South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Privacy Paradox in Industry 4.0: A review of library information services and data protection

Authors:
Yumnaa Ocks[1]
Oghenere G. Salubi[1]

Affiliations:
[1]Department of Library and Information Science, Faculty of Arts, University of the Western Cape, Cape Town, South Africa

Corresponding author:
Yumnaa Ocks,
3337222@myuwc.ac.za

Dates:
Received: 25 Feb. 2024
Accepted: 25 July 2024
Published: 29 Aug. 2024

How to cite this article:
Ocks, Y. & Salubi, O.G., 2024, 'Privacy Paradox in Industry 4.0: A review of library information services and data protection', *South African Journal of Information Management* 26(1), a1845. https://doi.org/10.4102/sajim.v26i1.1845

Background: In the wake of Industry 4.0, libraries are integrating Fourth Industrial Revolution (4IR) technologies to enhance efficiency. However, this shift in practice raises ethical and privacy concerns, particularly regarding the *Protection of Personal Information Act* (*PoPI Act*).

Objectives: This literature review explores the ethical and privacy challenges posed by 4IR technologies in delivering information services to library patrons including the impact on *PoPI Act* compliance in addressing data privacy concerns.

Method: Adopting a systematic approach, this literature review employs the Preferred Reporting Items for Systematic Reviews and Meta-Analyses flowchart and inclusion criteria focussed on 4IR in libraries and its relation to the *PoPI Act*. Peer-reviewed articles in English from 2013 to 2023 were sourced from scholarly databases.

Results: The review highlights the transformation of academic library services in the 4IR era and the consequent privacy challenges. Concerns arise from advanced library systems and extensive data retention. While libraries operate non-profitably, the adoption of 4IR technologies for data acquisition mirrors commercial practices, raising ethical questions. Patron privacy issues extend beyond traditional data collection to potential misuse and improper data handling as libraries often work with vendors.

Conclusion: The integration of 4IR technologies in academic libraries necessitates a delicate balance between improved services and safeguarding user privacy and the *PoPI Act* serves as a crucial regulatory framework. Librarians must navigate the evolving landscape of data ethics, emphasising transparency, accountability and adherence to privacy legislation.

Contribution: The introduction of artificial intelligence and 4IR technologies to library information services has unlimited possibilities including countering misinformation and disinformation, and the expansion of library services to tech-savvy users beyond the physical walls of the library building. However, the deployment of these technologies raises new questions about ethical concerns that the use of these technologies poses to information professionals in the rendition of library services. The results of this study will be useful for policy and professional practice in taking full advantage of 4IR technologies and services.

Keywords: Industry 4.0; F-TechEthix; privacy; academic libraries; information ethics; *PoPI Act*.

Introduction

Humanity has dedicated extensive efforts to comprehend the forces of nature and enhance survival prospects through the progression of scientific research and technological implementation (World Economic Forum 2023). The emergence of Industry 4.0 has not only introduced new products and innovative practices but has also integrated them into libraries, thereby elevating the efficiency of library services. In the realm of higher education, academic libraries hold a pivotal role, providing crucial support for teaching, learning and research endeavours of faculty, students and lifelong learners alike (Cook 2019). However, at a global scale, the Fourth Industrial Revolution (4IR) has brought about substantial changes in the daily operations of libraries and information centres. This transformation necessitates a profound shift in their practices to effectively cater to the dynamic and multifaceted requirements of their user base. However, it is important to note that this transformation has shaped how libraries protect patron privacy, concerns the computerisation of library services and operations, and the transformation of libraries into digital consumers. Libraries today consume various network-based products that manage information systems and services for patrons. Palmer, Freeman and Geary (2020) concur and indicate that the shifting method of content and service provision comes with new concerns for the collection, retention and use of patron data. In this context, Chigwada and Nwaohiri (2021) argue that addressing the challenges posed by 4IR demands interdisciplinary and collective competencies, integrating knowledge and skills from the realms of electronics, machinery and information communication.

Phillips (2020) argues that personal data should be safeguarded based on the fundamental right to privacy by regulating its processing and proving individuals' rights over data (Phillips 2020). Studies show that before 2022, over 120 countries had enacted privacy and data protection laws (Thales 2019). The last decade, 2010–2019 saw a record of 62 countries enacting data protection laws (Greenleaf & Cottier 2020). These legal advances include the United Kingdom (UK) 2016 General Data Protection Regulation (GDPR) to safeguard personal data from unlawful handling, processing and access. This shows that the interest in data protection is gaining momentum because of pressure to meet international trade requirements and fulfil the fundamental right to privacy.

Furthermore, the integration of cutting-edge technologies such as 5G, big data, the Internet of Things (IoT) and artificial intelligence (AI) has not only heightened the efficiency of libraries but has also empowered them to make evidence-based decisions. According to Michalak and Rysavy (2019), there is a growing trend in academic libraries, where the utilisation of personally identifiable information (PII), specifically patron data, has become a prevalent practice for informed decision-making through learning analytics programmes. The examination spans global libraries and highlights instances of PII application in decision-making related to operational aspects such as library hours (gate count), electronic resources (collection usage and authentication) and research assistance (virtual reference).

The utilisation of data analytics emerges as a pivotal tool, contributing to a comprehensive understanding of customer preferences and the dynamic shifts within the market, consequently optimising the overall efficacy of library operations (World Economic Forum 2016). In this era of technological advancement, library patrons now enjoy seamless and cost-effective access to the digital realm, transcending geographical constraints and time limitations. The convenience of accessing library services has reached unprecedented levels, enabling patrons to connect with information resources both on and off campus with a mere Internet connection. Studies have noted the profound impact of technological proliferation on libraries, patrons and society at large, with notable implications for privacy (Hess, LaPorte-Fiori & Engwall 2015; Witt 2017). Over the years, concerns regarding the privacy of library patrons have escalated, primarily attributed to advanced library systems, legal rulings and the extensive retention of data by libraries (Gayshun 2015).

Libraries, librarians and privacy

For libraries and information professionals to unlock the full potential of Fourth Industrial Revolution (4IR) technologies in providing effective and efficient information services, a comprehensive examination of opportunities and risks associated with these technologies is imperative (Makori & Bitso 2021; Salubi 2023). Standardised professional ethical practices must also be scrutinised and analysed in light of the *Protection of Personal Information Act* (*PoPI Act*). While libraries have held 'privacy value' dearly over the past decades, studies show that not all library vendors uphold the same value (Bareh 2022). Libraries enter into contracts with vendors to meet their daily operational needs, such as digital content, consortium, library automation software, cloud hosting, etc. While providing services, most third parties collect patron data for personalisation or analytics in numerous ways. Alongside the growth in outsourcing library services to third-party vendors, patrons are increasingly encouraged to engage in their integrated social and Web 2.0 features, ranging from maintaining user profiles, creating book lists, communicating and sharing resources with other users. Many platforms also aggregate patron data to fuel algorithmic filtering, provide personalised content, suggest recommendations and help analyse trends. In fact, studies show that patrons have difficulty understanding whether they are using library services offered by their institutional library or they are linked to an external site. This is coupled with the lack of technical know-how to tackle these issues. However, working alongside vendors is essential to provide better service while considering users' privacy. A study conducted by Avuglah et al. (2020) highlights the results showcasing the attitudes, perceptions and concerns of students in relation to online privacy in the library. The results indicated that they were concerned about privacy while using the Internet, nearly all the respondents (91.7% of students) indicated that they were very concerned or somewhat concerned. The results further show that 79.9% of students said they were very concerned or somewhat concerned about family, friends and other acquaintances getting personal information about them and their web activities. Similarly, 83% of students were either very concerned or somewhat concerned about businesses and people whom they do not know getting personal information about them and their web activities. Consequently, library privacy is a crucial aspect, because of the 'chilling effect', in which users become aware or suspect that they are being monitored and change their behaviour as a result. Equipped with this information, librarians are responsible for safeguarding patron's privacy, and they would need to have the necessary information to negotiate contracts more reflective of their profession's standards.

It is therefore crucial that academic libraries are responsive institutions that recognise the need for data privacy within their walls and proactively institute and act upon policies that address this need. This study aims to assess the ethical and privacy dilemmas arising from the integration of 4IR technologies in delivering information services to library patrons, specifically within the framework of the *PoPI Act* passed in South Africa. The extensive collection and utilisation of data pose a threat to individual privacy, carrying both social and legal consequences (Gayshun 2015). Furthermore, if patrons perceive a lack of privacy in their interactions with library content and services, they may opt to abstain from utilising library resources altogether (Corrado 2022).

Despite academic libraries operating as non-profit entities, the incorporation of information services in the era of Industry 4.0 mandates the adoption of technologies akin to those employed by for-profit Internet service providers for user data acquisition (Wissinger 2017). Personal data have emerged as a valuable asset, globally traded and exploited by some organisations for marketing purposes. The distinctive feature lies in the non-commercial nature of data utilisation within libraries. However, similar to the contentions surrounding the commodification and privacy of users in commercial settings, these issues must be addressed to fully harness the benefits of these technologies for libraries and users alike (Maceli 2019). The conflict between the desire to use personal data to inform decision-making and the desire to uphold patron privacy has tremendous ramifications for the future of academic libraries.

A study of public library data policies in the United States of America, involving a random sample of 1000 libraries, revealed that less than half had a data privacy policy (Mohammed 2020). The study concluded that many public libraries lack online data privacy policies, emphasising the importance of broader accessibility and the implementation of these laws. Presently, little is known about the landscape of data privacy among libraries. Unlike some aspects of public services, like higher education accreditation, there is little oversight on the services and support that public libraries must provide in terms of privacy measures. The evolving landscape of threats to patrons' privacy in libraries is fuelled by novel technologies that extend beyond the traditional physical library space. Recognising this shift, libraries are actively engaging in educating patrons about privacy threats, protective measures and available tools. Maceli (2018) noted key challenging issues faced by libraries in effectively educating and advocating for the use of privacy-protection technology tools including substantial technology-related knowledge gaps among patrons, librarians and library staff, the need to support a diverse array of technology tools and techniques, and the importance of gaining insights into the perspectives of the creators behind these tools. A European study was carried out by Lund (2021) to analyse privacy policies concerning patron data on public use computers across 1000 randomly selected public libraries from an initial population of over 8000 listed in the Institution of Museum and Library Services' Survey. The results of the study indicate that less than half (44.6%) of the sampled libraries have a data privacy policy, with approximately two-thirds of these libraries having updated their policies in the last 5 years. Conversely, 15.9% of the policies were last updated before 2016, with the oldest update dating back to 2002. Over the years, there has been an increasing adoption of cloud-based and Library 2.0 solutions by libraries to offer patrons more interactive and user-focussed platforms for accessing library resources. However, these platforms often involve the collection and aggregation of patron data, raising concerns about potential disruptions to long-standing ethical norms in librarianship focussed on safeguarding patron privacy. Kritikos and Zimmer (2017) noted in their findings from a pilot research study on how libraries are implementing third-party cloud computing services, the potential impact on patron privacy, and how libraries are addressing these concerns, suggesting limited adjustment or implementation of specific privacy-related practices. Gangadharan (2016) shares this sentiment and elaborates that within these environments, libraries generate new kinds of patron data in their roles as digital providers, and contract services with third-party vendors who, in turn, generate new kinds of data about patrons. He highlights the fact that within this context, the institutional practice of defending privacy arguably also grows more complex; the number and types of threats to patron data multiply with each digital offering made available in the library setting, which leaves patrons at risk of being spied on, targeted or victimised through the unfair or illegal use of data, patrons face a range of government and commercial threats at various points in their library experience.

Studies also reveal that professionals and researchers often disagree as to the extent to which a privacy or access balance should be maintained. Authors like Nicholson and Smith (2007) lean in favour of a strict privacy policy. Others, however, are more in favour of adopting new technologies as soon as possible, overlooking short-term privacy implications (Quach, Thaichon & Martin 2022). Research also reveals that while security professionals perceive prudent and responsible behaviour as crucial, users view it as an overhead that impedes their ability to accomplish their tasks (Harrison 2006). This is further elaborated by Tam et al. (2020), who suggested examining the trade-offs users make with respect to computer security. Applying the negative externality concept from economics to security, he suggests that most users are not concerned about security because they believe the immediate and negative consequences of a security breach will affect others rather than themselves. Kim and Noh (2014) indicated that though many patrons had a strong interest in preserving their privacy, most had little knowledge of their library's specific privacy practices or what is necessary for privacy to be maintained. Patrons seemed particularly concerned about the sharing of information with third parties, with more trust in libraries and library employees than others outside of the library. Kritikos and Zimmer (2017) indicated similar concerns in their study of third-party library cloud computing platforms.

Research by Tummon and McKinnon (2018) on Canadian academic librarians' perspectives on privacy-related issues noted concerns about online privacy, identity theft and tracking by various entities are evident. The study further reported that the majority of respondents feel that libraries should never share personal information without authorisation, but opinions on whether libraries are doing enough to prevent unauthorised access are more varied. A notable majority express increased concern about privacy compared to 5 years ago, often attributing it to a heightened awareness of risks and political climate. The findings offer insights into Canadian academic librarians' perspectives on privacy-related issues and practices within their institutions.

Methodology

A systematic approach was used in this review. The systematic approach to literature review is distinguished by a meticulously outlined review process that is both well-defined and replicable. It follows a series of explicit steps, providing substantiated justifications for the inclusion or exclusion of articles. Furthermore, systematic reviews are a way of synthesising scientific evidence to answer a particular research question in a way that is transparent and reproducible, while seeking to include all published evidence on the topic and appraising the quality of this evidence. It considers topical focus areas, geographical locations, research methodologies and other relevant variables, all of which contribute to delineating the boundaries of knowledge evident in the literature (Liberati et al. 2009; Moher et al. 2009). In this search process, we employed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flowchart, adapted from Moher et al. (2009). The PRISMA statement, designed to assist systematic reviewers in transparently reporting the purpose, methods and findings of the review, was utilised in this study (see Figure 1).

The review included the following five-step process and is tabulated below:

- The definition of the inclusion and exclusion criteria (Table 1)
- Data sources and strategies
- Quality assessment of resources
- Extracting relevant materials from the search outcomes
- Synthesising and presenting the findings.

Step 1: Inclusion and exclusion criteria

The inclusion criteria are the elements of an article that must be present in order for it to be eligible for inclusion in a review. Conversely, the exclusion criteria are the elements of an article that disqualify the study from inclusion in the review (see Table 1).

Step 2: Data sources and search strategies

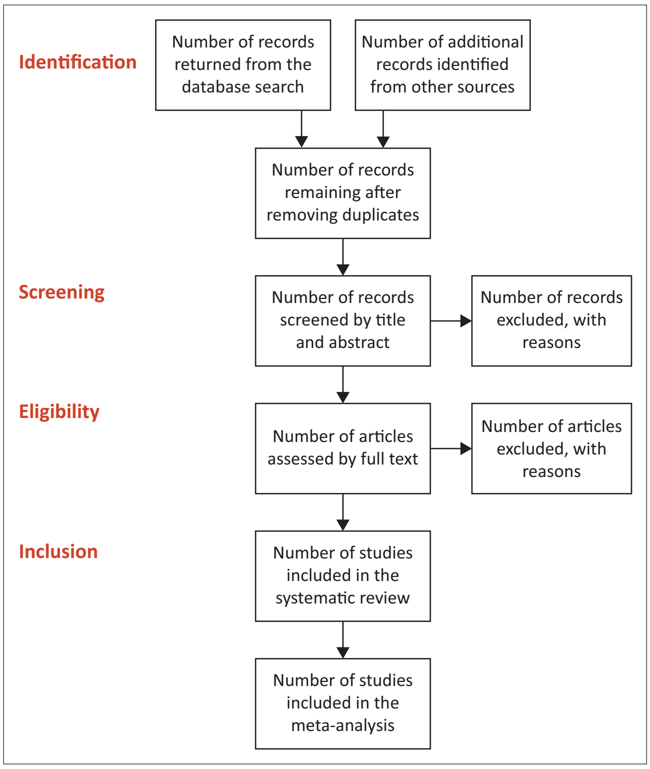
In this systematic review, comprehensive literature searches were systematically carried out across various academic electronic databases, including Academic Search Complete, EBSCOhost, Research Gate, Taylor & Francis and Google Scholar. These databases were deliberately chosen because of their repository of high-quality, peer-reviewed academic literature. The search criteria incorporated specific keywords such as 'artificial intelligence', 'academic libraries', 'data privacy', '4th Industrial Revolution' and 'user privacy'. The timeframe for the inclusion of studies spanned from 2013 to 2023. The collective searches across these platforms yielded a substantial pool of 7330 records. Subsequently, employing rigorous inclusion and exclusion criteria, a refined selection process resulted in the inclusion of 27 articles for further analysis.

Step 3: Quality assessments of resources

A fundamental element of a systematic review involves conducting a quality assessment, in conjunction with establishing clear inclusion and exclusion criteria, as emphasised by Al-Emran et al. (2018). In our pursuit of maintaining the utmost quality in the literature considered for this study, we devised a meticulous checklist. This checklist aimed at identifying the most pertinent articles addressing the ethical and privacy challenges arising from the implementation of 4IR technologies in delivering information services to library users. Particularly, we explored the implications for information professionals and libraries in the context of the *Protection of Personal Information Act* (*PoPI Act*).

Ethical considerations

Ethical clearance was received from the University of the Western Cape Research and Ethics Committee (reference no: HS23/1/17 and permission reference no.: UWCRP507795).


Identification
Number of records returned from the database search
Number of additional records identified from other sources
Number of records remaining after removing duplicates
Screening
Number of records screened by title and abstract
Number of records excluded, with reasons
Eligibility
Number of articles assessed by full text
Number of articles excluded, with reasons
Inclusion
Number of studies included in the systematic review
Number of studies included in the meta-analysis

Source: Edanz, 2023, *The 4 stages of a PRISMA flow diagram*, viewed n.d., from https://www. edanz.com/blog/prisma-flow-diagram

FIGURE 1: Preferred reporting items for systematic reviews and meta-analyses flow diagram.

TABLE 1: Inclusion and exclusion criteria.

Inclusion criteria	Exclusion criteria
Related to 4IR in libraries	4IR that is not related to libraries
Related to online privacy and libraries	Online privacy that is not related to libraries
Does not duplicate studies	Duplication of studies
Peer reviewed literature	Non-peer reviewed literature
English language	Language other than English (full text)
Informative or credible results	Not informative or credible results

4IR, Fourth Industrial Revolution.

Research findings

Privacy and privacy acts in information services provision in Industry 4.0

Contemporary libraries are increasingly shifting their focus towards meeting the evolving needs and experiences of their users, transforming into hubs of learning, instruction and research. Recognising that it is imperative to adapt to patrons' ever-changing information requirements, academic libraries and librarians are actively exploring innovative modes and models for library services to stay relevant (Yassin 2022). For librarians committed to delivering high-quality services, adopting a perspective grounded in critical inquiry, assessment and thoughtful design is essential. This approach involves planning, delivering and assessing services based on collected data and evidence. Librarians play a pivotal role in staying abreast of cutting-edge technologies and seamlessly integrating them within the library to enhance the overall experience for patrons (McKinnon & Turp 2022). Libraries are proactively exploring avenues to engage with learning analytics, aligning these insights with both student and patron success, as highlighted by Oakleaf (2018). This proactive stance underscores the dynamic nature of contemporary libraries and their commitment to continually enhancing user experiences and outcomes. However, it is crucial to note that some of these technologies such as the Internet and social media are a menace to information security challenges. Some of these risks include authorised access, theft and the unlawful use of information classified as confidential and sensitive (Masilela & Nel 2021).

A 2018 study of 279 academic library websites, focussing on the privacy implications associated with web tracking reported a limited adoption of Hypertext Transfer Protocol Secure (HTTPS) on library websites, with many lacking secure connections and automatic redirects. Despite the widespread use of Google Analytics and/or Google Tag Manager, only a few libraries establish secure connections to Google via HTTPS or employ Internet Protocol (IP) anonymisation in Google Analytics (O'Brien et al. 2018). The study underscores the need for increased awareness among librarians, advocating coordinated action in areas such as implementing secure web protocols, enhancing user education, formulating robust privacy policies, obtaining informed consent and conducting thorough risk/benefit analyses to address privacy concerns related to web tracking on academic library websites. An investigation on the unintended implications of third-party resources on Association of Research Libraries (ARL) member homepages, specifically focussing on the prevalence and implications of third-party tracking cookies was carried out through an examination of 124 ARL member libraries. According to Marino (2021), the study revealed that a substantial portion of these institutions contributes to user tracking, with one-third featuring third-party tracking cookies. Notably, the findings highlight variations in user interactions with tracking cookies based on institutional traits, emphasising concerns about transparency and user privacy within the online library environment.

User traffic analysis involves the systematic collection and examination of data related to a website's interactions with its users. Extensive research underscores the widespread recognition of user traffic analysis as a pivotal tool for enhancing website functionality and user experience (Jansen 2022). This approach has rapidly evolved into a premier service for capturing and dissecting intricate website data, particularly amid the surge in data sources, signifying its increasingly vital role in the future (O'Brien et al. 2018). However, within the field of Library and Information Science, existing scholarship highlights that user traffic analysis remains relatively underexplored. Arshad and Ahmad's (2020) study emphasises the imperative role of user traffic analysis in expediting performance and boosting conversion rates, fostering heightened website traffic. The authors assert that it provides valuable insights into visitor preferences, enabling tailored content creation. Utilising user traffic analytics, site owners can identify the origin of their traffic, popular blog posts, topics, pages, peak traffic times and the search queries leading users to the website. The literature indicates that websites serve as valuable repositories of information on user behaviour and trends, with the caveat that they must stay current and aligned with contemporary practices (Jiang et al. 2015). The study emphasises the need for website users to possess proficiency in information and communication technology (ICT), familiarity with the virtual realm, and competence in using emerging tools for handling big data. Furthermore, the research highlights that meticulous measurement, assessment and analysis of collected user traffic data provide valuable insights for identifying and rectifying website issues, enhancing performance and optimising effectiveness (Anna & Mannan 2020). It also suggests that judicious resource utilisation can significantly amplify efficacy and usability. However, it is essential to acknowledge that practical insights derived from log files have limitations, as they may omit certain visitor data categories, such as visitor particulars and incomplete system information used for site access, thereby posing challenges for end users.

Control over personal information: User perspectives on privacy

Recent strides in library initiatives have outpaced traditional search methods, necessitating a shift towards more personalised services facilitated by the advent of digital libraries. The foundation of personalised service lies in understanding user needs to enable precise positioning services. As the primary conduit for users to access online information and collections, the library system provides a convenient, expeditious and secure channel for network users to connect to the Internet (Gillespie 2018). To enhance the overall performance of network library information and service application systems, technology researchers have progressively shifted their focus from the application and development of literary resources to investigating user behaviour (Greenhalgh et al. 2016).

The swift expansion of library initiatives across universities has led to increased utilisation of diverse library information resources by user groups. Users' subjective judgement contributes to the search engine's inability to precisely deliver required information, emphasising the urgent need to analyse user needs and provide accurate recommendations (Ekbia et al. 2015). By analysing user information behaviour, innovative modern tools can offer precise service recommendations to increase the accuracy of search results. Personalised information services empower users to configure source methods, expression forms, specific online functions and other modes of online information services within a particular network framework according to their objectives and requirements (Buhalis & Foerste 2015). This user-centred approach prioritises catering to users' needs comprehensively. Personalised service, a fundamental feature of the modern information society, exhibits notable vitality by adapting to the distinct needs of various groups amid a competitive landscape (Huang 2020). The analysis and ensuing service suggestions enable users to partake in more convenient, expedient, intimate and humanised services within university libraries, significantly enhancing the overall quality of comprehensive service provision in academic institutions. According to Palmer et al. (2020), librarians are regularly requested to supply data and information that measures their quality of service, posing the challenge of defining the boundaries. Research by Mann et al. (2023) argues that understanding the context surrounding patron privacy requires uncovering and highlighting the history of privacy protection in libraries. Historically proactive in safeguarding information and data rights, libraries face increased complexity with the digitisation of patron data.

Current concerns regarding patron privacy extend beyond the manual or electronic collection of circulation data to potential improper data collection or misuse. According to Palmer et al. (2020), patrons who now access library resources through single sign-on service providers may be required to provide personal information to third-party vendors for content access and engage in various library services to enhance their learning experience. This shift in content and service provision has given rise to new concerns about the collection, retention and use of patron information. In a study by Gariepy (2019) investigating undergraduate student perspectives on the acquisition, utilisation and privacy of search data within academic libraries, as well as their preferences for data handling by librarians, face-to-face interviews with 27 students revealed a general comfort with libraries collecting search data for their benefit. However, there was moderate apprehension about potential government agency utilisation of their search data and a desire for increased agency in managing their own data. This research provides valuable insights into student perceptions, contributing to a more comprehensive understanding of these issues. Data analysis from Avuglah et al.'s (2020) study shows that 86.5% of students believe individuals should control who sees their personal information, and 50.4% feel third-party firms collect excessive amounts of personal information from online library users. Respondents (80.8% of students) agreed that search engines and social networking sites should prominently display policies on user information handling. This aligns with studies by Tummon and McKinnon (2018) indicating library users and librarians are highly concerned about patron safety online and emphasise the need for patron education. The respondents also stressed the importance of an authoritative body monitoring and tracking unauthorised access, such as hackers and malicious parties.

Contextualising privacy in information services provision in Industry 4.0 and the *Protection of Personal Information Act*

An imperative aspect worthy of note is the implications of the *Protection of Personal Information Act* (*PoPI Act*) on library information services provision in Industry 4.0. Enacted to regulate the processing of personal information and safeguard individuals' privacy, the *PoPI Act* holds particular significance for libraries as custodians of vast amounts of user data (POPIA 2019). The South African parliament assented to the *PoPI Act* on 19 November 2013. The commencement date of section 1, Part A of Chapter 5, section 112 and section 113 of the Act was 11 April 2014. The commencement date of the other sections was 01 July 2020 (with the exception of section 110 and 114[4]). The President of South Africa has proclaimed the *PoPI Act* commencement date to be 01 July 2020.

In the context of Industry 4.0, characterised by digital technologies and data-driven services, academic libraries must navigate complex challenges to ensure compliance with the Act's principles. In the context of Industry 4.0, characterised by the integration of advanced technologies, the *PoPI Act* holds significant implications for library information services provision.

Lawful processing in digital libraries and data minimisation in big data era

With the digitisation of library services, the *PoPI Act* necessitates that personal information is processed lawfully and transparently (POPIA 2019). Libraries must ensure that digital platforms adhere to the Act's principles to protect user privacy. In the realm of technological advancements that facilitate pervasive surveillance, the paramount concern revolves around safeguarding the privacy of end users. Jones and Hinchliffe (2023) emphasise that while the analysis of student data has been an ongoing practice in higher education, the granularity and sensitivity of such data have escalated with students increasingly relying on technology infrastructures, applications and devices in their pursuit of higher education studies. Despite the potential utility of data related to students' academic performance and personal behaviours, ethical challenges loom large in the practices of accessing, managing and utilising this information. Steiner et al. (2016) further underscore the ethical and legal questionability of data collection in such contexts. Additionally, it is noteworthy that AI meticulously records and analyses every user action (Adejo & Misau 2021).

In an era where libraries harness big data for enhanced services, the *PoPI Act*'s principle of data minimisation becomes crucial. Libraries should only collect and process the minimum amount of personal information necessary for their intended purposes. In light of libraries' escalating dependence on electronic systems for personal data management, it becomes imperative for them to establish comprehensive guidelines and policies ensuring strict legal compliance (Mishra et al. 2022). The absence of robust platforms opens the door to unauthorised access to the personal details of library users. With contemporary technologies capable of gathering, sharing and analysing personal data, concerns regarding privacy become pronounced. Hence, the discernible trend points towards the expanding importance of data privacy, wherein safeguarding personal data empowers users to define the extent of data usage, its intended purpose and associated particulars (Laurent & Levallois-Barth 2015). It is clear that whenever a compromise or data breach occurs, both the patron and the library suffer. A data breach could cause harm to the library's reputation, it could result in legal penalties for the library if it failed to adhere to any stipulated regulations (Nield et al. 2020). It is therefore imperative for libraries to address relevant privacy policies and develop guiding principles, surrounding the retention of data and public disclosure of data.

Data subject rights in the digital landscape and security safeguards for digital platforms

The *PoPI Act* grants individuals various rights, including the right to access their information, request corrections and object to processing (POPIA 2019). In Industry 4.0, libraries must facilitate the exercise of these rights in the digital landscape. The primary objective of the *Protection of Personal Information Act* (*PoPI Act*) is articulated in its preamble, which affirms its intention to give effect to the right to privacy enshrined in section 14 of the *Constitution* (Larsen 2019). A breach of an individual's personal data transpires when there is an unauthorised exposure, substitution or modification of any personal information that has been transmitted, stored or otherwise manipulated (Cheng et al. 2017). These breaches encompass three distinct categories, each classified as a variant of a security incident: A breach of confidentiality arises from the inadvertent disclosure or unauthorised access of personal data. A breach of availability pertains to the unintended or unauthorised loss of access to, or destruction of, personal information.

Industry 4.0 involves extensive use of digital platforms. From the *PoPI Act* mandates, academic libraries should implement robust security measures to safeguard personal information from unauthorised access, data breaches and cyber threats. Libraries have integrated a plethora of technological tools and services into their daily operations to optimise service delivery and elevate user experiences. These technologies encompass applications such as research and reference tools, academic databases, social networking sites, video-sharing platforms, blogs and reference chats (Xu et al. 2015). However, the adoption of these sophisticated tools raises concerns about the privacy of users' data and information. This concern is echoed by Dunmade and Tella (2023), who acknowledge the numerous benefits brought by ICTs while underscoring the ethical challenges they pose. Yusuf (2021) further emphasises that the vast proliferation of information across diverse knowledge domains has sparked critical inquiries into privacy, freedom of expression and information accessibility. In response, librarians must prioritise compliance with information ethics in their service offerings. Vaughan (2020) highlights that these technologies aggregate users' data, tracking their online behaviour and certain library tools process and retain various types of data, sharing it with service providers. Ferreira (2021) concurs and states that the relationship between the online platform and the consumer or data subject is an ongoing one. He further argues that this has implications for consumer trust in the online space because the consumer is required, at the outset, to provide initial personal information and further information will be collected whenever the consumer interacts with the online platform. The ongoing nature of this relationship can make it difficult to obtain consent for all future data collection, and there is great potential for the consumer's information to be exploited.

Information privacy is a foundational value in librarianship (Hansson 2017). However, it is challenged in the current information landscape, making it more complex for librarians to uphold their commitment. Despite these challenges, librarians must steadfastly protect users' personal data, upholding their entrusted role as guardians of data privacy rights.

Adaptation to evolving technologies and cross-border data transfers in global networks

Libraries need to adapt their information services to comply with the *PoPI Act*'s principles as technologies evolve. Continuous vigilance and updates are essential to maintain compliance in the dynamic landscape of Industry 4.0. In the 21st century, libraries have evolved into dynamic platforms fostering individual growth and knowledge in an environment that ensures the authoritative and accurate nature of information resources for users' exploration and utilisation of their informational needs (Gangadharan 2016). A study by Agbor et al. (2018), encompassing 16 participants from South African companies, reveals a consensus that implementing the *PoPI Act* goes beyond the mere establishment of control measures and systems. The study underscores that enforcing the *PoPI Act* necessitates a fundamental shift in how employees and organisations conduct their business. One respondent highlighted the need for organisational culture and processes to adapt to the altered landscape of processing and transmitting personal data.

As libraries increasingly operate in global networks, adherence to the *PoPI Act*'s provisions regarding cross-border data transfers becomes essential. Libraries must ensure that data are transferred with adequate protection and in compliance with the Act. Libraries have traditionally championed a culture of accountability in ensuring user privacy for an enriched user experience (Prindle & Loos 2017). It is imperative for libraries when entering agreements with publishers or aggregators to not only secure users' lawful and ethical right to privacy but also align with the institution's legal obligation for robust information security. It is important for libraries to put this right at the forefront as the right to the protection of personal data is 'an enabling human right that renders a discrete contribution to the realisation of a number of other rights and freedoms of the individual'. Furthermore, data protection allows for intervention in data processing, and this protects the individual's right to autonomy and dignity.

Beyond legal considerations, to wield substantial influence in this realm, library policies should mandate staff to possess a comprehensive understanding of the institution's Identity Provider (IdP) software, serving as an intermediary connecting the university, publisher and user. Fallis (2017) underscores that compliance with information ethics primarily involves judiciously allocating access to specific information, addressing concerns related to intellectual freedom, safeguarding personal information, ensuring equitable information access and preserving intellectual property rights.

Research by Yusuf (2021) argues that adherence to information ethics regulations empowers university librarians and other library personnel to align with and uphold ethical standards. These principles, acting as a guiding framework, enhance the quality of service provided to users. Yusuf further emphasises the library's capacity to intervene in network-related issues. Eroglu and Cakmak's study (2020) highlights the imperative for libraries to engage in relevant initiatives and raise awareness about the crucial responsibility of safeguarding library users' data, a duty entrusted to library professionals. The *PoPI Act* aligns with the principles of user empowerment and privacy protection. Libraries must empower users to control their personal information, make informed choices and ensure that data processing aligns with their expectations.

In light of libraries' escalating dependence on electronic systems for personal data management, it becomes imperative for them to establish comprehensive guidelines and policies ensuring strict legal compliance (Mishra et al. 2022). The absence of robust platforms opens the door to unauthorised access to the personal details of library users. With contemporary technologies capable of gathering, sharing and analysing personal data, concerns regarding privacy become pronounced. Hence, the discernible trend points towards the expanding importance of data privacy, wherein safeguarding personal data empowers users to define the extent of data usage, its intended purpose and associated particulars (Laurent & Levallois-Barth 2015). It is clear that both the patron and the library experience harm during a compromise or data breach. A data breach could cause harm to the library's reputation, it could result in legal penalties for the library if it failed to adhere to any stipulated regulations (Nield et al. 2020). It is therefore imperative for libraries to address relevant privacy policies and develop guiding principles, surrounding the retention of data and public disclosure of data.

Privacy and privacy acts in information services provision in Industry 4.0: A conceptual framework proposal

In the era of Industry 4.0, where technology intertwines with every facet of our lives, the provision of information services emerges as a pivotal focal point for libraries and information centres navigating this dynamic landscape. Rooted in the understanding that user needs are in constant flux, the Technology and Ethics in Information Services Framework (F-TechEthix) is proposed. The F-TechEthix is delineated by four foundational constructs: User-Centric Information Services, Privacy and Data Protection, Technological Integration and Ethical Practices, and Global Network Compliance. Each of these pillars plays a distinct yet interconnected role in shaping the delivery of information services in a manner that not only aligns with evolving technological advancements but also underscores the ethical imperative of safeguarding user privacy and complying with relevant laws, such as the *PoPI Act*.

The F-TechEthix integrates key elements of privacy considerations, user behaviour analysis and compliance with the *Protection of Personal Information Act* (*PoPI Act*) in the context of information services provision in Industry 4.0 within libraries. The F-TechEthix encompasses four main pillars.

User-centric information services

- *Objective:* Understand and fulfil the evolving needs of users in Industry 4.0.
- *Components:*
  - Conduct continuous analysis of user behaviour, preferences and information needs using user traffic analytics.
  - Implement personalised information services to enhance user experience and satisfaction.
  - Empower users to configure service preferences and control their personal information.

The User-Centric Information Services construct revolves around the objective of comprehending and meeting the evolving needs of users. By employing continuous analysis of user behaviour and preferences through user traffic analytics, organisations can tailor personalised information services, thereby enhancing user experience. Users are empowered to configure service preferences and maintain control over their personal information.

Privacy and data protection

- *Objective:* Safeguard user privacy and comply with the *PoPI Act*.
- *Components:*
  - Establish and enforce comprehensive privacy policies and guidelines.
  - Implement secure web protocols (HTTPS) and IP anonymisation to mitigate privacy risks associated with web tracking.

  - Ensure secure connections and data minimisation principles in the collection and processing of personal information.
  - Adhere to principles of lawful processing, data subject rights and security safeguards outlined in the *PoPI Act*.
  - Maintain a schedule of all records which will include retention and destruction schedules.

The second construct, Privacy and Data Protection, is committed to safeguarding user privacy and ensuring compliance with the *PoPI Act*. This involves the establishment of comprehensive privacy policies, implementation of secure web protocols, and adherence to principles such as lawful processing and data minimisation. Privacy risks are mitigated through IP anonymisation, and the focus lies on securing connections while respecting data subject rights outlined in the *PoPI Act*.

Technological integration and ethical practices

- *Objective:* Seamlessly integrate technology while adhering to ethical standards.
- *Components:*
  - Regularly update and adapt technological tools and platforms to align with evolving privacy regulations.
  - Foster an organisational culture that prioritises information ethics and user privacy.
  - Equip library staff with comprehensive knowledge of identity providers and relevant software to ensure secure data practices.

The third construct, Technological Integration and Ethical Practices, seeks to seamlessly integrate technology while upholding ethical standards. Regular updates to technological tools align with evolving privacy regulations, and an organisational culture prioritising information ethics is fostered. Library staff are equipped with comprehensive knowledge to ensure secure data practices.

Global network compliance

- *Objective:* Ensure compliance with the *PoPI Act* in cross-border data transfers.
- *Components:*
  - Prioritise legal and ethical considerations in agreements with publishers and aggregators.
  - Educate library staff on the importance of safeguarding user data in a global network.
  - Empower users with information about their rights, choices and expectations regarding data processing.

The fourth construct, Global Network Compliance, centres on ensuring compliance with the *PoPI Act* in cross-border data transfers. Legal and ethical considerations are prioritised in agreements with publishers, and library staff are educated on safeguarding user data globally. Users are empowered with information about their rights and expectations regarding data processing. These interconnected dynamics result in outcomes such as enhanced user satisfaction, the mitigation of privacy risks, adaptable technological infrastructure and a global network approach that upholds legal and ethical data practices.

The four constructs of the F-TechEthix form a holistic approach to information services provision. User-centric services are built on understanding user behaviour, respecting privacy and complying with relevant laws. Privacy and data protection principles are integral to user-centric services and are guided by ethical practices. Technological integration supports both user-centric services and privacy compliance. Global network compliance ensures that privacy and data protection principles are upheld in cross-border activities. The F-TechEthix provides a comprehensive and adaptable approach for libraries in Industry 4.0 to navigate the complexities of user-centric information services, privacy considerations and compliance with the *PoPI Act*. It emphasises the interconnected nature of these elements, encouraging a holistic and user-focussed approach to information services provision in the digital age. The key outcomes would include enhanced user satisfaction and experience through personalised, secure and ethically managed information services; mitigation of privacy risks and compliance with the *PoPI Act*, fostering of users' trust; adaptable technological infrastructure aligned with evolving privacy regulations; and a global network approach that ensures legal and ethical data practices in cross-border interactions.

Sturges (2002) proposed the implementation of comprehensive checklists to evaluate privacy policies, emphasising the necessity to assess whether these policies are ethical, lawful and realistic; whether they represent public interests and whether they serve the interests of the parties most affected. Furthermore, he highlighted the importance of technical security measures, installing security patches and deleting unnecessary accounts are some of the measures libraries can take to ensure information security. From a managerial perspective, Sturges recommended that libraries establish privacy protection guidelines, restrict information access to prevent physical leakage, include confidentiality and privacy protection provisions in library regulations, develop ethical guidelines to avoid indiscriminate information collection, publish these guidelines on the library's website, and appoint staff responsible for overseeing privacy and information protection. Similarly, Park (2009) advocated for privacy protection guidelines concerning the collection, use, service provision, maintenance and disposal of personal information to enhance the privacy protection of library users.

Conclusion

As libraries transcend their traditional roles, becoming vibrant centres of learning and research, the imperative to embrace cutting-edge technologies and address privacy concerns takes centre stage. Librarians, in their commitment to delivering high-quality services, are not merely adapting to change but actively shaping the future. The exploration of user-centric services, privacy considerations and compliance with the *PoPI Act* lays the groundwork for a future where libraries seamlessly integrate into the digital fabric of society. Moreover, the exploration of user perspectives on privacy reveals a nuanced landscape, with varying comfort levels regarding data collection and usage among library patrons (Avuglah et al. 2020; Gariepy 2019). These findings highlight the importance of user education, privacy policies and ethical considerations in information services provision. The proposed conceptual framework, F-TechEthix, aims to act as a compass, guiding libraries towards a future where user satisfaction is not just met but exceeded through personalised, secure and ethically managed information services.

It is clear based on the findings of the studies consulted that 4IR's technological confluence has increased connectivity, predominantly with IoT and smart devices. Systems that were once isolated are suddenly talking to each other, relaying information and setting up notifications. In spite of the conveniences offered by connected systems, cyberattacks are possible. A device linked online can be publicly discovered and accessed. A sensor or device that is part of the IoT, such as a smartphone, Wi-Fi television or smart fridge, communicates openly over Wi-Fi networks and may be connected to the public Internet. However, even the most sophisticated 4IR technologies can succumb to human errors. Human errors, poorly secured business processes and technological vulnerabilities may be exploited by hackers to disrupt critical systems, steal sensitive information and encrypt data. The interconnected dynamics presented in F-TechEthix herald a future where libraries are not only repositories of knowledge but also guardians of privacy rights, information ethics and technological advancements. As they navigate the complexities of cross-border data transfers, user preferences and technological integration, libraries stand as beacons of trust in an era where the ethical use of information is paramount. The synthesis of the conceptual framework, rooted in the challenges and opportunities of today, paves the way for a future where libraries play a central role in shaping the narrative of information services provision, embracing the possibilities that Industry 4.0 offers.

Recommendations

Looking ahead, there is a need for libraries to become proactive architects of their own destiny. As technology continues its relentless march forward, libraries must not only keep pace but also pioneer innovations that prioritise user experiences, data privacy and legal compliance. It is necessary for librarians to understand if patrons are aware of the information collected and used by the library and library vendors through provided resources and services. Beyond awareness, libraries should analyse and understand patrons' perceptions towards the potential use of their personal data within the library sphere, and whether they are concerned with personal consent. Using policies and practices that strike a balance between harnessing the potential of collected data and safeguarding individual rights, Payton and Claypoole (2023) argue that libraries can advocate for policies and practices that are consistent with the organisation's mission and philosophy. Furthermore, professional associations in the field should look at updating their documentation and providing practical tools which can help the commitment towards professional integrity when and practices in relation to data privacy. In addition to this, participating in outreach projects relating to the importance of data privacy and the privacy rights of patrons is recommended for promoting the importance of protecting personal information and raising awareness of rights, responsibilities and best practices, among both patrons and professionals.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

Y.O. contributed to the conception and design, validation, writing of the original draft, and data curation and resources of the study. O.G.S. contributed to the data collection, formal analysis, writing and supervision of the results of the study. All authors reviewed the results and approved the final version of the article.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. It does not necessarily reflect the official policy or position of any affiliated institution, funder, agency or that of the publisher. The authors are responsible for this article's results, findings and content.

References

Adejo, A.A. & Misau, Y., 2021, 'Application of artificial intelligence in academic libraries in Nigeria', *Library Philosophy and Practice* 11(18), 6639.

Avuglah, B.K., Owusu-Ansah, C.M., Tachie-Donkor, G. & Yeboah, E.B., 2020, 'Privacy issues in libraries with online services: Attitudes and concerns of academic librarians and university students in Ghana', *College & Research Libraries* 81(6), 997. https://doi.org/10.5860/crl.81.6.997

Bareh, C.K., 2022, 'Privacy policy analysis for compliance and readability of library vendors in India', *The Serials Librarian* 83(2), 148–165. https://doi.org/10.1080/0361526X.2022.2143467

Corrado, E., 2022, 'Libraries and protecting patron privacy', *Technical Services Quarterly* 37(1), 44–54. https://doi.org/10.1080/07317131.2019.1691761

Dunmade, A.O. & Tella, A., 2023, 'Libraries and librarians' roles in ensuring cyberethical behaviour', *Library Hi Tech News* 40(7), 7–11. https://doi.org/10.1108/LHTN-04-2023-0068

Edanz, 2023, *The 4 stages of a PRISMA flow diagram*, viewed n.d., from https://www.edanz.com/blog/prisma-flow-diagram.

Ekbia, H., Mattioli, M., Kouper, I., Arave, G., Ghazinejad, A., Bowman, T., 2015, 'Big data, bigger dilemmas: A critical review', *Journal of the Association for Information Science and Technology* 66(8), 1523–1545. https://doi.org/10.1002/asi.23294

Eroğlu, Ş. & Çakmak, T., 2020, 'Personal data perceptions and privacy in Turkish academic libraries: An evaluation for administrations', *The Journal of Academic Librarianship* 46(6), 102251. https://doi.org/10.1016/j.acalib.2020.102251

Gangadharan, S.P., 2016, 'Library privacy in practice: System change and challenges', *ISJLP* 13, 175.

Gayshun, I.V., 2015, 'IFLA statement on privacy in the library environment', *Russian Journal of Library Science* 5, 93–95. https://doi.org/10.25281/0869-608X-2015-0-5-93-95

Gillespie, T., 2018, *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press, New Haven.

Greenleaf, G. & Cottier, B., 2020, *2020 ends a decade of 62 new data privacy laws*, Privacy Laws & Business International Report 24–26, University of New South Wales, Sydney.

Hansson, J., 2017, 'Professional value and ethical self-regulation in the development of modern librarianship: The documentality of library ethics', *Journal of Documentation* 73(6), 1261–1280. https://doi.org/10.1108/JD-02-2017-0022

Hartman-Caverly, S. & Chisholm, A., 2020, 'Privacy literacy instruction practices in academic libraries: Past, present, and possibilities', *IFLA Journal* 46(4), 305–327. https://doi.org/10.1177/0340035220956804

Hess, A.N., LaPorte-Fiori, R. & Engwall, K., 2015, 'Preserving patron privacy in the 21st century academic library', *The Journal of Academic Librarianship* 41(1), 105–114. https://doi.org/10.1016/j.acalib.2014.10.010

Jansen, B.J., 2022, '*Understanding user-web interactions via web analytics*, Springer Nature.

Jones, K.M. & Hinchliffe, L.J., 2023, 'Ethical issues and learning analytics: Are academic library practitioners prepared? *The Journal of Academic Librarianship* 49(1), 102621. https://doi.org/10.1016/j.acalib.2022.102621

Kim, D.S. & Noh, Y., 2014, 'A study of public library patrons' understanding of library records and data privacy', *International Journal of Knowledge Content Development & Technology* 4(1), 53–78. https://doi.org/10.5865/IJKCT.2014.4.1.053

Kritikos, K.C. & Zimmer, M., 2017, 'Privacy policies and practices with cloud-based services in public libraries: An exploratory case of bibliocommons', *Journal of Intellectual Freedom & Privacy* 2(1), 23–37. https://doi.org/10.5860/jifp.v2i1.6252

Larsen, C.L., 2019, 'Data privacy protection in South Africa: An analysis of vicarious liability in light of the Protection Of Personal Information Act 4 of 2013 (" POPIA")', Doctoral dissertation, University of KwaZulu-Natal.

Laurent, M. & Levallois-Barth, C., 2015, 'Privacy management and protection of personal data', in *Digital Identity Management* 4, 137–205. https://doi.org/10.1016/B978-1-78548-004-1.50004-3

Maceli, M., 2019, 'Librarians' mental models and use of privacy-protection technologies', *Journal of Intellectual Freedom & Privacy* 4(1), 18–32. https://doi.org/10.5860/jifp.v4i1.6907

Maceli, M.G., 2018, 'Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries', *IFLA Journal* 44(3), 195–202. https://doi.org/10.1177/0340035218773786

Makori, E.O. & Bitso, C., 2021, 'Information profession in digital transformation and development: Future directions', in B.J. Hollard (ed.), *Handbook of research on knowledge and organization systems in library and information science*, pp. 1–24, IGI Global, New York.

Masilela, L. & Nel, D., 2021, 'The role of data and information security governance in protecting public sector data and information assets in national government in South Africa', *Africa's Public Service Delivery and Performance Review* 9(1), 385. https://doi.org/10.4102/apsdpr.v9i1.385

McKinnon, D. & Turp, C., 2022, 'Are library vendors doing enough to protect users? A content analysis of major ILS privacy policies', *The Journal of Academic Librarianship* 48(2), 102505. https://doi.org/10.1016/j.acalib.2022.102505

Michalak, R. & Rysavy, M.D., 2019, 'Data privacy and academic libraries: Non-PII, PII, and librarians' reflections (part 2)', *Journal of Library Administration* 59(7), 768–785. https://doi.org/10.1080/01930826.2019.1649969

Mishra, A., Alzoubi, Y.I., Anwar, M.J. & Gill, A.Q., 2022, 'Attributes impacting cybersecurity policy development: An evidence from seven nations', *Computers & Security* 120, 102820. https://doi.org/10.1016/j.cose.2022.102820

Mohammed, I.A., 2020, 'Usability and privacy in academic libraries: Regaining a foothold through identity and access management', *International Journal of Innovations in Engineering Research and Technology* 7(3), 43–48.

Nicholson, S. & Smith, C.A., 2007, 'Using lessons from health care to protect the privacy of library users: Guidelines for the de-identification of library data based on HIPAA', *Journal of the American Society for Information Science and Technology* 58(8), 1198–1206. https://doi.org/10.1002/asi.20600

Palmer, M., Freeman, A.D. & Geary, J., 2020, 'I always feel like somebody's watching me: Student perceptions of library data privacy', *South Carolina Libraries* 4(1), 20. https://doi.org/10.51221/sc.scl.2020.4.1.9

Payton, T. & Claypoole, T., 2023, *Privacy in the age of Big data: Recognizing threats, defending your rights, and protecting your family*, Rowman & Littlefield, London.

Phillips, B., 2020, 'Critically analyse the approaches to GDPR and DPA 2019 compliance within the UK Further Education Sector', MSC dissertation, pp. 1–72, Solent University.

Prindle, S. & Loos, A., 2017, 'Information ethics and academic libraries: Data privacy in the era of big data', *Journal of Information Ethics* 26(2), 22–33.

Quach, S., Thaichon, P. & Martin, K.D., 2022, 'Digital technologies: Tensions in privacy and data', *Journal of the Academic Marketing Science* 50, 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Salubi, O., 2023, 'Transforming libraries and information professionals for the industry 4.0 in developing countries: Towards the development of a framework for accelerating change post-Covid-19', *Alexandria: The Journal of National and International Library and Information Issue*, viewed 30 April 2024, from https://journals.sagepub.com/doi/pdf/10.1177/09557490231197971.

Tummon, N. & McKinnon, D., 2018, 'Attitudes and practices of Canadian academic librarians regarding library and online privacy: A national study', *Library & Information Science Research* 40(2), 86–97. https://doi.org/10.1016/j.lisr.2018.05.002

Wissinger, C.L., 2017, 'Privacy literacy: From theory to practice', *Communications in Information Literacy* 11(2), 378–389. https://doi.org/10.15760/comminfolit.2017.11.2.9

Witt, S., 2017, 'The evolution of privacy within the American library association, 1906–2002', *Library Trends* 65(4), 639–657. https://doi.org/10.1353/lib.2017.0022

World Economic Forum, 2023, *Fourth industrial revolution*, viewed 13 June 2024, from https://www.weforum.org/focus/fourth-industrial-revolution.

Xu, J., Kang, Q., Song, Z.F. & Clarke, C.P., 2015, 'Applications of mobile social media: WeChat among academic libraries in China', *The Journal of Academic Librarianship* 41(1), 21–30. https://doi.org/10.1016/j.acalib.2014.10.012

Yassin, E., 2022, 'Privacy and personal data protection in libraries: A scientific review', *International Journal of Library and Information Sciences* 9(2), 477–490.