions can follow a single card system for many purposes to avoid many duplication of data and in turn it will respect privacy
- Libraries need to implement proper policies, procedures and infrastructure to handle data security and maintain regulations around user privacy.
- Maintain trust between Librarian and the library users.
- Establish a library privacy policy of a library website, social media site, OPAC or discovery service.
- Clear third party privacy agreement and terms for users
- Limit the amount of personal information collected about users. Provide users with information on how it may be used.
- Provide training on privacy awareness to library staff and understanding of best practices for safeguarding user privacy.
- Privacy literacy to users by informing users about privacy of their data and effective strategies made by libraries to protect it

CONCLUSION

User privacy is a crucial issue in today's digital age. With the rise of technology and the internet, more personal information is being shared online, making it vulnerable to threats and misuse.

One of the biggest concerns with user privacy is the collection and sharing of personal data. Another concern with user privacy is the lack of control that users have over their personal information. Many libraries share user data with third parties without their consent, and users are often not aware of this sharing.

To protect user privacy, it is important to be transparent about their data collection and sharing practices. Users should be made aware of what data is being collected and how it is being used, and should have the option to opt out of data collection or sharing. Additionally, libraries should have robust security measures in place to protect user data from threats.

It's important to acknowledge that user privacy is a shared responsibility between libraries and individuals, and that it's important to continuously educate about the importance of user privacy.

REFERENCES

[1] IFLA.2015. https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment/Governing Board. (*Retrieved on March 31, 2025*)

[2]American Library association code of ethics. 2008. https://www.ala.org/advocacy/intfreedom/privacyconfidentiality.(*Retrieved on March 31, 2025*)

[3] Kuzma (J). European digital libraries: web security vulnerabilities. *Library Hi Tech*. 28, 3; 2010, Sep, p402-13. DOI: 10.1108/07378831011076657. (*Retrieved on April 2, 2025*)

[4] Devi (S S). Academic importance of social networking sites: Usage and awareness by the students of Manipur University. In : SINGH (S KR), BRAHMA (S), DEKA (P KR), & SINGH (I) Eds. *1st International Conference on Transforming Libraries*. 2017. MRB Publishers; Guwahati, India: p27–41.

[5] Kritikos (K), and Zimmer (M). Privacy policies and practices with cloud-based services in public libraries: An exploratory case of BiblioCommons. *Journal of Intellectual Freedom and Privacy*. 2, 1; 2017, July, p24-37. DOI: 10.5860/jifp.v2i1.6252. (*Retrieved on April 2, 2025*)

[6] Marden (B). The path to creating a new privacy policy: NYPL's Story. *Journal of Intellectual Freedom and Privacy*. 2, 1; 2017, Spring, p5-7. DOI: https://doi.org/10.5860/jifp.v2i1. (*Retrieved on March 31, 2025*)

[7] Pekala (S). Privacy and user experience in 21st century library discovery. *Information Technology and Libraries*. 36, 2; 2017, June, p48-58. DOI: 10.6017/ital.v36i2.9817. (*Retrieved on April 2, 2025*)

[8] Yoose, (B). Balancing privacy and strategic planning needs: A case study in de-identification of patron data. *Journal of Intellectual Freedom and Privacy*. 2, 1; 2017, Spring, p15-22. DOI: https://doi.org/10.5860/jifp.v2i1. (*Retrieved on March 31, 2025*)

[9] Wu (Z). An approach for the protection of users' book browsing preference privacy in a digital library. *The Electronic Library*. 36, 6; 2018, Oct, p1154-66. DOI: 10.1108/EL-07-2017-0162. (*Retrieved on April 2, 2025*)

[10] Thomchick (R), and Nicolas-Rocca (T. S). Application level security in a public library: A case study. *Information Technology and Libraries*. 37, 4; 2018, Dec, p107–18. DOI:10.6017/ital.v37i4.10405. (*Retrieved on March 31, 2025*)

[11] Lamanna (T). Public libraries leading the way on educating patrons on privacy and maximizing library resources. *Information Technology and Libraries*. 38, 3; 2019, Sep, p4-7. DOI: 10.6017/ital.v38i3.11571. (*Retrieved on March 31, 2025*)

[12] Maceli (M). Librarians' mental models and use of privacy-protection technologies. *Journal of Intellectual Freedom and Privacy*. 4, 1; 2019, Spring, p18-32. DOI: https://doi.org/10.5860/jifp.v4i1.6907. (*Retrieved on March 31, 2025*)

[13] Nicolas-Rocca (T), & Burkhard (R). Information security in libraries: Examining the effects of knowledge transfer. *Information Technology and Libraries*. 38, 2; 2019, June, p58-72. DOI: https://doi.org/10.6017/ital.v38i2.10973. (*Retrieved on March 31, 2025*)

[14] Katulić (A), Katulić (T) and Grgić (I H). Application of the principle of transparency in processing of European national libraries patrons' personal data. *Digital Library Perspectives*. 38,4; 2022, Feb, p399-411. DOI: 10.1108/DLP-11-2021-0097. (*Retrieved on April 2, 2025*)
