DESIDOC Journal of Library & Information Technology, Vol. 44, No. 1, January 2024, pp.50-58, DOI : 10.14429/djlit.44.1.18410

Reviewing the Privacy Implications of India's Digital Personal Data Protection Act (2023) from Library Contexts

Chanlang Ki Bareh[1-2]

[1]*Department of Library and Information Science, North-Eastern Hill University, Shillong - 793 022, India*
[2]*Central Library, Nagaland University, Lumami - 798 627, India*
E-mail: Shanlang88@gmail.com

ABSTRACT

The study reviews the provisions and privacy implications of the India's Digital Personal Data Protection Act, 2023 (referred to as "DPDP Act" in this study) from the library context. The immense nature of personal data breaches prompted the government to enact the DPDP Act on 11th August 2023. Through the DPDP Act, this study addresses the privacy concerns in the library by articulating the eleven (11) privacy principles, viz., data collection & notice; data retention; data processing; data sharing; users consent; children's data; user's rights; users security; reporting; accountability, and compensation. These principles can act as privacy guidelines for libraries when negotiating with library vendors; these principles will further guide e-vendors into creating an online environment where user's privacy rights are protected. Also, this study aims to address the online privacy gaps in libraries by providing additional corrective measures and examples, such as - setting up an itemised privacy policy, a simple policy that is easily accessible, reducing the use of web tracking technologies, encouraging the use of privacy-enhancing technologies, de-identification of patron's data, and emphasising on user's right in the web environments. The study may also empower the government and online businesses by preserving the privacy rights of users.

Keywords: India digital personal data protection act; Personal data; Privacy policy; Privacy principle; Privacy compliance; Library privacy; Patron privacy

1. INTRODUCTION

India is the second-largest online market globally; India has over 560 million Internet users, with an estimate of over 650 million by 2023. This usage stood at 50 % as of 2020, which indicates that about half of India's population does not have access to the Internet in 2020[1]. Indian government, under the National e-Governance Plan (NeGP) initiated in 2006, started implementing various digital projects covering a wide range of departments, viz., agriculture, unique identification, health, education, passports seva, police and taxes, etc. These e-governance projects host major data assets such as the-Unique Identification numbers 'Aadhaar'; the Open Government Data (ODG) platform to facilitate access to government shareable data; Sugamya Bharat Abhiyaan, a mobile app for disability to have equal opportunity; Agri market app for farmers; Beti Bachao Beti Padhao to ensure gender equality; BHIM (Bharat Interface for Money) a financial transaction app; Crime and Criminal Tracking Network & Systems (CCTNS) to enhance effective policing, etc.,[2]. With the enormous nature of data generation by government and non-government organisations in India, there are bound to be privacy breaches.

Received : 10 August 2022, Revised : 01 December 2023
Accepted : 07 December 2023, Online published : 23 January 2024

According to Business Today, India ranked third in data breaches, with 86.63 million users breached as of November 2021[3]. Data breaches invade users' privacy and were considered one of the most common types of cybercrime. These leakages consist of personal data (For example: name, sex, phone no, address, passwords and unique identification numbers, etc.) that were sold/shared with third-party for analytics or cybercrime activities. A few examples of data breaches in India includes-the Air India personal data breach of 4.5 million passengers in 2021; the Leakage of 190,000 personal identifiable information (PII) test results of the Common Admission Test (CAT) 2020, and the COVID-19 lab test leaked by government websites[4].

Despite these data leakages, government and private enterprise's adoption of various digital services were not slowing down; it has increased by many folds, which is solely based on the Internet's ability to provide ease of accessibility and convenience to its users. With this background, the Indian parliament enacted the Digital Personal Data Protection Act of 2023 (referred to as "DPDP Act" in this study) to address privacy rights of its citizens. With the recent enactment of the DPDP Act in India on the 11th August 2023, both digital government initiatives and private businesses in the form of e-commerce or online vendors ought to be regulated.

Studies have shown the lack of privacy policy regulations in India[5-7]. Similarly in libraries, the lack of a privacy policy to regulate patron's privacy [8-10,28] when delivering online services puts the patrons at risk of exposing their personal data to the e-vendors or third-party services. Against this background, the author intends to review the DPDP Act and privacy literature to understand the following objectives:

- To discuss privacy issues and values from library perspectives.
- To understand the background of the DPDP Act, that will give clearer understanding of its origin and features.
- Thirdly, to summarise the key concepts of the DPDP Act by articulating them into eleven (11) privacy principles for compliance by e-vendors and libraries alike.
- To provide suggestive measures to library professionals when negotiating with e-vendors.

2. LIBRARY AND PRIVACY

Libraries have long-held 'Patron's Privacy' dearly. According to the American Library Association [11], the Library Bill of Rights in Article 7, stated that –

> *"All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate, and protect people's privacy."*

Privacy is fundamental in the library since it empowers patrons to choose, access, and read freely without being judged. An absence of privacy protection can greatly affect their trust in the library system[10]. Library vendors' disclosure and sharing of circulation records or browsing behaviour undermined patron's right to privacy. Therefore, genuine freedom towards patrons' information needs and online seeking behaviours must be protected. Monitoring or illegal sharing of personal data without taking prior permission from patrons should be discouraged. For this to happen, librarians must step in to advocate for patrons' privacy rights.

Few studies have addressed privacy concerns when opting for online library services. A study by Magi[8] on 27 e-journals mentioned the collection of patron's search history and preferences by e-journal vendors. Magi also pointed to the vendors' policy that was not matching with privacy standards of libraries. Similarly, a study by Lambert[9], *et al.* on five popular digital content vendors concluded that vendors' privacy policies fell short of meeting the privacy standards. Another study on major integrated library systems indicated that vendors collect personal data for various purposes, such as transactions, research, and maintaining communications with users. However, none explicitly refer to this information as confidential or private[10]. This implies that once patrons use these outsourced library services, they lose control over their personal data.

An attitude study on librarians' perspectives in the United States by Zimmer's[12] indicated a high privacy concern among library professionals and expressed their desire to have control over the use of their personal information. Zimmer's[12] findings also revealed that 57 per cent of libraries provide a written privacy policy to their patrons. At the same time, almost 80 per cent of these library professionals feel that libraries should play a role in imparting knowledge about privacy issues[12]. There is also a report of low awareness level from the administrators of 16 academic libraries in Turkey regarding the privacy of patrons' personal data[13]. Similarly, to address these shortcomings on privacy issues. Magi[8] suggests for librarians to protect their patrons' privacy from vendors through education[8] and training[13]. Lambert[9], *et al.* even suggest for stronger negotiation with library vendors to work in line with the library code of ethics[9]. Therefore, libraries must ensure that online service providers must meet the library code of ethics, such as-confidentiality of patrons' data or legal obligations concerning the breaches of patron's data.

Libraries are secular institutions that envisage the idea of Intellectual freedom by granting access to reading materials to meet users immediate and future information needs without causing harm to the user's privacy. But often at times, the services rendered by online library services were taken for granted by patrons who otherwise think that libraries do protects their privacy. These patrons were the ones libraries should put in time and effort to educate about privacy. However, there may be an exception that may apply to patrons' who are wary about their intellectual autonomy; who fears the influence upon their future reading habits by recommending materials based on their previous searches/preferences. Also, there may be some patrons who were not concerned at all. Hence, this may explain why? The concerns for privacy in libraries are ongoing and technologically ever-changing as libraries were encouraged to opt for online systems and services from third-party vendors.

3. BACKGROUND: DIGITAL PERSONAL DATA PROTECTION ACT 2023

India did not have exhaustive data protection legislation before the Personal Data Protection Bill 2019. However, this 2019 bill was recently replaced by the Digital Personal Data Protection Bill of 2022. Furthermore, this bill was enacted into the Digital Personal Data Protection Act 2023 (referred to as 'DPDP Act') on August 11th 2023. Prior to this DPDP Act in India, there was only sectoral acts like-the Indian Penal Code, 1860; Protection of Children from Sexual Offences Act, 2012; The Credit Information Companies (Regulation) Act, 2006, that partially address the citizen's right to privacy[14]. Also, the Information Technology Act, 2000, and Information Technology Rules, 2011, under sections 43A and 72A of the Act, were related to data protection. Unlike other sectoral Acts, the Information Technology Rules, 2011 somehow protect personal information and sensitive personal information by insisting that the corporate body must obtain consent before disclosing information[15].

Considering the insufficiency of these sectoral Acts to protect its citizen's data, it is imperative that India's data protection laws must be comprehensive to deter the breaches of privacy.

The developmental phase of the privacy legislation in India can be traced to the declaration of "Privacy rights' as a fundamental right by the supreme court of India on 24th August 2017, in the case of Justice K.S. Puttaswamy (Retd.) and Anr. V. Union of India ("Right to Privacy"). After that, the need was felt to have a stronger legislation in place, and in August 2017, the government appointed a committee chaired by retired Supreme court judge Justice Srikrishna. In 2018, the committee released the draft bill after incorporating the recommendations of the industry stakeholders, and a year after, the Personal Data Protection Bill (Bill No. 373 of 2019) was introduced in the Lok Sabha (lower house) of the Indian parliament[17]. It was introduced by the Minister of Electronics and Information Technology (MEITY), Shri Ravi Shankar Prasad, on 11th December 2019. The Bill seeks to protect its citizens' personal data or information and set up a Data Protection Authority (DPA) for the same[16].

On 11th December 2019, the 2019 Bill was referred to a Joint Parliamentary Committee ("JPC") for further deliberation. On 16th December 2021, after almost two (2) years of deliberation on the 2019 Bill, the JPC tabled its report on the Personal Data Protection Bill 2019. Recently, a committee report under the Chairmanship of Justice B.N. Srikrishna lays down various modifications to the Personal Data Protection Bill of 2019, which ultimately lead to the proposal of the The Digital Personal Data Protection Bill of 2022 (referred to as 'DPDP Bill' in this study)[17].

On 3rd August 2022, the Centre withdrew the Personal Data Protection Bill 2019 and superseded it with the DPDP Bill which consists of six (6) chapters, thirty (30) sections and one (1) schedule that were more comprehensive to safeguard the personal data of the users in digital contexts. After receiving approval from Lok Sabha and Rajya Sabha, the DPDP Bill 2022 was formally enacted by the president's of India on 11th August 2023, and thus came into existence the Digital Personal Data Protection Act, 2023. This enactment marked a significant achievement for the protection of personal data, both in digital or non-digital format (with subsequent conversion to digital format). This DPDP Act will have a significant impact with e-vendors that handles citizen's personal and non-personal data[18].

4. PRIVACY PRINCIPLES: DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 of India which was the first-ever act to protect its citizen's personal data was influenced by Europe's General Data Protection Right (GDPR). The DPDP Act provides comprehensive coverage under its nine (9) chapters and one schedule[18]. The basic idea behind summarising the key privacy principles from the DPDP Act was to protect patrons' privacy. The construction of these eleven (11) principles may act as privacy guidelines for libraries and e-vendors alike. For categorising these relevant sections and sub-sections into a single concept or principle, the author read through each chapters/sub-sections and clubbed relevant concepts that fulfilled the given description (see Table 1).

These eleven privacy principles in Table 1, articulated from the various sections of the DPDP Act, provide straightforward explanations with examples for libraries and e-vendors to achieve privacy compliance. These principles also empower the librarians to take precautionary steps and safeguard patrons' privacy when negotiating with e-vendors.

5. WHY 'PRIVACY COMPLIANCE' FOR LIBRARY VENDORS?

Due to the recent pandemic, many libraries started shifting to digital services and cloud hosting[10] to provide easy access to various resources. This led to the vendors collecting a massive amount of personal data from library users. Similarly, a massive surge in data generation from resource usage or the use of various online services (products, references, training and tutorials, etc.) forms an integral part of the library's services. According to Sawant[19], some of the most common services seen during the covid 19 pandemic was the remote access service. Sawant's also remarked on the most common services seen in India, like digital guides, e-contents and online references or increased participation in webinars. While personal data were considered as the new currency? This has led to 'Privacy compliance' gaining the spotlight. 'Privacy compliance,' from the library context, refers to the current privacy practices or obligations of library e-vendors in handling patrons' personal data and non-personal data (search queries, reading history, usage stats, etc) that were gathered, processed and shared using automated means or through users registration.

Privacy compliance for library vendors can be achieved with the implementation of privacy protection mechanism in place. The simplest way for vendors to achieve this is by incorporating an itemised 'Privacy Policy' to build the company image and enhance its value. In Jafar's and Abdullat's words[20], the privacy policy in a website keeps the users informed about policies and protocols concerning their data collection (like the use of cookies, web beacons, etc.), purpose of use, sharing, access to data, technologies used to secure the data and disclosure of personal information. However, apart from this, there were other reasons why privacy compliance can be important for vendors:

- Compliance with the 11 privacy principles articulated in Table 1 can safeguard patron's privacy rights and intellectual freedom.
- Non-compliance of vendors to abide by these principles may attract penalties and compensation from government agencies and libraries.
- Having a written notice or itemised privacy policy in place will instill trust in the users[21-23].

Table 1. The eleven (11) privacy principles for compliance by libraries and e-vendors

1	Data collection & notice	This principle laid down the collection of personal data, including online and offline data (subsequently converted into digitised formats). E-vendors must issue a privacy notice or itemised policy in simple language about the justifiable purposes of data collected from its users. ***For example:*** A user applies for library registration or online services to access e-resources. The e-vendor/ library may ask the patron to furnish (Personal data - University ID, Photo proof, Email, etc.) for communication and verification purposes. Before collecting personal data from users, the e-vendor or library shall give a clear privacy notice or e-policy to the user stating the purpose of obtaining these personal data for a specified purpose. It should also note the confidentiality policy of these personal data. DPDP Act: (Chapter I, Section 3); (Chapter II, Section 5(1 & 2a)); (Chapter IX, Section 40 (2a & b)).
2	Data retention	E-vendors must erase personal data unless required by law. E-vendors or libraries must cease storing digitised data when no longer serves the purpose or when users withdraw their consent. ***For example:*** E-vendor 'A' may share the user's personal data with e-vendor 'B' to create users' accounts. After the expiration of the subscription period or if users wish to withdraw the membership access, 'A' deletes the account. Once 'A' deletes the account, 'B' must stop retaining the personal data of 'A' or remove any identifiable data that can link to the users. DPDP Act: (Chapter II, Section 8, (7a & b)).
3	Data processing	This principle prohibits the processing of users' personal data without consent. Users may give voluntary consent provided that e-vendors/libraries must present an itemised notice or e-policy in simple language for a specific purpose. ***For example:*** A user downloads a digital library app. The app may request the user's consent for personal data processing, such as search queries to personalised searches. A user signifies his/her consent for processing search queries; hence, the consent shall be limited to processing only search queries and not processing the user's contact list, device location, etc. Also, when the users uninstall the app, the vendor shall cease to process user's data. An e-vendor may engage a data processor to process users' data to make helpful decisions for the users/services, but a data processor must not disclose the data to another e-vendor. DPDP Act: (Chapter II, Section 4-8).
4	Data sharing	Personal data breach means any unauthorised sharing of data that compromises the confidentiality, integrity or availability of personal data. While data sharing is a common practice, e-vendors/libraries must cease sharing personal data once they receive withdrawal requests from the users. E-vendors must stop sharing the personal data of users once its purposes were fulfilled or no longer required. But sharing shall be exempted in case of lawful prevention or investigation or punishable offences. ***For example*:** A user joins the online reference service to receive suitable article suggestions and hence shares his/her personal data for this purpose. Thus allowing the online reference service to process personal data in order to intimate the details of research articles available with the particular library. After that, the user may inform the online reference service that help is no longer required. Thus rendering the online service provider to cease sharing/processing of personal data. The government also restrict e-vendors/libraries the transfer of user's personal data to another e-vendor (outside India). However, this transfer shall be exempted in case of India's sovereign, research purposes, archives and statistical purposes (i.e., without affecting the person whose personal data the statistical analysis was carried out) DPDP Act: (Chapter II, Section 7(a)); (Chapter III, Section 11(1 & 2)); (Chapter IV, Section 16 & 17(2a & b)).
5	User's consent	Consent means the agreement between the users and the e-vendors/libraries regarding collecting, processing and retaining the user's personal data. E-vendors may appoint a consent manager (A person registered with the Data Protection Board of India) to manage, review, give and withdraw user's consent through a transparent and interoperable platform. Processing of user's personal data by e-vendors/libraries can only be done upon receiving user's consent. Every personal data request made by e-vendors shall be accompanied by a notice (or e-policy) in English or any language as specified in the eight schedules of Indian constitution. Users have the right to withdraw their consent at any time, but the users shall bear the consequences of withdrawal. The Act states that the withdrawal of consent shall not affect the processing of personal data based on previous consent before the withdrawal. ***For example:*** If e-vendor 'A' integrates its e-resources with another e-vendor 'B' who offers a discovery service such as federated searches. As part of their agreement, 'B' consents to processing users' data by 'A'. If user's withdraws consent to the processing of personal data by 'A', 'A' shall stop processing user's data immediately and this applies to e-vendor 'B' or others e-vendors with ties with e-vendor 'A'. DPDP Act: (Chapter II, Section 6(7-9)); (Chapter I, Section 2(g)); (Chapter II, Section 4-5); (Chapter II, Section 5(2b)); (Chapter II, Section 6(4-5)).

6	Children's data	According to this Act, a child is someone below 18 years old or a lawful guardian of such a child. E-vendors shall not process the personal data of a child that may cause harm. Before processing the child's personal data, the e-vendors/libraries must obtain verifiable parental consent. The e-vendors shall not track/ monitor children's behaviour or used them for targeted advertisement. ***For example:*** School libraries must take note of children's personal data by not sharing it with e-vendors or obtained consent from a lawful guardian if sharing is required. DPDP Act: (Chapter I, Section 2(j)); (Chapter II, Section 9(2-4)).
7	User's rights	This principle talks about various user's rights: • Right to access information about personal data (***For example:*** Personal data being processed or shared by e-vendors/libraries). • Right to correction & erasure of personal data (***For example:*** E-vendors or libraries upon receiving request from users, shall correct misleading or inaccurate personal data; complete user's partial data or update user's personal data). • Right to grievances redressal (***For example:*** E-vendors or consent manager shall provide available means to address user's grievances within a stipulated time before approaching the Data Protection Board of India). • Right to nominate (***For example:*** E-vendors shall not deny user's right to nominate another user to handle their personal data in case of death or incapacity (mind or body). The users shall also comply with their duties to provide accurate personal data, avoid using false information, and impersonate another individual to the e-vendors/libraries per the applicable law. DPDP Act: (Chapter III, Section 11(a & b)); (Chapter III, Section 12(1-2)); (Chapter III, Section 13(1-3)); (Chapter III, Section 14(1-2)); (Chapter III, Section 15).
8	User's security	It is required for e-vendors/libraries to implement the latest security protocols to protect personal data under their possession. ***For example:*** To prevent privacy breaches, e-vendors/libraries must use the newest encryption tools and web technologies - Https, Privacy-enhancing technologies, plugins and extensions, anonymised users, etc. DPDP Act: (Chapter II, Section 8(5)).
9	Reporting	E-vendors must report any privacy breach to the data protection board of India and its affected users. It is the board's responsibility to develop measures for e-vendors to avoid data breaches that may harm users. To suggest remedial measures in the event of data breach reported by the users; to impose restrictions on e-vendors in case of breach and impose appropriate penalties. ***For example***: The e-vendors shall notify the library and its users immediately if library records or personal data breaches occur. Similarly, the e-vendors must also report the same to the board or governing body prescribed by law. DPDP Act: (Chapter II, Section 8(6)); (Chapter VI, Section 27(a-e)).
10	Accountability	E-vendors shall appoint a Data Protection Officer (DPO) based in India who shall acts as a point of contact to address user's grievances. E-vendors shall provide DPO's contact information in a transparent manner. A DPO must be accountable towards the board or a similar governing body as prescribed by law. A DPO must evaluate the compliance of e-vendors with the current regulations and conduct regular data assessments to ensure transparency. E-vendors shall appoint an independent data auditor who will study the e-vendor's data impact assessment from time to time. ***For example***: If library users need clarification about the e-vendor's privacy policies or data breaches, they can always communicate with the DPO, whose job is to answer questions (in plain English) on behalf of the e-vendors. Libraries must insist for DPO's contact information to be readily available on e-vendors website. DPDP Act: (Chapter II, Section 10(2)); (Chapter II, Section 6(3) & 8(9)).
11	Compensation	In the event of data breaches, complaints received from users or non-compliance by e-vendors; it is the responsibility of the Data Protection Board of India to inquire and impose penalties. This principle specifies penalties for non-compliance of e-vendors depending on the nature and type of offences. The penalties may range from INR 10,000 for non-compliance to INR 250 crore, depending upon the nature and type of data breach. ***For example:*** The library must consult a legal expert on this principle before drafting a library privacy policy. DPDP Act: (Chapter VI, Section 27); (Chapter VIII, Section 33); (The Schedule).

Source: Digital Personal Data Protection Act, 2023[18]

- Complying with these principles will help gain the trust of library users and library organisations. This will also put an e-vendor a step ahead in a competitive market.
- Enabling up-to-date security and privacy tools to secure the usage of digital services may help e-vendors prevent future privacy violations and breaches.

6. WHAT ARE THE SUGGESTIONS FOR LIBRARIES?

As more online service providers recognise the market value of data analytics, it is expected for librarians to

see efforts on the part of e-vendors/libraries to obtain more personal information from library users in the future. Magi[8] pointed to the extent vendors may use to cover the front of data collection techniques to improve users' experience (Examples: save keywords searches, read favourite or preferred articles, etc.). Magi remarked that such practices might provide convenience to users; however, Magi's study revealed that vendors do not commit to the privacy value the librarians uphold[8]. Therefore, library professionals must track how this personal and non-personal information is collected and used. If not checked, librarians must at least be cautious while reading through the contracts before opting for services rendered by third-party vendors. The following points summarize the lesson learned for library professionals to be proactive in protecting users' privacy:

- Libraries must devise their own itemised privacy policy when setting up digital libraries or offer online services from third-party vendors that reflect the 11 privacy principles in Table 1. It should be written in simple, transparent and easy-to-comprehend statements[7]. While doing so, it is recommended that vendors adhere to the privacy standards that were laid down by the American Library Association (ALA) code of ethics[8-9]. Libraries may also refer to their regional regulatory guidelines, Professional associations guides, or data protection authority.
- Library and vendor privacy policies should be flexible enough to meet local needs. This is particularly applicable to cloud-based services and library 2.0 solutions, said Kritikos & Zimmer's[24] to avail interactive services and explore library resources freely.
- Ideally, libraries should post their privacy policies in areas easily accessible by patrons, thereby providing direct access to the privacy policy on the library homepage[24]. Ease of access is vital for both libraries and vendors alike; doing so will demonstrate their commitment towards data transparency.
- Kristikos's & Zimmer's[24] also share their concerns regarding libraries' reliance on third-party service providers to maintain their privacy policies, especially since libraries commitment to patron privacy might not coincide with third-party technology providers' interests. Hence, librarians must insist on the need to keep the vendor's privacy policy up-to-date, accurate and aligned with library privacy policy.
- Library professionals must ask questions in case of generic and unclear privacy statements in the vendor's contract. Libraries can focus on the missing elements from vendor policies and negotiate accordingly to improve their understanding of these privacy issues[10].
- According to Eroğlu & Çakmak's[13], library administrators in Turkey expressed uncertainty about using personal data in library services. Their results pointed out the lack of awareness concerning personal data privacy. To bridge this, education in the form of receiving staff training, attending workshops and providing orientation may enhance privacy literacy. The inclusion of online security and privacy topic into the library science syllabus might go a long way to educate the future custodian of knowledge.
- Librarians must emphasise to vendors the de-identification or anonymisation of patron's data in the web environments. If personal data were shared, it should be anonymised and aggregated to safeguard the patron's privacy[10].
- Libraries should discourage using web analytics services like Google Analytics (GA) or other third-party tracking embedded in library websites or solutions. Libraries should allow only basic tracking needed to avail services without hampering users' experience. Online libraries systems and services should use the latest encryption technology to protect their users; the same is to be insisted on vendor's services. An example of a secure connection includes using HTTPS websites that redirect to a secure connection or Internet Protocol (IP) anonymisation[25].
- When implementing cookie management schemes into products and solutions, librarians must insist on 'Cookie compliance' with the vendors according to GDPR regulations or ePrivacy Directive (EPD)[26]. Principle no. 5 in this study also discussed about taking users' consent before collecting, storing, sharing and processing personal data.
- Libraries should encourage the use of privacy-enhancing technologies (PET) to ensure security and privacy for library users. This can be done by using PET to secure connections between Internet users and the services (or solutions) platforms. Examples of PET include-checking for a privacy badge or seal on the vendor's website, use of privacy plugins or extensions, ads blockers, privacy-focused browsers like Brave and Tor, use of Virtual Private Networks (VPN), etc. Grooming patrons with these tools may guarantee their privacy safety while seeking information from the web[7].
- Libraries should also set up their clauses and terms before signing the vendor's contract. Libraries may include the termination of services or compensation in case of privacy breach. Monetary penalties may also apply in accordance with local government regulations.

These suggestions above may act as a starting point for libraries to take the requisite steps to safeguard their patrons' personal data rights.

7. FUTURE OF THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

The DPDP Act due to its recent enactment may invite multiple regulatory improvements in the future. The incorporation of offline data (with subsequent conversion to online data) provides more clarity to Indian consumers and online library users. The exemption of government agencies from applying the DPDP Bill on grounds such as the state's security, public order, and prevention of offences may violate the fundamental right to privacy.

Also, it did not mention the right to data portability or the right to be forgotten, as was mentioned in the previous draft of 2019. However, it may incorporate emerging privacy implications that may arise from evolving socio-technological changes. Also, its affect towards consumers, e-vendors, businesses, and overall economic growth were yet to be felt.

8. LIMITATION

In short, reviewing the DPDP Act was extensive and conceptually difficult from the library contexts. This may limit the author's comprehension, but efforts were made to cover relevant concepts and supplement with recent literature to understand personal data in web environments. Unlike known organisations like the American Library Association (ALA), the International Federation of Library Association (IFLA), the Australia Library and Information Association (ALIA) that has 'Privacy Standards' or 'Library Code of Ethics.' Nevertheless, these standards and privacy guidelines were still nascent in India. This absence of privacy literature has rendered this review from giving Indian references.

9. DISCUSSION

The eleven (11) privacy principles obtained from the DPDP Act may act as a get-go for Indian libraries to tackle the issues of patron's privacy. The first principle, 'Data collection,' aims to limit the collection of personal data. This concerns the excess collection of patron's search history, which reflected in Magi's[8] evaluation of the 27 e-journal vendors. This concern was also evident in the attitude study in Ghana, which revealed that 50 % of librarians and 50.4 % of students either agree or strongly agree that vendors collect too much personal data in online library systems[27].

The formation of (see Principles no. 1&2) in this review were also in line with the American Library Association, who passed a "Resolution on the Retention of Library Records," which educates library organisations to avoid collecting, storing and creating unnecessary records. These principles insist on maintaining strict security of patron records[9].

When it comes to designing a notice or privacy policy as indicated in (see Principle no.1). Vendors and libraries must insist on creating an itemised privacy policy that fits the ever-changing socio-technological landscape; while keeping in mind the simplicity of a statement when drafting a privacy policy. According to Jafar's and Abdullat's pointers, a privacy policy must be written using clear and simple word choices[20]. This way, patrons will be kept well-informed and well-aware. The third principle, 'Data processing,' aims to limit how vendors process personal information from patrons. Lambert[9], *et al.* even remarked on this uncontrolled data processing of personal information as a violation of fundamental rights.

While 71.6 % of librarians and 80.9 % of students agree or strongly agree that libraries should never share personal information or circulation data with third parties unless prescribed by the law[27]. This notion to safeguard unauthorised sharing of patron's data were expressed in (see Principle no. 4). This may also apply to third-parties integration such as social media in online library services.

The fact as to why taking patron's consent (see Principle no. 5) is necessary because a study by McKinnon and Turp has shown that online library vendors such as EBSCO, Ex Libris, OCLC and SirsiDynix did not indicate how they share patron's information after acquiring patron's consent; even though they claimed to follow strict privacy standards[10].

In the context of (see Principles no. 5, 7&9), the library 'codes of ethics' have already devised the importance of giving patrons a control over their online privacy. As Eroğlu & Çakmak's remarked, losing control over patron's personal information in libraries will result in privacy breaches and may undermine patron's trust in the library system[13]. A survey of 74 librarians and 752 students in Ghana also revealed that 75.7 % of librarians and 86.5 % of students either strongly agree or agree that patrons should be able to control who sees their personal data[27].

The growing concerns about the security of patron's personal information were definitely felt and thus addressed by (see Principle no 8) in this review. This concern was expressed by 91.9 % of librarians over the security of personal data given to third-party vendors[27]. Mckinnon's and Turp's evaluation of library vendors' privacy policies indicates that all four (4) vendors' policies mentioned how data was stored and secured; however, all these vendors do not mention patron anonymity[10]. This means that the patron's online identity could be at risk. This was also highlighted in (see Principle no 8), which stipulate that vendors or libraries must maintain full control over their online service to prevent third parties violations and also laid down protocols to safeguard privacy breach, such as setting up a reporting authority (see Principles no. 8, 9&10).

10. CONCLUSION

To conclude, this review discusses the implications of the DPDP Act from online library environments. The current privacy gaps in libraries reported in the latest literature was addressed by the eleven (11) privacy principles summarised in this study; these principles may act as privacy guidelines for libraries and e-vendors. It will also create awareness about privacy policies in Indian libraries. The corrective measures suggested, like de-identification of patrons' data, limiting the use of web tracking, mandating a privacy policy as part of library policies, set-up owns privacy terms and conditions, might go a long way towards protecting library users. The Indian government has achieved milestones in implementing new policies and its efficiency in dealing with issues at the local, national and global levels. However, it is hopeful that with the implementation of the DPDP Act, libraries in India will also follow the footsteps of this Act.

REFERENCES

1. Keelery, S. Internet usage in India - statistics & facts. Statista. 2021. Retrieved from, https://www.statista.com/topics/2157/internet-usage-in-india/#dossierContents__outerWrapper (accessed on 1 July 2022).
2. Digital India. Digital India Initiatives. 2022. Retrieved from, https://www.digitalindia.gov.in/di-initiatives (accessed on 20 June 2022).
3. Business Today. India ranks third in global data breaches in 2021. https://www.businesstoday.in/latest/trends/story/india-ranks-third-in-global-data-breaches-in-2021-report-315750-2021-12-15 (accessed on 15 June 2022).
4. Ghosh, S. The biggest data breaches in India. CSO Enterprise. 2021. Retrieved from, https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html (accessed on 1 July 2022).
5. De, S.J. & Shukla, R. An analysis of privacy policies of public COVID-19 apps: Evidence from India. *J. Public Affairs*, 2021. doi: 10.1002/pa.2801.
6. Javed, Y.; Salehin, K.M. & Shehab, M. A Study of South Asian websites on privacy compliance. *IEEE Access,* 2020, **8**, 156067–156083. doi: 10.1109/ACCESS.2020.3019334.
7. Bareh, C.K. Assessment of the privacy and security practices of the Indian academic websites. *Library Philosophy & Practice (e-Journal)*, 2021, 6426. https://digitalcommons.unl.edu/libphilprac/6426/ (accessed on 9 January 2022).
8. Magi, T.J.A content analysis of library vendor privacy policies: Do they meet our standards? *College and Res. Libraries*, 2010, **71**(3), 254–272. doi: 10.5860/0710254.
9. Lambert, A.D.; Parker, M. & Bashir, M. Library patron privacy in jeopardy an analysis of the privacy policies of digital content vendors. *Proceedings of the Association for Information Science and Technol.,* 2015, **52**(1), 1–9. doi: 10.1002/pra2.2015.145052010044.
10. McKinnon, D. & Turp, C. Are library vendors doing enough to protect users? A content analysis of major ILS privacy policies. *J. Academic Librarianship,* 2022, **48**(2), 102505. doi: 10.1016/j.acalib.2022.102505.
11. American Library Association. Privacy. American Library Association, 2021. Retrieved from, https://www.ala.org/advocacy/privacy (accessed on 1 July 2022).
12. Zimmer, M. Librarians' attitudes regarding information and internet privacy. *Library Quarterly*, 2014, **84**(2), 123–151. https://www.jstor.org/stable/10.1086/675329.
13. Eroğlu, Ş. & Çakmak, T. Personal data perceptions and privacy in Turkish academic libraries: An evaluation for administrations. *J. Academic Librarianship*, 2020, **46**(6), 102251. doi: 10.1016/j.acalib.2020.102251.
14. Manjunathan, M. India: Privacy and Data Protection Laws in India (Part 3). 2022. https://www.mondaq.com/india/privacy-protection/1170436/privacy-and-data-protection-laws-in-india-part-3?type=popular (accessed on 10 March 2022).
15. Chopra, R. & Mansharamani, M. India: Privacy in India: Data Protection Bill and OTT Regulations. 2021. Retrieved from, https://www.mondaq.com/india/data-protection/1089802/privacy-in-india-data-protection-bill-and-ott-regulations-#:~:text=India%3A Privacy In India%3A Data Protection Bill And,THE PRESENT SCENARIO. ... 4 OTT REGULATIONS. (accessed on 16 July 2021).
16. Trilegal India: The Data Protection Bill, 2021. Retrieved from, Mondaq. https://www.mondaq.com/india/privacy-protection/1145790/the-data-protection-bill-2021 (accessed on 30 December 2021).
17. Alpha Partners. India: Update on Data Protection Law. 2022. Retrieved from, https://www.mondaq.com/india/privacy-protection/1146570/update-on-data-protection-law?type=popular (accessed on 3 January 2022).
18. Digital Personal Data Protection Act, 2023. https://prsindia.org/acts/parliament (accessed on 16 September 2023).
19. Sawant, S. Services offered by Indian libraries during covid-19. *Annals of Library and Information Studies*, 2021, **68**(3), 230–237. http://op.niscair.res.in/index.php/ALIS/article/view/41395 (accessed on 3 March 2022).
20. Jafar, M.J. & Abdullat, A. Exploratory analysis of the readability of information privacy statement of the primary social networks. *J. Business & Economics Research (JBER)*, 2009, **7**(12). doi: 10.19030/jber.v7i12.2371.
21. Aïmeur, E.; Lawani, O. & Dalkir, K. When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior*, 2016, **58**, 368–379. doi: 10.1016/j.chb.2015.11.014.
22. Chang, Y.; Wong, S.F.; Libaqye-Saenz, C.F. & Lee, H. The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, 2018, **35**(3), 445–459. doi: 10.1016/j.giq.2018.04.002.
23. De, S.J. & Shukla, R. Privacy policies of e-governance initiatives: Evidence from India. *J. Public Affairs*, 2020, **20**(4), 1–11. doi: 10.1002/pa.2160.
24. Kristos, K.C. & Zimmer, M. Privacy policies and practices with cloud-based services in public ibraries: An Exploratory case of BiblioCommons. *J. Intellectual Freedom and Privacy*, 2017, **2**(1), 23-37. https://journals.ala.org/index.php/jifp/article/view/6252/8394 (accessed on 25 March 2022).
25. O'Brien, P.; W.H. Young, S.; Arlitsch, K. & Benedict, K. Protecting privacy on the web: A study of HTTPS and Google analytics implementation in academic library websites. *Online Infor. Review*, 2018, **42**(6),

734–751.
doi: 10.1108/OIR-02-2018-0056.
26. General Data Protection Regulation. Cookies, the GDPR, and the ePrivacy Directive. 2022. https://gdpr.eu/cookies/ (accessed on 30 June 2022).
27. Avuglah, B.K.; Owusu-Ansah, C.M.; Tachie-Donkor, G. & Yeboah, E.B. Privacy issues in libraries with online services: Attitudes and concerns of academic librarians and university students in Ghana. *College and Research Libraries*, 2020, **81**(6), 997–1020. doi: 10.5860/crl.81.6.997.
28. Bareh, C.K. Privacy policy analysis for compliance and readability of library vendors in India. *Serial Librarian*, 2022, **83**(2), 148-165. doi: 10.1080/0361526X.2022.2143467.

CONTRIBUTOR

Mr Chanlang Ki Bareh is a Assistant Librarian in the Central Library at Nagaland University, India. He holds an MLISc degree and is simultaneously pursuing a PhD programme in the area of Information behaviour and Privacy Studies from the Department of Library & Information Science at North-Eastern Hill University, India.