THE IMPACT OF DATA PRIVACY POLICIES AND DATA RIGHTS ON THE MODERN LIBRARY ECOSYSTEM

Ruma Kumari Singh
PhD Scholar, RTMNU, Nagpur
Email: ruma.rumi@gmail.com

Dr. Satyaprakash Nikose
Dept. of Library and Information Science
RTMU, Nagpur
Email: drsmnikose@gmail.com

Crossref DOI - https://doi.org/10.63665/rh.v7i1.53

Abstract :

Libraries have long been places where individuals might think freely. One of their most fundamental moral rules is to keep users' privacy safe. But the swift shift to digital library services, such cloud-based catalogues and biometric access management, has fundamentally transformed this. This article looks at the clash between modern data privacy laws (including GDPR, CCPA, and new digital rights frameworks) and how libraries work in real life. This article asserts that "privacy" has transitioned from a passive condition of anonymity to an active, resource-demanding service, as demonstrated by an analysis of vendor agreements, cybersecurity frameworks, and user conduct. The findings demonstrate that while customisation enhances user involvement, it simultaneously imposes obligations that require a thorough revision of library management practices.

Keywords : Data Privacy, Privacy laws, Digital Rights, Digital Libraries, Cybersecurity Frameworks

---

Introduction :

The Evolution of Libraries in a Data-Centric World :

Libraries have always had a special place in their communities. For generations, librarians have known that privacy is important for intellectual freedom to thrive. Readers should be able to explore ideas, access sensitive materials, and seek knowledge without worrying about being watched, judged, or having their information shared. This tradition, which comes from the American Library Association's founding principles and professional ethics codes, is very human: it is the idea that what we read, look for, and learn is fundamentally ours. Today, libraries are dealing with a strange situation that has never happened before. Digital transformation, which sped up a lot during the COVID-19 pandemic, has led to amazing new services like virtual reference services, real-time learning analytics, remote access to collections, and personalised discovery systems. But every new idea creates personal data. Every time you search a catalogue, log into a database, download an e-resource, use Wi-Fi, or chat online, you leave a digital footprint. At the same time,

governments all over the world are recognising data protection as a basic human right and making it law.

This convergence between data-heavy library operations and rights-based data governance is fundamentally changing how libraries can, must, and should work. The question is no longer simply "Can we collect this data?" but rather "Should we? Who for? At what price for trust?"

The regulatory setting and the area it covers :

There have been huge changes in the rules about data privacy. The General Data Protection Regulation (GDPR) of the European Union set a global standard that changed how people thought about data protection on all continents. India's Digital Personal Data Protection Act, which went into effect on August 11, 2023, is the first full privacy law in Asia's largest democracy, which has more than 560 million internet users. Brazil (LGPD), South Africa (POPIA), and many U.S. states have all added or strengthened privacy protections.

These rules aren't just pointless bureaucratic exercises. They show a change in philosophy*: the idea that people have basic rights over their own information and that organisations, including libraries, must respect those rights or face serious legal and reputational consequences.*

Purpose of the Study :

This article looks at how changing data rights and privacy policies are changing how libraries work in different types of institutions, such as schools, public libraries, and academic libraries. It offers evidence-based analysis rooted in legislation, case studies of actual library incidents, vendor practices, and evolving best practices. The analysis is based on India's DPDP Act, which turns privacy principles into rules that can be used in any situation.

Learning About Data Privacy and Data Rights in Libraries :

1. What Libraries Collect: A Complete List of Personal Information :

People who aren't in the library field are often surprised by how much data libraries now handle. It goes way beyond the usual "patron record" or borrowing history:

- Name, address, email address, phone number,
- Institutional ID, proof of identity documents, employment status, and age are all examples of identity and contact information.

Usage and Behavioural Data :

Full histories of circulation (every book borrowed, every audiobook streamed, and every journal article downloaded), patterns of renewals, requests for reservations and holds,

requests for interlibrary loans, use of physical space (room bookings, computer reservations), and patterns of library use over time.

Digital Interaction Data :

Search queries in discovery systems and catalogues, materials viewed but not borrowed, time spent on different library databases, clickstreams within library systems, device types and IP addresses, and session-level information from library networks.

Content and Research Data :

Reading lists and course reserves information, subject areas of interest (inferred from searches and downloads), academic or research topics pursued, citations managers and research tools used, and institutional repository submissions (which may reveal research interests and career trajectories).

Sensitive Proxy Data :

Libraries don't usually ask for direct information about health, political beliefs, or religious beliefs, but the materials that people look at often show these things. Someone reading about HIV/AIDS treatment, gender-affirming care, political dissent, or certain religious traditions makes data that, if shared, could lead to discrimination, harassment, or worse.

Libraries have historically occupied a sacred trust in the communities. For generations, librarians have understood that intellectual freedom flourishes only when privacy is protected—when readers can explore ideas, access sensitive materials, and pursue knowledge without fear of surveillance, judgment, or disclosure. This tradition, rooted in professional ethics codes dating back to the American Library Association's foundational principles, represents something deeply human: the belief that what we read, seek, and learn is fundamentally our own.

Today, libraries face an unprecedented paradox. Digital transformation—accelerated dramatically during the COVID-19 pandemic—has enabled remarkable service innovations: remote access to collections, personalized discovery systems, virtual reference services, and real-time learning analytics. Yet each innovation generates personal data. Every catalog search, database login, e-resource download, Wi-Fi session, and virtual chat creates a digital footprint. Simultaneously, governments worldwide are recognizing data protection as a fundamental human right and codifying it into law.

This convergence—*between data-intensive library operations and rights-based data governance—is fundamentally reshaping how libraries can, must, and should operate. The question is no longer simply "Can we collect this data?" but rather "Should we? For whom? At what cost to trust?"*

1. **Privacy as an Institutional and Individual Value :**

Ethics says clearly that librarians must "protect each library user's right to privacy and confidentiality with respect to information sought at the library and borrowed, purchased, or accessed through the library." This is not just a choice; it is a professional duty based on the idea that intellectual freedom can't exist when people are being watched.

Privacy as a Key Part of Intellectual Freedom :

Intellectual freedom is a key part of librarianship. It means that people can think about things, learn new things, and come up with new ideas without anyone else judging or controlling them. But this freedom doesn't mean anything if people are afraid that their searches, borrowing, or reading habits are being watched, shared, or used against them. Studies show that when people think their search behaviour is being tracked, they "self-censor" by avoiding search terms, materials, or topics they think might be used to judge or discriminate against them. Someone looking into a medical condition might not search if they think their information will be shared with their boss. A teenager who is trying to figure out their gender identity might not go to the library at all if they are afraid of being found out. In this way, violations of privacy directly hurt intellectual freedom.

Privacy as Trust Infrastructure :

People in their communities' trust libraries to do the right thing. You don't earn this trust just by having good collections or helpful staff; you earn it by showing that you care about user privacy. Libraries tell their communities, "You are safe here," when they handle personal data safely, clearly explain how they do things, and protect user information very well. Your information is yours. On the other hand, data breaches, sharing information without a clear reason, or unclear data practices quickly and deeply damage that trust

Data Rights: Giving People More Control :

Data rights are a philosophical and legal change from the past. In the past, organisations (including libraries) gathered and managed personal information with little input from users. Modern data rights frameworks give individuals—the "data principals" or "data subjects" more control over their own information, which is a big change from the past.

Depending on the law, data rights usually include :

Right to Know :

People have the right to clear, easy-to-find information about what data is being collected, why, by whom, and for how long. When privacy notices are long, use legal language, or are hidden in policies that few people will read, this right is weakened.

Right of Access :

People can ask for a copy of all the personal information that is kept about them in a format that is easy to read. This means that a library user can ask for a full list of every book they've borrowed, every search they've done, and every program they've attended. This is a

picture of their intellectual and informational life.

Right to Fix or Change :

People can ask for corrections if the data is wrong or missing. This could mean correcting a misspelt email address or changing a patron's status that is no longer current.

Right to Erasure or "Right to Be Forgotten”:

People can ask for their personal data to be deleted once it is no longer needed for its original purpose, with some legal exceptions. Someone who closes their library account might ask for their borrowing history to be deleted, but libraries may have to keep some records for audit or preservation reasons.

Right to Limit Processing :

A customer might agree to having their data processed for service delivery but not for algorithmic recommendations or institutional learning analytics.

Right to Move Data :

In some places, people can ask for their data in a structured, widely used format so they can move it to another service provider. This is important for people who are switching library systems or putting all of their digital life together on different platforms.

Right to Object :

People can say no to some kinds of processing, especially automated decision-making and direct marketing.

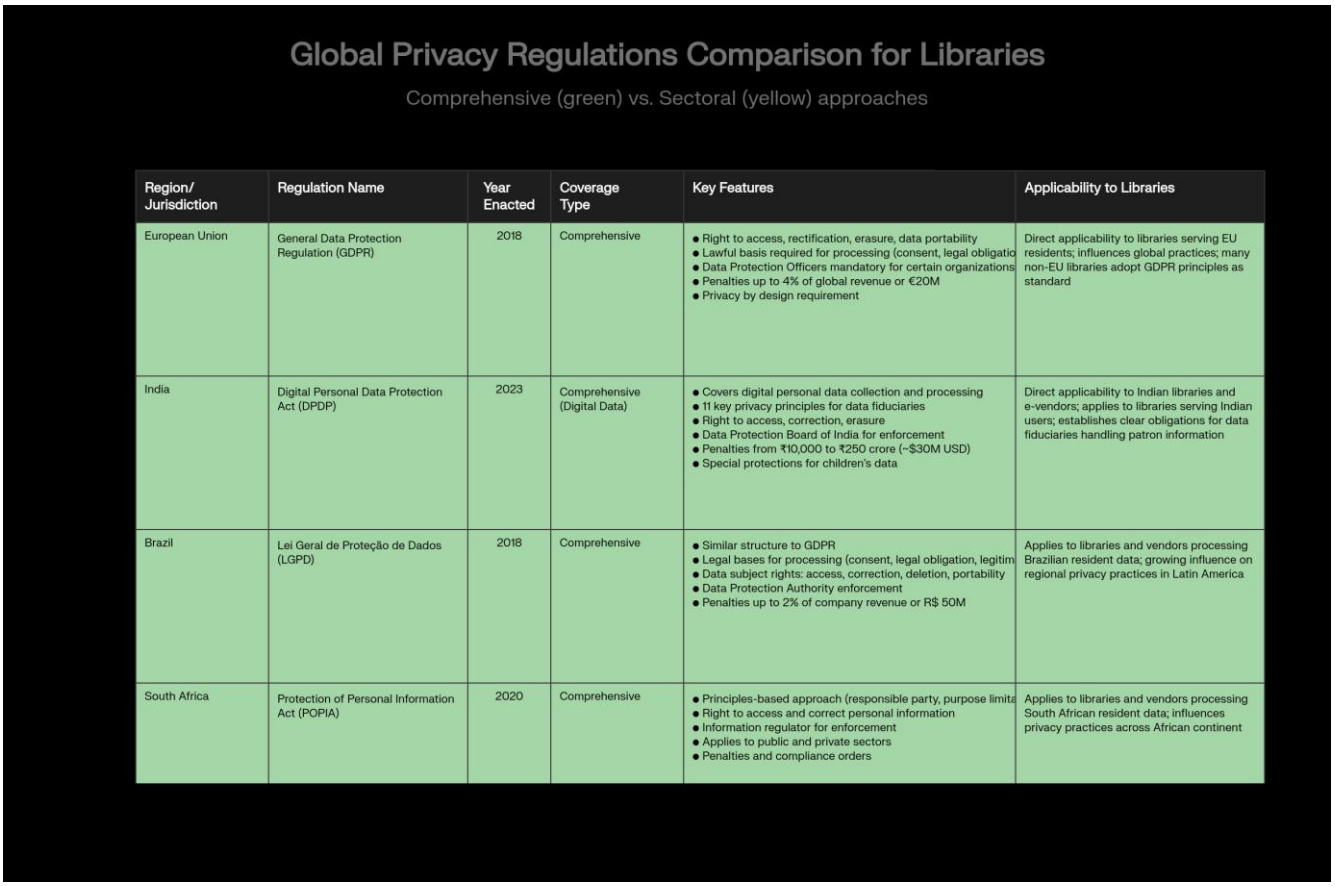
Right to Have Your Complaint Heard :

People who think their data rights have been broken can file complaints with the company and, if they aren't happy, with data protection authorities.

For people who use libraries, these rights mean real control: *"I can know what you know about me." If it's wrong, I can fix it. You can stop using it if I ask you to. If you mess it up, I can complain. This is a big shift in the balance of power.*

1. The Regulatory Framework: Global and Local Contexts :

This section emphasizes the global and local privacy regulations available and the framework suggested. The below figure presents the comparison amongst various global privacy regulations from libraries perspective.



Region/ Jurisdiction	Regulation Name	Year Enacted	Coverage Type	Key Features	Applicability to Libraries
European Union	General Data Protection Regulation (GDPR)	2018	Comprehensive	• Right to access, rectification, erasure, data portability • Lawful basis required for processing (consent, legal obligatio • Data Protection Officers mandatory for certain organizations • Penalties up to 4% of global revenue or €20M • Privacy by design requirement	Direct applicability to libraries serving EU residents; influences global practices; many non-EU libraries adopt GDPR principles as standard
India	Digital Personal Data Protection Act (DPDP)	2023	Comprehensive (Digital Data)	• Covers digital personal data collection and processing • 11 key privacy principles for data fiduciaries • Right to access, correction, erasure • Data Protection Board of India for enforcement • Penalties from ₹10,000 to ₹250 crore (~$30M USD) • Special protections for children's data	Direct applicability to Indian libraries and e-vendors; applies to libraries serving Indian users; establishes clear obligations for data fiduciaries handling patron information
Brazil	Lei Geral de Proteção de Dados (LGPD)	2018	Comprehensive	• Similar structure to GDPR • Legal bases for processing (consent, legal obligation, legitim • Data subject rights: access, correction, deletion, portability • Data Protection Authority enforcement • Penalties up to 2% of company revenue or R$ 50M	Applies to libraries and vendors processing Brazilian resident data; growing influence on regional privacy practices in Latin America
South Africa	Protection of Personal Information Act (POPIA)	2020	Comprehensive	• Principles-based approach (responsible party, purpose limita • Right to access and correct personal information • Information regulator for enforcement • Applies to public and private sectors • Penalties and compliance orders	Applies to libraries and vendors processing South African resident data; influences privacy practices across African continent

India's Digital Personal Data Protection Act, 2023: A Landmark for Asian Privacy :

The Digital Personal Data Protection Act (DPDP Act) in India is a huge step toward keeping data safe. It went into effect on August 11, 2023. More than 560 million people in the country use the internet, and both the government and businesses are swiftly going digital. The Act safeguards private information that is stored online.

The DPDP Act protects "data principals," or the people whose data is used, and provides requirements for "data fiduciaries," or the groups that decide how that data is used. It's evident that the Act encompasses libraries, which have a lot of information about their clients, as well as library workers, who work with that information.

The Act specifies that you can only use someone's personal information if they clearly and willingly give you permission or for "certain legitimate uses," such when the law says so, there is a public health risk, or the state needs it for security reasons. The Act creates the Data Protection Board of India. This group can take care of complaints, discipline people who disobey the rules, and make sure that everyone follows the regulations.

Libraries should observe these eleven rules about privacy that were created by researchers for libraries' privacy based on the DPDP Act:

1. **Data Collection and Notice** : Before libraries keep people's data, they must tell them what data they are collecting, why they are collecting it, how long they will keep it, and what rights those individuals have. Notices must be written in language that is

easy to understand.

2. **Data Retention** : Unless legally required, libraries must erase personal data once its purpose is fulfilled or consent is withdrawn. Retention schedules must be documented and enforced.
3. **Data Processing** You can only process personal data (such utilising it in learning analytics or personalisation algorithms) if the person agrees and for the reason that was agreed upon.
4. **Sharing Data** : You must seek the customer's permission before sharing their data with partners or other third parties. If the person requests you to stop distributing it, or if the link ends, you should stop. There are limits on what you can bring from one country to another.
5. **User Consent** : Users must give their consent in a clear, accurate, and free way. People can change their minds at any time.
6. **Information about Kids** : It is safer for kids under 18 than for adults. Without their parents' permission, you can't keep an eye on or track kids' behavior or utilize their information for targeted marketing.
7. **User Rights** : Users have actionable rights to access their data, correct inaccuracies, request deletion, receive grievance redressal, and nominate representatives.
8. **User Security** : Libraries must implement current encryption, secure authentication, and security protocols to prevent unauthorized access
9. **Reporting** : Data breaches must be reported to authorities and affected users immediately
10. **Data Protection Officers** : Libraries, especially "Significant Data Fiduciaries," need to engage Data Protection Officers, undertake effect assessments, and keep records that can be verified to make sure they are following the requirements.
11. **Compensation** : For minor offences, they might be as low as ₹10,000, which is roughly $120 USD. For serious offences, they might be as high as ₹250 crore, or around $30 million USD.

The GDPR in Europe: A Model for the Whole World :

This site is largely on the European GDPR (2018), but it has become a de facto global standard that affects how businesses throughout the world think about privacy, even those that don't have to obey it. Many libraries in the US, Asia, and other regions use GDPR as a guide for their guidelines. The GDPR contains these main parts:

- Easy rules for acquiring authorisation to undertake most of the tasks.
- User rights, like the right to see, alter, delete, and move data. "Privacy by design" means that privacy was taken into account and planned for from the start of the system.
- Big fines (up to 4% of sales or €20 million, whichever is higher) - Sometimes you need data security officers.

The United States: Different Ways of Doing Things and Different State Privacy Laws :

The GDPR and India's DPDP Act are both better than any Privacy Act in the U.S. Instead, rules that only apply to certain places manage privacy:

- **The Family Educational Rights and Privacy Act (FERPA)** : This law protects youngsters' school records in libraries.
- **The Child Online Privacy Protection Act (COPPA)** makes it tougher to collect personal information from youngsters under 13.
- **State library privacy laws** : Many states in the U.S. have legislation that protect library records. The Texas State Library and Archives Commission revised the rules for obtaining recognised in 2025. By July 31, 2027, all public libraries must have a documented policy about privacy.

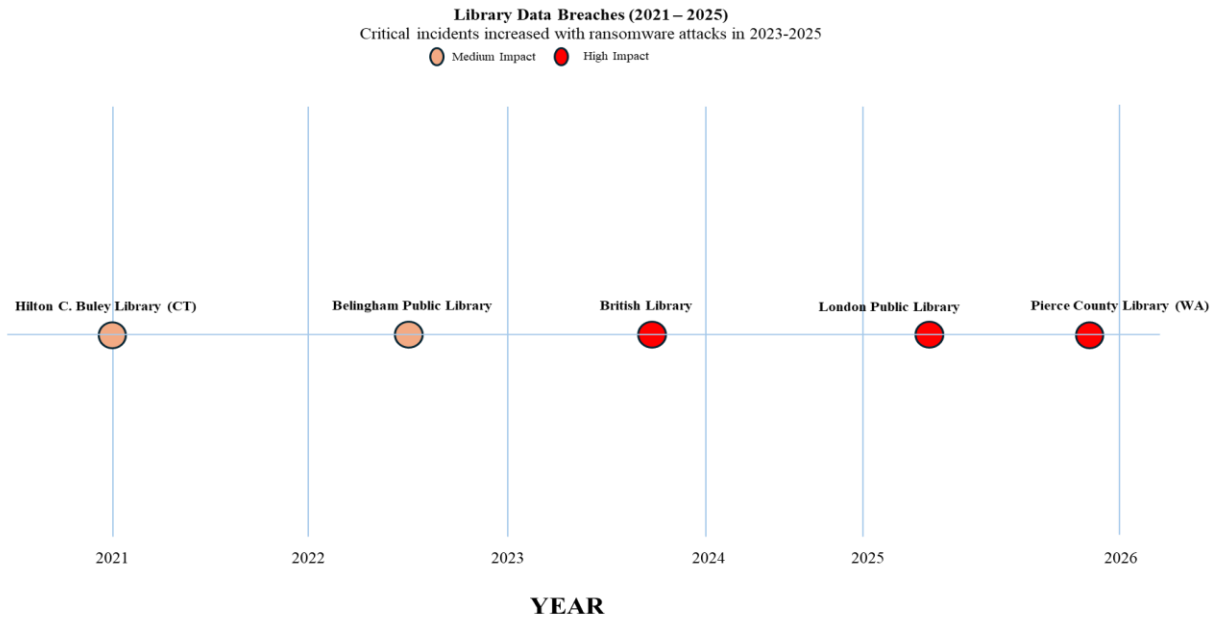
Many U.S. states, including California, Virginia, and Colorado, approved tough privacy laws in 2024 and 2025. These restrictions would apply to libraries in those states that keep records of persons who dwell there.

The LGPD and POPIA in Brazil and South Africa: A New Global Standard :

People all throughout the world are working to make data safer. In South Africa, the Protection of Personal Information Act (POPIA) went into effect in 2020. In Brazil, the Lei Geral de Proteção de Dados (LGPD) went into effect in 2018. The GDPR, Brazil's LGPD, and India's DPDP Act all share the same major points: they all need a legal purpose to handle data, they all safeguard user rights, they all need data security, and they all have robust enforcement procedures with high fines.

The Shadow Side: Data Breaches, Vendor Failures & Human Impact :

There is significant rise in data breaches post COVID 19. The below figure depicts few of the high-profile data breaches happened globally between 2021-2025.



List of data breaches at Libraries across the globe :

- **The British Library Ransomware Attack (October 2023) :** The Rhysida hacking group broke into the British Library and caused huge damage to the library data. The hacking group stole almost 600 GB of data that roughly translates to 50,000 files. This includes private information on library staff and customers. The hackers asked for a ransom of 20 bitcoins, which is roughly £600,000. When the Library refused to pay, hackers put 573 GB of information on the dark web, including scans of employee passports and contracts. This event shows that data breaches may hurt individuals and that even the most secured and reputed companies can also be hacked.
- **Pierce County Library Data Breach (December 2025) :** The Pierce County Library in Washington State says that a data breach put the private information of 340,000 patrons and employees at risk. The scale and scope of the problem reveal that it impacts libraries all around the world and in all sorts of libraries.
- **Cyberattack on the London Public Library (June 2025) :** A ransomware attack that used a zero-day exploit put the personal information of current and former staff, patrons, contributors, and the public at risk. The attack locked up library systems, which stopped services and forced staff to use paper-based procedures. It was a frightening reminder of how much libraries depend on digital infrastructure.
- **Unauthorised Data Download at Bellingham Public Library (June 2022) :** People stole patron data from library computer networks without permission. The non-compliance to the standards and security implementation caused the breach.

Vendor Practices: Not Following Library Ethics :

Scholarly research has uncovered widespread privacy concerns among library providers. Magi's groundbreaking study of 27 e-journal providers showed that they all kept track of consumers' search history and usage data. Many of these companies had privacy policies that didn't make these practices clear or that put the vendor's needs ahead of the customer's privacy. Lambert and others investigated five well-known digital material distributors, namely Axis 360, Hoopla, and OverDrive. They determined that these companies' privacy policies "did not meet library privacy standards."

McKinnon and Turp looked examined the privacy policies of major integrated library system suppliers (EBSCO, Ex Libris, OCLC, and SirsiDynix) and found that these companies said they followed privacy rules but didn't give much information on how they would share user data after getting permission. Some suppliers kept track of search history and behaviour for their own analytics or even sold the information to other companies. These actions were not in line with library rules of conduct.

Problems with the Chat Platform :

The Hilton C. Buley Library at Southern Connecticut State University found that their chat reference platform made users give their name, phone number, email address, and

reference question content. They couldn't do this without revealing who they were. The library changed the settings so that PII was no longer needed and changed the privacy policy to make it clear that chat services can be dangerous. This case shows that libraries need to be careful because not all vendors worry about privacy when they make something.

Impact on people :

About 340,000 people data compromised in Pierce County, these include personal data like medical subscription, religion preferences and other sensitive information. The British Library's breach showed what 500,000 individuals were interested in learning about. Every violation is a big deal that breaks trust.

Also, it has been shown that privacy violations might cause problems in the future. People whose health information is made public may have a hard time getting insurance or a job. People who do political research and share it with others may be harassed or worse. Teenagers who are LGBTQ+ and whose online activity is made public are in real risk. These aren't just vague threats; they're genuine physical hurts that people feel long after a breach is "fixed."

Good Things: How Library Privacy Rules Make Them Stronger :

Following the regulations could be hard and cost a lot of money for libraries, but it can also help them be more honest and earn the trust of the community.

Bringing back the most important principles of the field :

Librarians can now put into action concepts they have long believed in but have had problems doing so because of privacy regulations. When an institution can't use "security through obscurity" or "no one cares about privacy anyway," librarians have the right to fight for policies that are in line with professional ethics.

A Real-Life Example :

The library's research office is telling the library to integrate learning analytics to its systems for locating things. To do this, you need to keep track of each user's search patterns, the things they looked at, and how long they spent on them. Then you need to connect this to their grades and graduation rates. Before, the library might have talked about things in a casual way. The library can say now under the GDPR or India's DPDP Act until the school gets clear, informed consent from the students. Instead of just saying what they think is best, the library can also go to court. When you say, "This is what the law says," instead of, "Librarians are being difficult," the law is on your side.

Helping institutions and users trust each other :

People are more likely to trust libraries when they are open about how they handle data, only collect data that is necessary, and give users real control over their information. People who handle data in a dishonest or careless way hurt their reputation in ways that go

beyond privacy circles. When a library has a breach and doesn't tell patrons or take responsibility, it loses the trust of the community and privacy advocates.

At a time when many people are unsure about digital platforms and how businesses manage data, it's great to see libraries that make it clear that user privacy is their first priority.

Encouraging new ideas while respecting privacy :

Innovative libraries are using privacy laws as a design feature instead of seeing privacy as something that gets in the way of new ideas. This includes, Libraries can see trends at the collection or cohort level (for example, "Which subject areas generated 20% more interest this semester?") The anonymised and aggregated analytics can help libraries in collecting this information without revealing the names of individual users.

Problems and limitations in the system :

There is a lot of great potential, but it's hard to put good privacy protections in place, especially for libraries who don't have the money to do so.

The cost of not having enough money and following the rules :

Small and medium-sized libraries, especially those in rural or poor areas, don't have a lot of resources. To stay within the law when it comes to privacy, you must:

The technical infrastructure includes encryption technologies, safe authentication (such multi-factor authentication), and secure hosting, which usually means switching from old on-premises systems to compliant cloud providers.

Governance and Documentation: Staff training, privacy impact assessments, data mapping (making a list of the systems and the personal data they store), retention schedules, and ways to respond to incidents.

Costs for legal and expert advice: hiring data protection experts, reviewing vendor contracts, and keeping an eye on the rules.

Many rules say that a company must have a Data Protection Officer (DPO), but smaller enterprises may not be able to find one.

These expenditures are directly competing with collection development, program funding, and hiring staff in a medium-sized city's public library or a school that doesn't have enough money for an academic library. The library director has to choose between paying for private compliance or hiring a new librarian. This isn't a made-up problem.

Old systems and technology debt :

More than five years ago, when privacy wasn't as big of a deal, many libraries established integrated library systems (ILS), discovery platforms, and digital repositories.

These old methods would often:

- Keep data in ways that make it impossible to completely hide or separate
- Don't have strong encryption or safe ways to sign in
- Create logs and session data that are hard to delete
- Connect to third-party services in ways that are hard to check or undo

Upgrading or replacing present systems is expensive and difficult. Libraries need to weigh the costs and service interruptions that come with modernisation against the privacy benefits it brings.

The Analytics Paradox: Evidence-Based Management vs. Privacy :

Libraries are under a lot of stress to explain how they are making a difference. Institutional stakeholders need to know which databases are ideal for research. How does being able to use the library affect how many students stay in school? What communities aren't getting the aid they need? You can answer these questions with correct usage data, but getting that data would violate privacy rules.

Libraries should be very careful about how they talk about this. Using analytics that are gathered together and made anonymous, you can answer a lot of questions without showing how people answer. But you need to know a lot about data science and be okay with results that aren't as complete. Some groups don't know how to achieve this.

Unfair power in negotiations and vendor lock-in :

Most library services depend on outside firms for things like e-resource platforms (EBSCO, ProQuest, SirsiDynix), discovery systems (Ex Libris, Primo), digital preservation systems, and authentication providers. These vendors are often big, well-known companies that have a lot of power when it comes to making deals. The library can't do anything if the vendor's privacy practices are different from the library's.

A tiny library can't just say, "We'll switch to your competitor unless you change how you handle data." This is because the competitor usually does the same thing, and it costs too much to move. This causes a "race to the bottom," in which vendors provide capabilities like behavioural tracking, cross-device targeting, and algorithmic suggestions, since they can make money off the data and know that most libraries will accept them.

Some libraries are fighting back. Libraries might be able to negotiate better when they buy things together. Professional groups like ALA and IFLA are working on standard licence language that puts privacy first. But the power imbalance is still there.

Issues arising from fragmented responsibility and governance :

In a lot of cases, academic and institutional libraries don't have proper defined rules and regulations in place. Central IT departments that don't know anything about library ethics

may administer library systems. Institutional identity services are in charge of user authentication.

A library director's commitment to privacy may be compromised by IT decisions made by others, vendor partnerships negotiated by others, or institutional rules that supersede library preferences. If there isn't a clear chain of command and integrated governance, privacy rules might become goals instead of things we do.

Strategic Reponses: How Libraries can Help :

Libraries that are ahead of the curve are looking for ways to keep their promises about privacy, even when they don't have enough money or staff to do it.

Making it easier to find and understand warnings and privacy policies :

The first step in this process is for the organization to have a clear privacy policy. Tells you what data is collected: Not in technical terms, but in plain English. For example, "When you visit our library website, we collect information about your web browser and your IP address (the unique number that identifies your internet connection). This helps us understand how the site is used and make it work better."

"We don't use your IP address to find you or keep track of what you do online; we use it to find threats to security and stop abuse."

"We automatically delete your website session data after 90 days. To meet financial audit requirements, we keep circulation records for 7 years." This is what the duration of data storage means.

"You have the right to ask for a copy of all the information we have about you. You can also ask us to fix any incorrect information. You can also ask us to delete records that are not required by law. If you have a complaint, you can file it with our privacy officer or, in places where there are data protection authorities, with the national data protection authority." Gives Contact Information: "If you have questions about privacy, please email privacy@library.org or call XX-XXXX."

The library's website needs to make this policy easy to find, in a number of languages that reflect the people it serves, and at a level that is easy to understand.

Putting Privacy by design into Action :

- Libraries should make sure that privacy is built into the design and function of their systems from the start, not added later. Libraries should have minimal data approach, that means collecting as much as required and as much is important.
- **Purpose Limitation** : Only use data for the purpose for which it was given. You need to get new permission before using data that was collected for service delivery for institutional study.
- **Pseudonymization and Anonymisation** : If you can, use codes or hashes instead of

names and IDs to obscure who you are. For analytics, keep patron and behaviour data separate so you can see trends in usage without knowing who gave you the data.

- **Secure by Default** : Use HTTPS (secure internet connections), strong password policies, multi-factor authentication for important services, and role-based access restriction (only library workers who need to see patron data can do so).
- **Data Lifecycle Management** : Write down how long you keep certain types of data and set up automatic deletion when those times are up. After 30 days, a library's circulation system should automatically delete session logs, circulation records, and other records that the law says it ought to keep.

Bettering management and training employees :

For privacy governance to succeed, people need to know what their jobs are and keep learning:

- **Choose a Privacy Leader** : Hire a privacy officer to be in-charge of making changes to the privacy policy, making sure it is followed, and being the person to go to with questions or complaints regarding privacy. This person could work part-time or in a job that already exists.
- **Set up a Privacy Committee** that includes administrators, IT staff, librarians, and (ideally) community or patron representatives. Get together every so often to talk about privacy issues, look at new systems and vendor bids, and go over the privacy policy.
- **Give Regular Training** : Everyone who works with consumer data should get basic training on privacy. What kinds of personal information are safe? What should employees do if they think there has been a data breach? How do people use their rights, such demanding, to access their information? Training doesn't have to take a long time, but you should do it at least once a year.
- **Conduct Data Protection Impact Assessments (DPIA)** : The libraries should conduct Data Protection Impact Assessments on regular intervals, and it should be part of their defined policies and processes. This will help in assessing risks in advance and so the mitigation on time.

Maintaining contracts and taking care of vendor relationships :

Libraries must actively manage their relationships with vendors to protect privacy:

Do Your Research : Before you hire a new service provider, be sure you know how they handle privacy. Do they keep client information safe while it's being stored and while it's being moved? Do they have clear rules on how long they can keep information? Where do they save their data?

The libraries should develop or adopt the process of contracts that put privacy first.

The contract should have following but not limited to:

- The purpose of usage of customer data and under what circumstances
- No data can be used for marketing or profiling purpose unless explicit consent obtained from the librarian or authorized party
- Audit rights
    - Ensuring the deletion of data once either the contract is expired or the purpose is fulfilled etc.
- **Use standard licensing language**: The American Library Association and regional library consortia have come up with standard license language that includes privacy protections.
- **Collective Action:** Libraries can work together to form consortia or alliances, which makes them stronger when they bargain.

Making User Rights Work :

Libraries need to find ways for people to use their rights :

- **Make it easy to get personal data** : Users should be able to get a copy of the library's records about them by filling out a simple web form, sending an email, or asking in person. For instance, GDPR and a lot of other standards say that this should happen within 30 days.
- **Set Clear Rules for Fixing and Deleting** : The library should fix any wrong information straight away if a user finds it. The library should delete or make the data anonymous if a user asks for it to be done (with some legal limits).
- **Make a Way for People to File concerns** : People should be able to report privacy problems, and the library should have a written plan for how to look into and deal with concerns within a certain amount of time.
- **When You Can, Let Users Control Their Own Data** : Libraries can sometimes give users online dashboards that let them see their data, change their privacy settings, and choose who can see their data. For example, a library user could connect onto their account and see their circulation history, change their notification settings, or find out which databases they have used.

Using technology that keeps your privacy protected :

Libraries that are ahead of the curve are embracing technology to protect people's data:

- **Analytics Tools That Don't Share Personal Information :** Libraries can use analytics tools other than Google Analytics that don't follow users across the web. These approaches let libraries see overall trends without keeping an eye on each user.
- **VPN Services for Users** : Some libraries provide free VPN (Virtual Private Network) services. This allows people to protect their privacy and encrypt their internet traffic while they use library Wi-Fi or get library materials from home.
- **Federated Identity and Attribute-Based Access** : Libraries can use federated

authentication methods like Shibboleth or SAML to only give out the information needed for access, such "valid university affiliation" instead of a full student profile.

Looking Ahead: New Opportunities and Challenges :

AI and Algorithmic Responsibility :

Libraries are beginning to use AI in their services, like chatbots for reference, recommendation engines to help people find new things, and algorithmic content curation. When you teach AI systems about your personal data, they become responsible for your privacy. AI also raises worries about algorithmic bias, imprecise conclusions ("the algorithm suggested it, but I don't know why"), and the likelihood of unfair results.

Libraries need to :

- Tell businesses to be honest about how their algorithms work: How does the algorithm learn? What kind of information do you use? Can the library come up with ways to offer suggestions?
- Have people check algorithms should show information but not make decisions on their own.
- **Do bias audits** : check recommendation systems to make sure they don't treat people differently based on their race, gender, handicap status, or other protected traits.
- Users should have the option to not use it. For instance, if an algorithm decides which resources to highlight prominently, users should be able to turn it off or adjust it.

Data flows across borders and the complexity of jurisdiction :

More and more libraries are using cloud services and multinational providers. Data can be stored in many different countries, processed across borders, and subject to a wide range of laws. The DPDP Act in India only lets data be sent to countries that don't have good data protection. The GDPR in the EU has made a number of legal ways to move data useless.

Libraries have to :

- Make a map showing where vendor data is stored and used
- Know what the rules are for each area of compliance
- Use legal means, such as Standard Contractual Clauses, to move data across borders.- Add language to the contract that makes it clear that vendors must follow all applicable requirements.

The Function of Professional Associations and Policy Advocacy :

Libraries can't deal with big privacy problems on their own. The ALA, IFLA, and regional library associations are examples of professional groups that should:

- Write and keep model privacy standards and vendor contracts up to date

- Teach people about privacy and data protection and help them grow professionally
- Ask libraries how they protect their patrons' privacy and suggest modifications.
- Change privacy laws in the US and around the world so that they work for libraries.
- Give libraries that don't have enough money, guidance, templates, and training to help them follow the rules.

Putting privacy and data literacy into library science classes :

The next generation of librarians needs to know how to protect people's privacy, manage data, and make moral choices about data.

Graduate programs in library science should :

- Teach the basics of privacy and data protection.
- Give students the option to take classes in ethics, governance, and privacy law.
- Teach useful skills including how to undertake privacy impact assessments, negotiate vendor contracts, and design things with privacy in mind.
- Stress how privacy, freedom of speech, and professional ethics are all linked.

Talk About Putting Together Principles, Challenges, and Opportunities :

The information in this article shows that things are changing in this field. Libraries are stranded between the analogue era, when closed stacks and limited circulation records kept people's privacy safe, and the digital world, where data transfers between systems, organisations, and countries at a speed and volume never seen before. This change isn't only annoying, though. Privacy rules don't always mean that institutions have to follow them. In fact, they often agree with what librarians have always thought. Intellectual freedom is useless without privacy. People trust library service, and that's the most important thing about it. According to professional ethics, you should not share information about your clients. By making these promises into law, rules give librarians the power to fight for values they once held dear but found hard to put into action.

The realistic route forward needs :

1. **Leadership's Institutional Commitment** : Library managers and directors need to show that they care about privacy. When hiring, making budgets, choosing systems, and negotiating with vendors, you should think about this, not just follow the law. This promise lets librarians deal with privacy issues.
2. **Long-Term Investment in Capacity and Infrastructure** : To follow privacy laws, you need to keep spending money on systems that help keep data safe, train employees, manage vendors, and set rules. You have to do this all the time, not just once. It is important to organise library budgets in a sensible way.
3. **Collaborative Problem-Solving** : These issues don't only happen in one library. Libraries can share solutions, work together to get better prices from vendors, and seek expert help that they can't afford on their own through consortia, professional associations, and peer networks.

4. **Grounded in Values** : Libraries should preserve people's privacy because it's the right thing to do for their profession. They should treat individuals who come to learn and grow intellectually with respect and dignity, not because they are scared about being punished by the government.

Conclusion :

Data privacy legislation and data rights are one easy way to shift the balance of power between individuals and enterprises. Libraries have traditionally thought of themselves as trustworthy places to retain user information. Now they have a lot of power and a real chance to make a difference. It's clear what libraries do: they preserve private information that shows people's most personal academic interests, health concerns, political convictions, and spiritual journeys. You need to be very careful to keep this information safe. When libraries suffer data breaches, distribute information without permission, or act carelessly, people lose faith in them. Libraries can set themselves apart from other places by showing that they really care about privacy. This is really crucial right now because a lot of firms utilise people's personal information without their permission. But there are also a lot of chances. Privacy frameworks don't restrict libraries from coming up with new ideas; in fact, they enable them to do so. Libraries that follow privacy-by-design principles will make technologies that people can trust and that respect their privacy. If libraries make data governance clear and focus on the user, they will be able to hire the best people and keep patrons interested. Libraries that speak up for privacy during policy talks will modify the rules in ways that help both their libraries and the people they serve. The Digital Personal Data Protection Act in India provides 11 rules around privacy that advise you exactly what to do. But having principles alone isn't enough. You need dedicated resources, enough staff, governance frameworks, and constant support from leadership to make it happen. Users need to know what data is being gathered and why. This means that they need to talk to vendors about contracts and how they handle data, which is not easy. To protect your privacy, you often have to say "no" to things that put people's dignity behind convenience or institutional criteria. Doing this takes a lot of humility. Libraries and the people they serve have a lot to lose. Libraries protect free thought, human dignity, and informed citizenship in a world where more and more people are being watched, and their data is being used. To keep that promise in the digital era, we need to take data privacy and rights very seriously. There will be issues along the way. It is important, possible, and in line with what libraries have long stood for.

References :

- American Library Association. (2022). **ALA Code of ethics**. Retrieved from https://www.ala.org/tools-resources/guidelines-and-standards
- Bareh, C. K. (2024). Reviewing the privacy implications of India's digital personal data protection act (2023) from library contexts. **DESIDOC Journal of Library & Information Technology**, 44(1), 50–56. https://doi.org/10.14429/djlit.44.1.18410
- Chin, C. L. (2024). Patron privacy protections in public libraries. **Journal of Intellectual Freedom and Privacy**, 5(2), 45–62.
- Data Protection Ireland. (2023). **Your rights under the GDPR**. Retrieved from

http://www.dataprotection.ie/individuals/rights-individuals-under-general-data-protection-regulation

- European Union. (2018). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88.
- Klinefelter, A. (2016). Reader privacy in digital library collaborations. *Journal of Academic Librarianship*, 42(3), 194–203.
- Lambert, A., Parker, J., & Bashir, M. (2016). Evaluating digital vendor privacy policies: A framework for assessment. *Library Quarterly*, 86(2), 180–198.
- Magi, T. (2010). Undercover marketing in libraries: Ethical concerns and vendor practices. *Library Journal*, 135(12), 44–47.
- Ministry of Electronics and Information Technology (MEITY), Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*. New Delhi: Government of India Publications.
- Noh, Y. (2017). A study of users' privacy perceptions on the internet: Behavior-based segmentation and profiling. *Library & Information Science Research*, 39(3), 178–189.
- Sweeney, L., & Davis, S. (2021). Privacy risks of voice assistants in libraries and educational settings. *Information Privacy Law Journal*, 7(1), 33–51.
- Texas State Library and Archives Commission. (2025). *Information security and privacy policy standards for Texas public libraries*. Texas Administrative Code, Title 13, Chapter 4.
- Zimmer, M. (2014). Privacy in context: Technology, policy, and the integrity of social life. *Mosaic Press*.