ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Reader Privacy Under the Digital Personal Data Protection Act, 2023: Contextual Integrity and the Obligations of Indian Academic Libraries

Dheeraj[1], Dr. Sapna Sharma[2]

[1]Research Scholar, Department of Library and Information Science, Swami Vivekanand Subharti University, Meerut, Uttar Pradesh, India

[2]Assistant Professor, Department of Library and Information Science, SVSU, Meerut

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150700155

Received: 13 August 2026; Accepted: 19 August 2026; Published: 25 August 2026

ABSTRACT

The Digital Personal Data Protection Rules, 2025, notified in November 2025, brought India's first comprehensive data protection statute into operation, with full compliance required by May 2027. Every academic library in India is a processor of digital personal data on a substantial scale, and most are constituent units of institutions that will be data fiduciaries under the Act, yet the professional literature contains almost no analysis of what the statute requires of them. This paper provides that analysis. It applies Nissenbaum's theory of contextual integrity, together with the proportionality standard established in Puttaswamy, to argue that library records are not simply personal data among other categories but records of intellectual inquiry, whose disclosure produces a chilling effect that a consent-based compliance regime does not by itself prevent. The method is documentary policy and legal-instrument analysis, conducted through a transparent selection protocol yielding a corpus of 81 documents. The paper develops a systematic inventory of the personal data processed by a typical Indian academic library across four categories, maps each category against the requirements of the Act, and analyses four hard cases: users under the age of eighteen, where section 9 forbids the tracking and monitoring of behaviour despite consent; federated authentication under the One Nation One Subscription scheme, which hands over institutional identity to commercial publishers; vendor and publisher analytics, where the library asserts it has no control over data it has caused to be created; and closed-circuit television and biometric attendance, where a proportionality analysis is necessary and is not often conducted. It is argued that the Act protects library users less than the professional standards of IFLA and the American Library Association, that its amendment of the Right to Information Act weakens rather than strengthens accountability, and that compliance alone will not discharge the profession's obligation. Twelve recommendations follow.

Index Terms: Digital Personal Data Protection Act; reader privacy; contextual integrity; academic libraries; data protection; intellectual freedom; library records; India.

INTRODUCTION

A library records what its users read. It does so incidentally, as a by-product of lending books and providing access to electronic resources, and for most of the history of the institution those records were of little interest to anyone outside it. That condition no longer holds. An integrated library system retains a complete borrowing history; a discovery layer logs every search; a publisher platform records every article downloaded, by which user, from which institution, at what hour; a turnstile logs entry; a camera records the reading room; and in a growing number of Indian institutions a fingerprint or an iris scan is required to enter at all. The aggregate is a detailed and durable account of what a particular person has been thinking about.

The professional response to this condition is long established internationally. The IFLA Statement on Privacy in the Library Environment, endorsed in August 2015, records that library and information services should respect and advance privacy both as a matter of practice and as a principle, and the IFLA Code of Ethics

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

identifies respect for personal privacy, protection of personal data and confidentiality in the relationship between the user and the service as core commitments. In the United States the position is older still: Article XI of the 1939 Code of Ethics for Librarians asserted an obligation to treat as confidential any private information obtained through contact with library patrons, and Article III of the current Code of Ethics of the American Library Association restates it.

India has had no comparable professional instrument and, until recently, no general legal one either. That has now changed. The Digital Personal Data Protection Act, 2023 received Presidential assent on 11 August 2023, and the Digital Personal Data Protection Rules, 2025 were notified in November 2025, bringing the statute into operation with a phased implementation window and full compliance required by 13 May 2027. The penalties are substantial, extending to two hundred and fifty crore rupees for a failure to maintain reasonable security safeguards. Every institution that operates a library, and every library that operates an integrated library system, now falls within a binding statutory regime whose requirements the profession has barely begun to consider.

This paper undertakes that consideration. It has three purposes: to establish what the Act and the Rules require of an academic library in practice; to argue that compliance, while necessary, is not sufficient, because a consent-based statute does not by itself protect the particular interest that library records engage; and to indicate what Indian academic libraries and the profession that serves them should now do. The argument is developed through the theory of contextual integrity, which explains why a data flow may be perfectly lawful and nonetheless constitute a privacy violation.

PRIOR LITERATURE AND THE RESEARCH GAP

Library privacy as a professional tradition

The international literature on library privacy is substantial and is grounded in the connection between confidentiality and intellectual freedom. The American Library Association's interpretation of Article VII of the Library Bill of Rights states the connection directly: the absence of privacy and confidentiality has a chilling effect on users' selection of, access to and use of library resources, and users have a right to be free from unreasonable intrusion into or surveillance of their lawful library use. The materials treated as confidential extend well beyond the borrowing record to online search histories, database search records, integrated library system records, interlibrary loan records and reference interviews. In the United States this professional norm is reinforced by statute in almost every jurisdiction. The IFLA Statement of 2015 generalises the position internationally and situates it against both governmental surveillance and routine commercial data collection by the platforms through which libraries now deliver content.

The Indian legal literature

The Indian legal literature on the DPDP Act is by now considerable, and analyses of particular provisions are numerous: the consent architecture, the children's data provisions of section 9, the research exemption in section 17(2)(b), the amendment of the Right to Information Act by section 44(3), and the phased compliance obligations introduced by the 2025 Rules. Sectoral analyses have appeared for health, finance, education technology and employment. This literature is written by and for lawyers and compliance professionals, and it does not address libraries.

The gap

Four gaps follow. First, no published study systematically inventories the personal data processed by an Indian academic library and maps it against the obligations of the Act, with the consequence that a librarian seeking to understand her position has no document to consult. Second, no study applies a privacy-theoretical framework to Indian library data; the professional discussion of privacy in Indian librarianship, where it exists, is largely confined to the ethics of confidentiality without engaging the structure of the flows involved. Third, the interaction between the Act and the national access infrastructure has not been examined, although federated authentication under the One Nation One Subscription scheme transmits institutional identity to commercial

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

publishers as a matter of routine design. Fourth, no analysis compares the protection the Act affords library users against the protection that international professional standards would require, which is the comparison that determines whether compliance is sufficient.

This paper addresses those four gaps. Its contribution lies in combining a theoretical framework suited to the

analysis of records, a systematic data inventory mapped to statutory obligation, an analysis of four hard cases specific to Indian library practice, and an evaluation of the statute against professional norms.

THEORETICAL FRAMEWORK

Contextual integrity

The framework adopted here is Nissenbaum's theory of contextual integrity, which holds that privacy is neither secrecy nor control over information as such, but the maintenance of appropriate information flows. Every social context carries norms governing what information moves, about whom, to whom, and under what conditions of transmission. A flow that conforms to the norms of its context preserves contextual integrity; a flow that departs from them violates it, whether or not the information was secret and whether or not consent was obtained.

The theory is unusually well suited to library records. The context of the library carries an established norm: a user consults material in order to inquire, and the record of that consultation exists to return the book and not to characterise the reader. The transmission principle is confidentiality. When the same record moves into another context, an institutional disciplinary proceeding, a police inquiry, a publisher's recommendation engine, an accreditation return, the norms governing it are entirely different, and the consequences for the user are of a different order. Figure 1 sets out the structure.

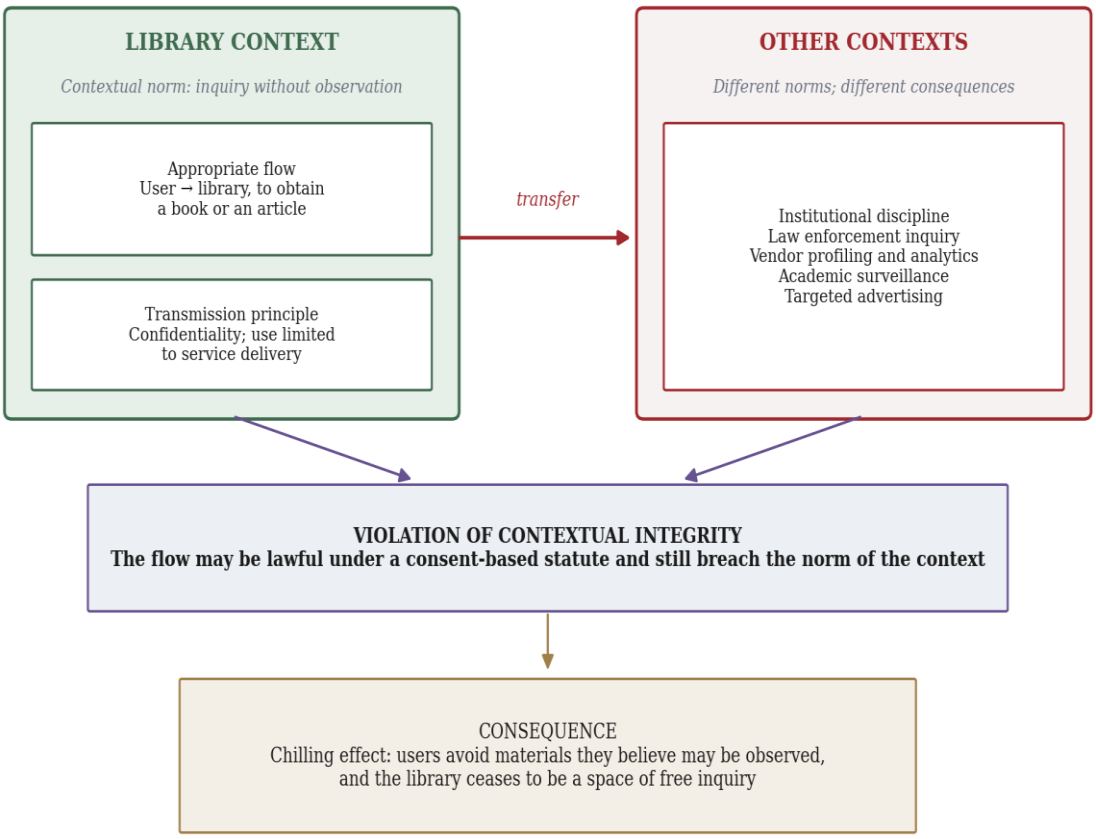

Figure 1. Contextual integrity applied to library data flows.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Two implications follow, and they organise the analysis. First, lawfulness and appropriateness are distinct. A library may obtain valid consent to share usage data with a publisher, satisfy every requirement of the Act, and still violate the contextual norm, because a user asked at the point of enrolment to accept a bundled privacy notice is not thereby making a considered judgement about the onward transmission of her reading history. Second, the harm at issue is not primarily embarrassment or financial loss but the chilling effect: a user who believes her consultations are being observed will avoid the material she thinks might attract attention, and the library ceases to be a place of inquiry while continuing to function perfectly well as a place of lending.

The Indian constitutional standard

Contextual integrity provides the analytical vocabulary; the Indian constitutional law provides the criterion with reference to which specific violations should be justified. In Justice K. S. Puttaswamy v. Union of India (2017) the Supreme Court held privacy to be a fundamental right under Article 21, and established that an intrusion must satisfy a test of legality, legitimate aim, proportionality and procedural safeguards. The proportionality limb is the operative one for library practice: a measure must be suitable to its aim, necessary in the sense that no less intrusive alternative would serve, and balanced in its effects. The DPDP Act is the statutory expression of the Puttaswamy right, and the two are used together here: the Act establishes what a library must do, and the proportionality standard establishes whether a particular practice, most obviously biometric attendance and continuous video surveillance, is justified at all.

OBJECTIVES, METHOD AND ANALYTICAL PROCEDURE

Objectives

The study pursues six objectives:

1. To establish the legal position of the academic library under the DPDP Act, 2023 and the DPDP Rules, 2025;
2. To construct a systematic inventory of personal data processed in a typical Indian academic library;
3. To map each category of data against the obligations of the Act and to identify where current practice is likely to be non-compliant;
4. To analyse four hard cases in which the application of the Act to library practice is contested or unclear;
5. To assess the protection afforded by the Act against international professional standards for library privacy;
6. To specify the resulting obligations for institutions, libraries and the profession.

Research design

The study employs qualitative documentary analysis of legal and policy instruments together with professional standards. No primary data were collected and no institutional practice was observed. The paper is an analysis of what the instruments require and of how they engage library operations; it is not, and does not present itself as, legal advice, and the interpretation of contested provisions offered here is an academic reading advanced for discussion.

Document selection protocol

Searches were conducted between June and August 2026 across three source classes. Statutory and regulatory instruments comprised the DPDP Act, 2023, the DPDP Rules, 2025 and their schedules, the draft Rules of January 2025, the Right to Information Act, 2005 as amended, and relevant Ministry of Electronics and Information Technology material. Peer-reviewed literature was retrieved from Scopus, Web of Science, LISTA and Google Scholar using the terms ‘library privacy’, ‘reader privacy’, ‘patron confidentiality’, ‘contextual integrity’, ‘data protection library’, ‘GDPR library’ and ‘DPDP Act’, with no date restriction for the theoretical literature and a 2023 to 2026 restriction for material on the Indian statute. Professional standards and commentary comprised IFLA and ALA instruments, legal commentary on the Act, and reportage. Screening

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

proceeded on title and abstract and thereafter in full text, with exclusions where a document had no bearing on library or educational contexts, duplicated an included source, was purely derivative, or was unretrievable. Figure 2 sets out the procedure, which yielded a corpus of 81 documents.

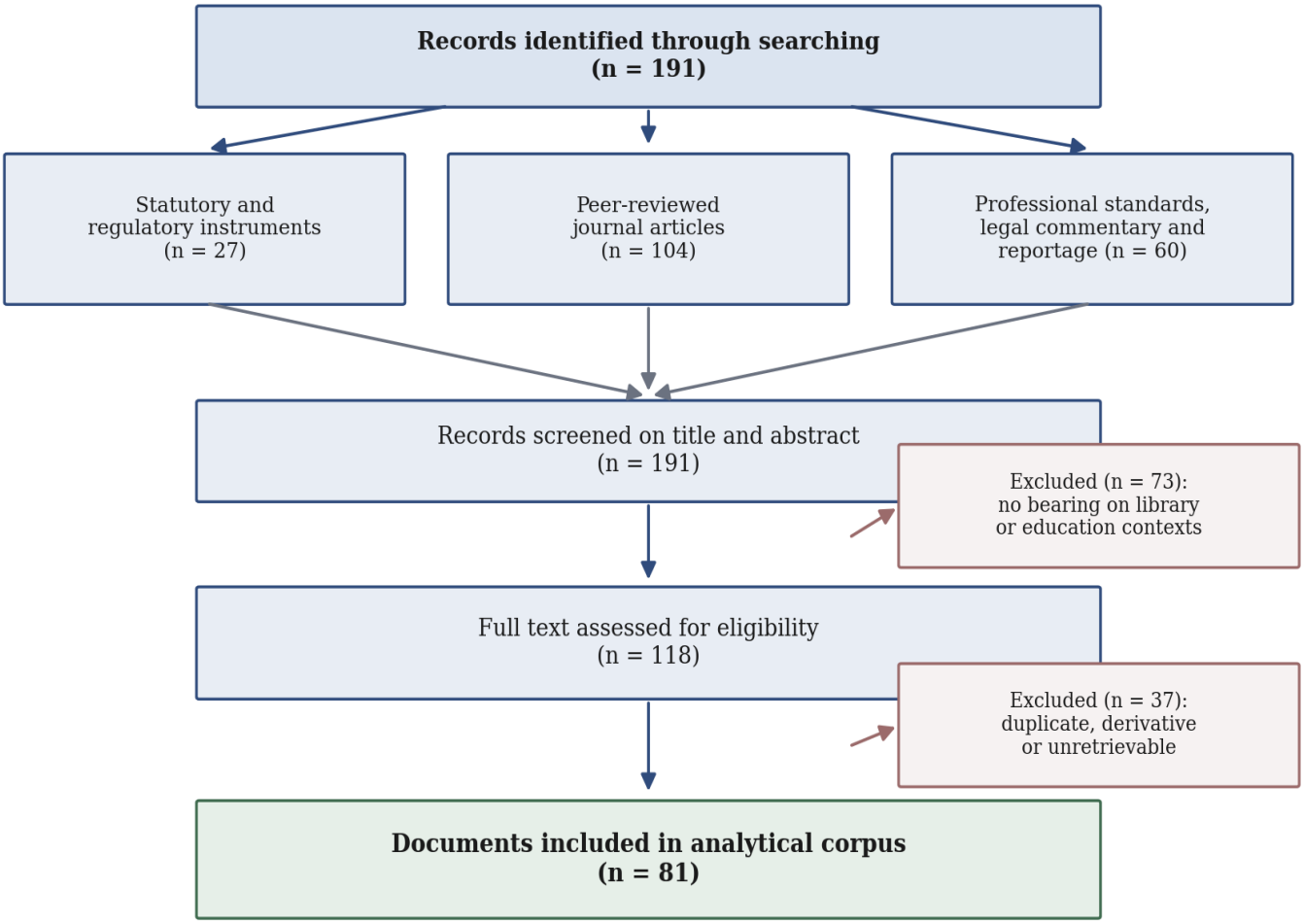

Figure 2. Document identification, screening and inclusion procedure.

Coding

Coding was deductive, using categories derived from the framework and from the structure of the statute. Table 1 presents the scheme.

Table 1. Deductive coding scheme.

Code	Category	Indicative content coded
LEG	Legal instrument	Provisions of the Act and Rules; definitions; obligations; exemptions; penalties
INV	Data inventory	Categories of personal data processed in library operations
FLO	Data flows	Transmission to processors, publishers, institutional units and third parties
CHL	Children’s data	Provisions and practices concerning users below eighteen years

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

PRO	Proportionality	Surveillance, biometrics and the justification of intrusive measures
NRM	Professional norms	IFLA, ALA and comparable instruments on library privacy
CMP	Comparative	GDPR and other regimes as they bear on library practice
GAP	Divergence	Points at which statutory protection falls short of professional norms

Validity and source appraisal

Documents were appraised against Scott's (1990) criteria of authenticity, credibility, representativeness and meaning. Statutory provisions were read in the primary instrument rather than through secondary description. Where commentary diverges, the divergence is reported rather than resolved. One instance is material to this paper: the standards contemplated by section 17(2)(b) for research, archiving and statistical processing were widely described during 2024 and early 2025 as not yet prescribed, and some commentary published as late as early 2026 continued to describe them as unpublished, whereas the Rules notified in November 2025 address the exemption and refer to standards set out in a schedule. Libraries and archives relying on that exemption should therefore verify its current operation directly rather than through secondary sources, and this paper does not rest any conclusion on the exemption being available.

A second limitation of the source base should be recorded. A considerable volume of the accessible commentary on the Act is produced by compliance vendors and law firms with a commercial interest in the perception of regulatory burden. Such material was used for orientation and for identifying provisions, and factual claims drawn from it were traced to the instruments themselves.

Positionality

The first author is a doctoral researcher in library and information science at an Indian state university whose research concerns the use of digital resources by students in state-sector colleges, and who is himself a library user subject to the systems analysed here. Neither author is legally qualified. The paper is offered as professional and scholarly analysis of a legal instrument as it bears on library practice, and institutions should obtain their own legal advice before adopting the positions advanced in Sections 6 to 8.

Limitations

- No survey of Indian library practice was conducted; statements about current practice are inferential and are presented as expectations to be tested rather than as findings.
- The inventory in Section 6 describes a typical academic library and will require adaptation to the circumstances of individual institutions.
- The law is recent and untested; no ruling of the Data Protection Board had been issued at the time of writing, and several of its provisions await authoritative interpretation.
- The analysis of federated authentication in Section 7.2 rests on the published architecture of the access system rather than on the underlying agreements, which are not in the public domain.

THE LEGAL FRAMEWORK

From Puttaswamy to the Rules

The sequence is set out in Figure 3. In 2017 the Supreme Court recognised informational privacy as a constitutional right protected by Article 21. Legislation was drafted over the six years that followed. The Act received assent in August 2023 but remained largely inoperative until subordinate legislation was made; draft Rules were issued for consultation in January 2025, and the final Rules were notified in November 2025 after consultations held in several cities with industry, civil society and government. Implementation is phased: the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

procedural provisions and the establishment of the Data Protection Board took effect immediately, the consent manager provisions after one year, and the substantive obligations of data fiduciaries at the end of an eighteen-month period, with full compliance required by 13 May 2027.

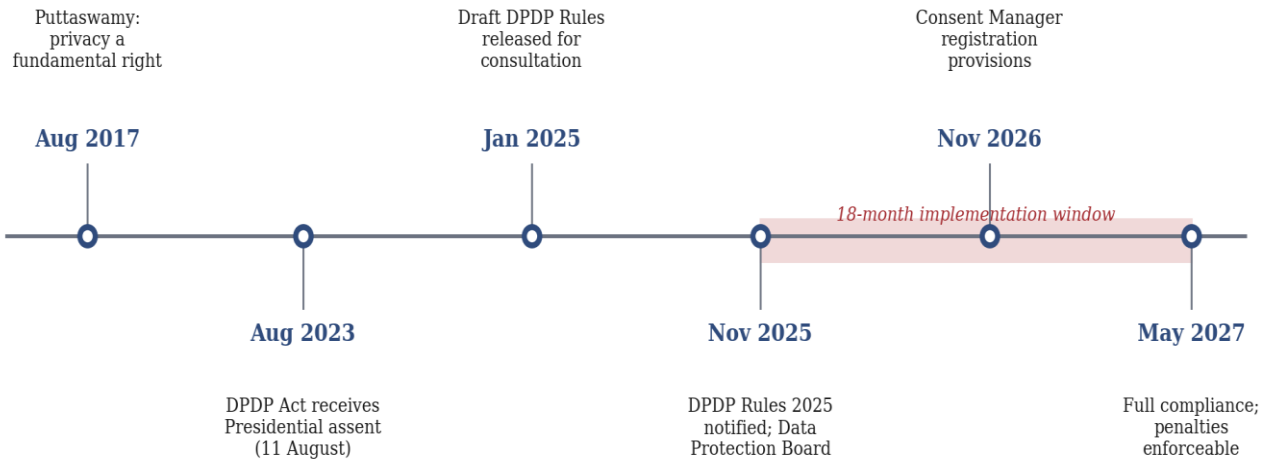

Figure 3. From Puttaswamy to full compliance: the chain of Indian data protection law.

The library's position under the Act

Three definitional points determine the library's position. The data principal is the individual to whom the personal data relates: for present purposes the student, research scholar, faculty member or visiting reader. The data fiduciary is the person who alone or with others determines the purpose and means of processing. In most Indian arrangements the fiduciary will be the parent institution rather than the library as such, since the library is not ordinarily a separate legal person; but it is the library that determines what is collected, retained and disclosed in respect of library services, and the obligations therefore bite on library practice whoever bears them formally. The data processor is a person who processes on behalf of the fiduciary, which describes the integrated library system vendor, the discovery service, the RFID supplier and the cloud host, and the fiduciary remains responsible for their conduct.

The Act rests on a consent-based architecture supplemented by specified legitimate uses. It imposes obligations of notice, purpose limitation, data minimisation, accuracy, retention limitation, security safeguards, breach notification and grievance redressal, and it confers on the data principal rights of access, correction, erasure and nomination. Entities designated as significant data fiduciaries carry additional duties, including periodic data protection impact assessment and independent audit. Penalties are graduated, the highest attaching to a failure to implement reasonable security safeguards.

One structural feature deserves emphasis because it shapes the whole of the analysis that follows. The Act does not create a category of sensitive personal data. Under the European regime, and under the Indian draft legislation that preceded this Act, certain categories attract heightened protection. Under the DPDP Act a record of the books a person has borrowed and a record of her postal address are subject to the same regime. From the standpoint of contextual integrity this is a significant omission, because the two records engage entirely different norms and produce entirely different consequences when they move.

THE LIBRARY AS PROCESSOR: A DATA INVENTORY

Compliance begins with knowing what is held. No inventory of library personal data has been published for the Indian context, and the following is offered as a working instrument. Four categories are distinguished by the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

manner of collection and by the character of the interest engaged. Figure 4 presents the structure together with the onward flows.

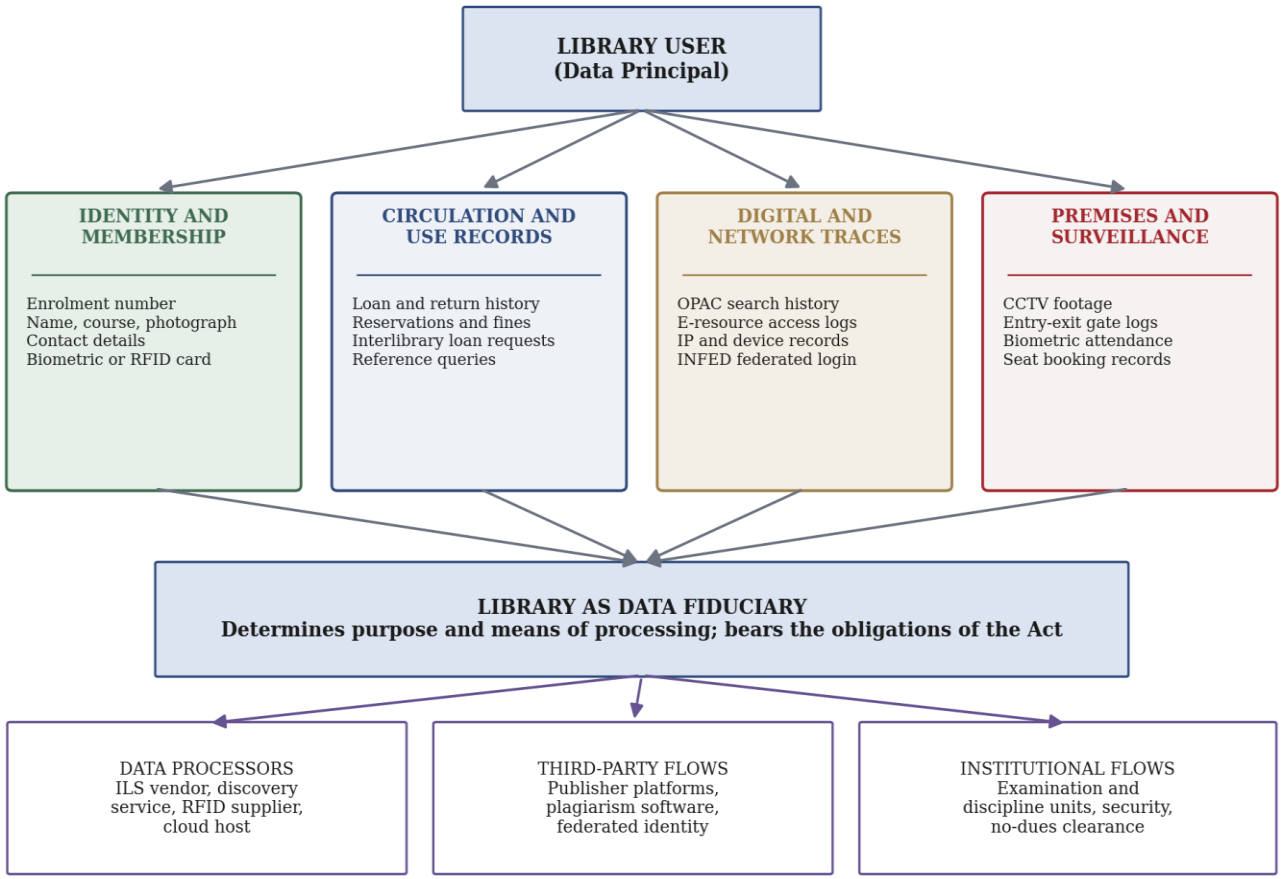

Figure 4. Categories of personal data processed in a typical Indian academic library, with onward flows.

Identity and membership data are collected at enrolment and are the least contentious: name, enrolment number, course and department, contact details, photograph and, increasingly, a biometric template or card identifier. Circulation and use records are generated by service delivery: loans, returns, reservations, fines, interlibrary loan requests and reference queries. Digital and network traces are generated automatically: catalogue and discovery searches, electronic resource access logs, IP and device records, proxy and federated authentication events. Premises data are generated by the building: video surveillance, entry and exit logs, biometric attendance and seat reservation systems.

The categories differ sharply in the interest they engage, and it is the second and third that carry the intellectual-freedom interest with which this paper is concerned. A borrowing history and a search log are not administrative records that happen to concern a person; they are records of what that person has been trying to find out. Table 2 maps the inventory against the principal obligations.

Table 2. Library personal data mapped to obligations under the Act.

Category	Examples	Interest engaged	Principal obligation	Common current practice

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Identity and membership	Name, enrolment number, course, contact details, photograph	Ordinary personal data	Notice; purpose limitation; accuracy; security	Collected at enrolment; often retained indefinitely
Biometric identifiers	Fingerprint or iris template for entry or attendance	Bodily integrity; irrevocable if breached	Proportionality; security; explicit purpose	Adopted for convenience; proportionality rarely assessed
Circulation records	Loan history, reservations, fines, interlibrary loan	Intellectual freedom	Purpose limitation; retention limitation; erasure	Full history retained after return; no deletion schedule
Reference and query records	Reference interviews, research consultations, request forms	Intellectual freedom; often acutely sensitive	Minimisation; confidentiality	Recorded informally; rarely governed by policy
Search and discovery logs	OPAC and discovery searches, session records	Intellectual freedom	Minimisation; retention limitation	Retained by default in system logs
E-resource access logs	Downloads by user, title, time; publisher-side records	Intellectual freedom; transmitted outside the institution	Purpose limitation; processor control; notice	Generated on publisher platforms; not governed by the library
Premises surveillance	CCTV footage, entry and exit logs, seat booking	Freedom from observation	Proportionality; retention limitation; notice	Continuous recording; retention undefined

FOUR HARD CASES

Users below eighteen years of age

The Act defines a child as any individual below eighteen years, a uniform national threshold higher than the European standard of thirteen to sixteen and the United States standard of thirteen. A data fiduciary must obtain the verifiable consent of a parent or lawful guardian before processing the personal data of a child. More important for library practice, the Act prohibits the tracking and behavioural monitoring of children and targeted advertising directed at them, and that prohibition cannot be lifted by parental consent. The Act empowers the Government to exempt classes of fiduciary or purpose, and educational institutions have been discussed in this connection, so the precise application to a college library must be verified against the Rules as they presently stand.

The implications are far-reaching and appear to be entirely unexamined in Indian library practice. Seventeen-year-olds form a regular part of undergraduate cohorts, and school libraries serve minors exclusively. On a straightforward reading, a library serving such users may not operate reading recommendation systems that profile individual borrowing behaviour, may not use analytics to track individual patterns of use over time, and may not permit vendor systems to do so on its behalf. Features ordinarily regarded as service improvements, such as the recommendation engine in a discovery layer or the usage dashboard that identifies low-engagement students for intervention, become legally questionable where the user is seventeen. The requirement of verifiable parental consent poses a further practical difficulty, since a library enrolling an incoming undergraduate cohort would have to establish the age of part of that cohort and obtain parental consent on their behalf.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

It is worth noting that on this point the statute and the professional tradition coincide, and that the statute is in some respects the more stringent of the two. The Act's prohibition on the behavioural monitoring of minors gives legal force to what library ethics has long maintained.

Federated authentication and the national access infrastructure

The second case arises from India's own access architecture. Under the One Nation One Subscription scheme, access to publisher content operates through institutional IP recognition on campus and through federated authentication off campus, by which the user presents institutional credentials and the publisher platform is informed of the institution and of a persistent user identifier. The scheme is a considerable public achievement and this paper does not question it. But its design has a data protection consequence that has not been discussed.

In contextual integrity terms, the flow is straightforward to state: an individual's reading of specific scholarly articles is transmitted, in an identifiable or pseudonymous but persistent form, to a commercial entity outside India, which retains it under terms the individual has not seen and the library has not negotiated. The library is not the counterparty to the publisher agreements, which are concluded centrally, and cannot therefore impose the vendor conditions that the American Library Association recommends: retention of institutional ownership of user data, audit rights over vendor collection and retention, and a contractual bar on secondary use. The individual library is obliged under the Act to give notice of processing it does not control and cannot inspect.

This is not an argument against national licensing. It is an argument that a national licence should carry national data protection terms, and that the negotiation which secured reading access should also have secured the conditions on which reading is recorded. The point is timely: the agreements underpinning the scheme fall for renewal within the same period as the compliance deadline.

Vendor and publisher analytics

The third case generalises the second. Integrated library systems, discovery services, plagiarism detection software and publisher platforms all generate and retain records of individual use, and Indian libraries typically procure them on the vendor's standard terms. The library is nonetheless within the chain of responsibility: under the Act the fiduciary remains answerable for processing carried out on its behalf, and the defence that the vendor collects the data is not available.

Plagiarism detection deserves specific mention. Such systems receive the full text of student work, retain it in a permanent comparison corpus, and are frequently hosted outside India. The student is not consulted, and where consultation does occur the student is in no position to refuse, since submission is a condition of assessment. The Act raises, and leaves unanswered, the question whether consent obtained in such circumstances is meaningful.

Surveillance and biometrics

The fourth case concerns the area of Indian practice that has advanced most rapidly and been reflected upon least. Continuous video monitoring of reading rooms is now common, and biometric entry and attendance systems are becoming steadily more widespread. Both are ordinarily justified by reference to the security of stock and the prevention of unauthorised access.

Tested against the Puttaswamy standard, these justifications must satisfy proportionality, a test with three limbs. The measure must be suitable to its aim: video surveillance of a reading room does deter theft. It must be necessary, in the sense that no less intrusive measure would achieve the aim: for stock security, radio-frequency detection at exits achieves the purpose without recording who sat where and for how long, which is a strong indication that continuous internal surveillance is not necessary for that aim. And its effects must be balanced: a biometric template is irrevocable, so that a breach cannot be remedied by reissuing a credential, and the gravity of that risk is not proportionate to the convenience of automated attendance. A library that has adopted biometric entry because the campus adopted it, without conducting this analysis, has taken a constitutionally significant decision without recognising that it was doing so.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Figure 5 positions the four cases and the other principal processing activities by the risk they create for the user and the effort their remediation requires.

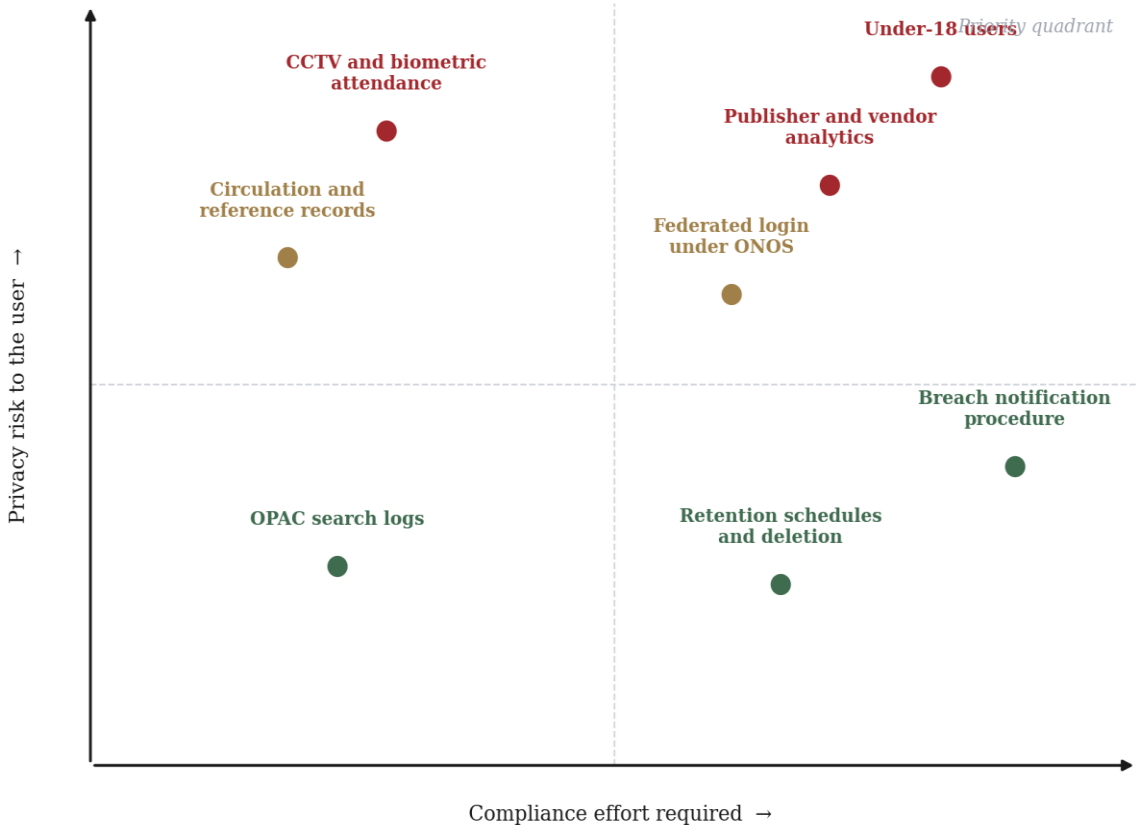

Figure 5. Library processing activities by privacy risk and compliance effort.

WHERE THE ACT FALLS SHORT OF PROFESSIONAL STANDARDS

The Act improves the position of Indian library users considerably, since their prior position was that no general data protection statute applied at all. It does not, however, deliver what the professional standards require, and four divergences are material.

No recognition of reading records as a distinct category

The Act creates no category of sensitive data and accordingly attaches no special protection to records of intellectual consultation. American state law and professional policy treat circulation records, search histories, interlibrary loan records and reference interviews as a class warranting specific confidentiality, and the ALA policy on confidentiality of library records recommends that such records be disclosed only pursuant to properly executed legal process and that libraries resist improper demands. The DPDP Act contains no equivalent. A library record is disclosable on the same footing as any other personal data, and the Act does not require legal process for institutional access to it.

Consent as a weak safeguard in an institutional setting

Consent presupposes a genuine freedom to refuse. A student cannot decline library membership, decline to use the campus authentication system or decline plagiarism screening and remain a student. Consent given in such circumstances is formally valid and substantively empty, and the Act, which depends heavily on consent, is silent on this asymmetry. Contextual integrity supplies a corrective: the question is not whether the user

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

consented but whether the flow conforms to the norms of the context, and a library should test itself against that question whatever consent it has obtained.

The amendment of the Right to Information Act

Section 44(3) of the Act amends section 8(1)(j) of the Right to Information Act, 2005 by removing the public interest override that previously qualified the exemption for personal information. The consequence is that information can be withheld as personal without the weighing of larger public interest that the earlier provision required. The provision has been widely criticised, and its bearing on libraries is specific and adverse: institutional information that a researcher might previously have obtained subject to a public interest test, including information about institutional data practices themselves, becomes harder to obtain. A statute that strengthens the protection of the individual reader while weakening the transparency of the institution has moved in two directions at once, and libraries, whose professional commitment is to access as well as to privacy, are placed on both sides of the shift.

The research and archiving exemption

Processing necessary for research, archiving or statistical purposes is exempted from significant parts of the Act, subject to the conditions that the data are not used to take a decision specific to a data principal and that prescribed standards are followed. For institutional repositories, digital archives and oral history collections the exemption is potentially important, and it is more explicit than the equivalent provisions in several other jurisdictions. Two cautions are nonetheless required. The exemption's scope has attracted criticism for breadth in the legal literature, and a library relying on it to justify indefinite retention of user data would be extending it well beyond its evident purpose. And the boundary between archiving in the public interest and record retention for institutional convenience is precisely the kind of distinction on which a library's position may turn.

Table 3. Protection of library users compared across three regimes.

Dimension	DPDP Act, 2023 (India)	GDPR (European Union)	Professional standards (IFLA, ALA)
Reading records as a category	No special category; treated as ordinary personal data	No specific category, but special categories exist and may be engaged by inference	Circulation, search, reference and interlibrary loan records treated as confidential by class
Basis of protection	Consent and defined legitimate uses	Six lawful bases; legitimate interests assessment	Professional duty independent of user consent
Children	Under 18; verifiable parental consent; tracking and behavioural monitoring prohibited	13 to 16 depending on Member State	Minors' privacy affirmed; balanced against guardian rights
Disclosure to authorities	No requirement of legal process specific to library records	Subject to lawful basis and safeguards	Disclosure only under properly executed legal process; resistance to improper demands recommended
Vendor conditions	Fiduciary responsible for processors; no library-specific terms	Processor contracts mandatory with specified content	Institutional ownership of user data; audit rights; bar on secondary use

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Transparency of the institution	RTI public interest override removed by section 44(3)	Not applicable	Openness about the library's own data practices

DISCUSSION: COMPLIANCE IS NOT THE STANDARD

The analysis supports a single organising conclusion. The Act establishes a floor, and the floor is welcome, but a library that treats compliance as the whole of its obligation will satisfy the statute and fail its users.

The reason is the one contextual integrity identifies. The Act regulates the lawfulness of flows; it does not ask whether a flow is appropriate to the context in which the information was generated. A library may retain a complete borrowing history indefinitely, provided it gives notice and states a purpose. It may disclose that history to a disciplinary committee. It may lawfully permit a publisher to build a profile of an individual reader, so long as this has been notified. None of these flows is prohibited by the statute, and every one of them breaches the norm that has governed the relationship between libraries and their readers since long before either the statute or the professional codes were written.

The remedy exists and is not new. It is already stated in the professional standards: minimise what is collected, retain nothing beyond the purpose the service requires, treat records of consultation as confidential by class rather than by consent, impose conditions on vendors regarding the handling of data, and resist disclosure otherwise than through proper legal process. What the Indian profession lacks is not the principle but an instrument. There is no Indian equivalent of the IFLA Statement adapted to Indian law, no model library privacy policy, and no professional guidance on any of the four hard cases examined above. The eighteen-month implementation window is the occasion for producing them, and roughly nine months of it remain.

There is a further consideration of professional interest. Data protection compliance is, in its operational substance, records management: knowing what is held, why, for how long, and who may see it. This is the historical competence of the library profession, and it is being assigned in most Indian institutions to information technology departments and legal cells. The librarian who can conduct a data inventory, write a retention schedule and assess a vendor agreement is performing a function the institution urgently requires and is unlikely to obtain elsewhere.

RECOMMENDATIONS

For institutions

1. Conduct a library data inventory using the categories set out in Section 6, recording for each category the purpose of collection, the retention period, the systems in which it resides and the parties to whom it flows.

2. Adopt a written library privacy policy, published to users, stating what is collected, why, for how long and under what circumstances it will be disclosed, and include the librarian in its drafting.

3. Conduct a documented proportionality assessment before deploying or continuing any biometric or continuous video surveillance system in a library, addressing suitability, necessity and balance, and record the less intrusive alternatives considered.

4. Establish and implement a retention schedule that severs the link between borrower and item on return, save where a fine or claim is outstanding, since a borrowing history retained after the transaction is complete serves no purpose the library can state.

5. Require, in all new procurement of library systems, contractual terms retaining institutional ownership of user data, prohibiting secondary use, permitting audit and specifying deletion on termination.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

6. Determine which library users are below eighteen years of age and establish a compliant process for them, including the suspension of individual behavioural profiling for that group.

For the national access architecture

1. Negotiate data protection terms centrally as part of the national subscription agreements, including limits on publisher retention of individual usage records, a prohibition on secondary use and profiling, and audit rights, so that individual institutions are not left answerable for flows they cannot audit.
2. Publish, in an accessible form, what personal data federated authentication transmits to publisher platforms and on what terms those data are retained.

For the profession and its associations

1. Publish an Indian statement on privacy in the library environment, adapting the IFLA Statement to the DPDP framework and addressing the four cases examined in Section 7.
2. Issue a model library privacy policy and a model retention schedule that institutions can adopt in full, since the absence of a template is the principal practical barrier to compliance in smaller institutions.
3. Incorporate data protection and privacy into library and information science education and continuing professional development, as the IFLA Statement recommends, so that the profession can supply the competence institutions now require.
4. Press for the recognition of records of intellectual consultation as a protected category, whether through subordinate rulemaking, through professional standards adopted by institutions, or ultimately through statute.

CONCLUSION

India now has a data protection statute, and every academic library in the country falls within it. The obligations are real, the timeline is short and the penalties are heavy. Libraries must therefore know what personal data they hold, why they hold it, for how long they retain it and to whom it is transmitted; at present most Indian academic libraries could not answer those questions. That is the compliance task, and it is urgent.

It is not, however, the whole of the obligation, and this paper has argued that the difference matters. A record of what a person has read is not an administrative record that happens to concern her: it is a record of her thinking, and it carries with it the norms of the context in which it was created. The Act does not recognise this. It creates no protected class for records of consultation, requires no legal process before their disclosure, and relies on a consent mechanism that means little when the person consenting cannot refuse and remain enrolled. A library may satisfy every provision of the statute and still permit its users' reading to be monitored, profiled and disclosed, and its users will adjust what they read in response. That adjustment is the harm, and it appears in no compliance audit.

What the statute does not supply, the professional standards do, and the Indian profession has not yet adapted them. There is no Indian statement on library privacy, no model policy and no guidance addressed to the conditions in which Indian libraries actually operate: undergraduate cohorts that include minors, national federated authentication transmitting reading behaviour to commercial publishers abroad, biometric access installed without any proportionality analysis, and plagiarism systems retaining student work indefinitely under foreign law. These are not hypothetical problems. They exist in most Indian institutions today, and the period available to address them is now short.

Two studies follow directly, and neither has been undertaken. The first is a survey of what Indian academic libraries actually collect and retain, without which the scale of the compliance gap remains unknown. The second is an assessment of what the national access infrastructure transmits to publishers, and on what contractual terms, which is a question of national rather than institutional interest and which no single library is placed to answer. Until both are carried out, the Indian library profession will be advising on a position it has not surveyed.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

REFERENCES

1. American Library Association. (2019). Privacy: An interpretation of the Library Bill of Rights. Chicago: ALA. https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy (accessed 12 August 2026)
2. American Library Association. (2021). Code of ethics of the American Library Association. Chicago: ALA.
3. American Library Association. (n.d.). Policy on confidentiality of library records. Chicago: ALA. https://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconfidentiality (accessed 12 August 2026)
4. American Library Association. (n.d.). State privacy laws regarding library records. Chicago: ALA. https://www.ala.org/advocacy/privacy/statelaws (accessed 12 August 2026)
5. Ayre, L. B., & Craner, J. (2018). Algorithms: Avoiding the implementation of institutional biases. Public Library Quarterly, 37(3), 341–347.
6. Bhattacharya, A. (2024). The Digital Personal Data Protection Act, 2023: An overview of the consent architecture. Indian Journal of Law and Technology.
7. Government of India. (2005). The Right to Information Act, 2005. New Delhi: Ministry of Law and Justice.
8. Government of India. (2023). The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). New Delhi: Ministry of Law and Justice.
9. Government of India. (2025). The Digital Personal Data Protection Rules, 2025. New Delhi: Ministry of Electronics and Information Technology.
10. International Federation of Library Associations and Institutions. (2012). IFLA code of ethics for librarians and other information workers. The Hague: IFLA.
11. International Federation of Library Associations and Institutions. (2015). IFLA statement on privacy in the library environment. The Hague: IFLA. https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment/ (accessed 12 August 2026)
12. Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
13. Lambert, A. D., Parker, M., & Bashir, M. (2015). Library patron privacy in jeopardy: An analysis of the privacy policies of digital content vendors. Proceedings of the Association for Information Science and Technology, 52(1), 1–9.
14. Magi, T. J. (2011). A content analysis of library vendor privacy policies: Do they meet our standards? College & Research Libraries, 71(3), 254–272.
15. National Information Standards Organization. (2015). NISO consensus principles on users' digital privacy in library, publisher, and software-provider systems. Baltimore: NISO.
16. Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–157.
17. Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford: Stanford University Press.
18. Press Information Bureau, Government of India. (2025, November 14). Digital Personal Data Protection (DPDP) Rules, 2025 [Press release]. New Delhi: PIB.
19. Rubel, A., & Zhang, M. (2015). Four facets of privacy and intellectual freedom in licensing contracts for electronic journals. College & Research Libraries, 76(4), 427–449.
20. Scott, J. (1990). A matter of record: Documentary sources in social research. Cambridge: Polity Press.
21. Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Oppenheim, C., & Hardy, R. (2003). User privacy in the digital library environment: An investigation of policies and preparedness. Library Management, 24(1–2), 44–50.
22. Zimmer, M. (2013). Patron privacy in the '2.0' era: Avoiding the Faustian bargain of library 2.0. Journal of Information Ethics, 22(1), 44–59.
23. Zimmer, M., & Tijerina, B. (2018). Library values and privacy in our national digital strategies: Field guides, convenings, and conversations. Milwaukee: University of Wisconsin-Milwaukee.