Security and Privacy in Digital Libraries: Challenges, Opportunities and Prospects

Mohammed Nasser Al-Suqri, Department of Information Studies, College of Arts and Social Sciences, Sultan Qaboos University, Al-Khoud, Sultanate of Oman

Esther Akomolafe-Fatuyi, Morgan State University, Department of World Languages and International Studies, Baltimore, MD, USA

ABSTRACT

Technological advances have led to a proliferation of digital libraries over the past decade or so. These offer valuable opportunities for convenient access to information and data, regardless of an individual’s location. For librarians though, the transition from physical to digital library collections brings many new challenges, not least in the areas of security and privacy. The purpose of this article is to examine the nature of these challenges and the opportunities available for overcoming them, so that libraries can continue to fulfill their important role of providing accurate, secure and timely information to users, while protecting their privacy and the confidentiality of their personal information. The article addresses in particular the following issues: protecting the information infrastructure; identification and authentication in security and privacy; standards and policies; access and control of digital information; ethical decision-making in design, implementation and evaluation of digital libraries; and privacy, anonymity and identity. The article concludes with consideration of the future prospects for security and privacy in digital libraries.

Keywords: Challenges, Confidentiality, Digital Libraries, Opportunities, Personal Information, Privacy, Security

INTRODUCTION

There has been a vast increase globally over the past decade or so in digital libraries, facilitated by technological advances and driven by consumer demand for easy and convenient access to knowledge and information from any location. The Digital Library Federation defines digital libraries as “organizations that provide the resources, including the specialized staff, to select, structure, offer intellectual access to, interpret, distribute, preserve the integrity of, and ensure the persistence over time of collections of digital works, so that they are readily and commercially available for use by a defined community or set of communities.” An
alternative definition put forward by Ershova and Hohlov (2001) describes the digital library as “a distributed information systems ensuring reliable storage and effective use of heterogeneous collections of electronic documents - text, graphics, audio, video, etc. - via global data transfer networks in a way convenient for the end user.” In brief, digital libraries are organizations that hold information resources in digital format. It has been predicted that they will play an increasingly more important and essential role in society, not only as data and knowledge repositories and the means of retrieving information from them, but as a focal point for all forms of knowledge, research and education (Birnbaum, 2004).

However, while bringing benefits to patrons and new opportunities for library professionals to expand their roles, the developments have also brought about new problems and challenges, especially relating to information security and user privacy. News reports of security breaches and identify theft in the online environment threaten to undermine consumer trust in Internet-based services generally, including digital libraries (Kuzma, 2010).

The purpose of this article is to examine the nature of these challenges and the opportunities available for overcoming them, so that libraries can continue to provide knowledge and information to users, while protecting their privacy and the confidentiality of their personal information and preserving the integrity of information for ongoing use.

BACKGROUND

Emerging digital technology has paved the way for the creation of digital libraries, which have made it easier for users to access information through digital systems and networks. The digital library is generally designed to perform and serve the same primary functions and tasks as a traditional library. What makes it different, though, is that it consists of data stored in digital form on computerized devices instead of in physical books and journals. In today’s globalized world, data are transmitted across the planet through the Internet, providing easier access to information and education for many people. While this technology provides current opportunities for expanded learning across the globe, there is also a need to ensure that the digital information can be preserved and made available for future generations.

The primary functions performed by libraries include developing and producing information records in print and non-print formats, managing these information records, and distributing information for the use of current and future generations. The role of libraries in facilitating information access has been widely discussed by many researchers (Borgman, 2000; Sturges, 2001; Hamilton & Pors, 2003). The continual evolution of technology and the resulting changes in the interface between users and information changes the librarian’s professional environment and their role. Fifty years ago, a librarian would help patrons find a book through a card catalogue; today, digital librarians use a computer to assist more patrons to simultaneously locate books, audiovisual media and on-line resources.

Digital librarians have an interest in the preservation of data in durable format and in the provision of access to vast information while keeping pace with the changing technologies. They need to be able to resolve issues of compatibility between old and new technologies while transferring information between them and providing access to end-users. At the same time, attention must be paid to ensuring the protection of the information infrastructure and the privacy of end users. The global increase in the overall quantity of information and in the digital devices on which it is stored has given rise to many issues of security and privacy pertaining to both library users and digital materials. The storage, management, retrieval and use of information from sources which are no longer
under the physical control of librarians, involve a range of risks which must be addressed using both technical and non-technical solutions.

**PROTECTING THE INFORMATION INFRASTRUCTURE**

The physical infrastructure on which digital resources are held is vulnerable to a range of risks including theft, damage and online attacks from viruses and various forms of malware (Zimmerman, 2009). Hardware and other infrastructure, as well as networks including wireless networks must be adequately secured to prevent unauthorized access or attacks on the integrity of the data held (Al-Suqri & Afzal, 2007). Regular data backups are also crucial to insure against data loss, along with other data preservation processes (Anday et al., 2012).

Standards and mechanisms for the protection of the information during data transfer are also very important as technology changes and improvements in information storage are made, earlier information resources in print format need to be transferred to progressively newer technologies over time, as older forms gradually become obsolete.

The privacy of end users will also be more easily achieved if standards for the protection of the digital infrastructure are met. Digital information users have access to a wide range of information and sources through various agencies and there is a need to establish appropriate standards for the storage and dissemination of this information. These should allow end users to access digital information subject to the standards of the particular source being used, and ensure strict adherence to rules and regulations intended to protect the users’ security and privacy. These types of standards are increasing and being adjusted to the proliferation of information on the Web and the demands of usage. As a result, digital information professionals are now required, for example, to identify and authenticate the security and privacy of their patrons.

**IDENTIFICATION AND AUTHENTICATION IN SECURITY AND PRIVACY**

The fundamental roles of information professionals are changing due to the information explosion, evolving forms of recording information, different processes of information, different procedures for dissemination of information, and vast increase in the number of library users. Governments know how important it is to protect their citizens’ privacy in the online world, and most disseminate official guidance on their privacy and rights in relation to the protection of personal information submitted to Web sites, which must be observed by digital librarians.

The Internet and its enabling technology are constantly changing; in similar vein, the standards for user privacy are evolving. Privacy laws are effectively in place to aid digital libraries in ensuring that the personal information of users is protected with security safeguards appropriate to the sensitivity of the information. Identification and authentication of digital library users, including verification of their claims or statements of identity, can assist in the protection of privacy and reduce unauthorized disclosures of private and sensitive information.

Technological advances are continually changing the methods by which individuals can be identified and authenticated online. The use of passwords and other identification codes is becoming critical in the prevention of identity theft and other types of fraud. Garfinkel (2003), discussing the advantages and weaknesses of email-based identification and authentication (EBIA), notes that “this technique uses an email address as a universal identifier and the ability to receive email at that address as a kind of authenticator” (p.22).

The digital information professional is a key player in the digital library environment for the identification and authentication of quality and relevant information. The public must have access to the professional for inquiries and assistance in retrieving the needed information in
a digital format. As technology changes and the need for information grows, it can be expected that the ease of identifying the information needs of users and retrieving and disseminating the requested information will increase.

**STANDARDS AND POLICIES IN DIGITAL LIBRARIES**

An information professional’s role is to provide accurate information in a timely manner and ensure that the integrity of that information is not compromised. According to Sturges, Davies, Dearmley, Iliffe, Oppenheim, and Hardy (2003), library users believe “that libraries will have policies on privacy and data protection in force” (p. 49). As digital information becomes more widely used, and as competition over the velocity of information dissemination sometimes overshadows integrity, the regulations and policies that govern the circulation of information have become increasingly important.

The Open Archival Information System (OAIS) has been widely adopted as an ISO standard for digital libraries, which incorporates recommended methods for both data preservation and retrieval processes. Individual countries have established their own initiatives for the development of digital data preservation standards (Voutssas, 2012) and also have data protection laws in place which specify technical and procedural requirements for securing personal data on computer systems (Kuzma, 2010). Qualitative research in Uganda and Kenya by Ngimwa and Adams (2011) found that the existence of institutional and national policies, for example covering legal and privacy-related issues, has a major impact on the design process of digital libraries, and the absence of such policies stifles innovation in this area.

The Digital Revolution has made information more accessible; it has also affected society’s morals by altering the perception of standards and policies of retrieving information or downloading media from the Internet. It is sometimes perceived to be the same as borrowing electronic devices from a friend. Information seekers often disregard laws and moral implications when they choose to pirate or otherwise use information for illicit purposes based on their own ethical standards. According to Seadle (2004), even “a reasonable fair use in ethical terms could still be an infringement in strict legal judgment,” (p. 109). Hence, there is a need to have a formal enforcement mechanism in place of the current situation in which peer pressure and ethical judgment determines whether intellectual property infringements occur.

Many governments have created protection stipulations in the form of copyrights; however, one of the major problems that digital librarians grapple with is how to ensure compliance with the various copyright and licensing laws of different countries (Posner, 2012). Premchand-Mohammed (2011) documented the difficulties faced by a medium-sized academic library in a multi-campus Caribbean university when transitioning from print to digital resources. Most of the subscriptions for electronic resources were governed by licenses developed overseas, which did not meet the needs of the university’s patrons, and the library staff reportedly lacked adequate legal expertise to properly review and negotiate licensing agreements. Difficulties also arise when applying conventional copyright laws to digital content: in the U.S., for example, e-books are licensed on a contractual basis rather than sold, and vendors sometimes require consumers to destroy the material on their computers at the end of the lending period, a requirement that is difficult for digital librarians to enforce (McDermott, 2012).

**ACCESS AND CONTROL OF DIGITAL INFORMATION**

The more information pumped into a society the more complex are the regulations needed to protect this information. Today, the information superhighway is where information is collected and kept in databases, retrieval systems, and digital libraries for the use of patrons. Access to their content is granted based on the users’ skills and knowledge (Borgman, 2000). Control
is given to creators, and government is given ownership as a means to initiate statutes, laws, and guidelines on the use and distribution of the information. However, technology has made it easier for users to copy and redistribute materials (Abie, Spilling, & Foyn, 2004), and there is a growing need for digital librarians to preserve and protect digital content from unauthorized or illegal use (Kuzma, 2010).

Many nations use agencies to regulate information for the purpose of national defense and broadcasting purpose. As a result, the extent to which access to information is available is often determined by the organizations that control it. Governments help protect all matters of national or global interest from finances to homeland defense. Global and national agencies and commissions assist in keeping information flowing through a society. These same agencies help to protect digital information, its content, its access, its design, and its implementation, while simultaneously regulating its ethical usage.

The digital library as an agency has a key role to play in ensuring access to digital information as well as controlling it. Today, the digital library is a central hub in the world of digital information, with the responsibility of converting information from traditional to digital format for preservation purposes, and regulating access to and control over its use. Since the act of preservation has always been a primary function of libraries, concerns are now being raised over responsibilities for the future preservation of materials in digital format, now that this function is “slowly shifting to the publishers” (Urs, 2004, p. 206).

There is a growing conflict between providers’ concerns about protecting their information from piracy and the library profession’s concern to make resources available for “fair use” by the public. According to the IFLA’s “Position on copyright in the digital environment”, digital information resources should not be subject to different copyright laws than traditional print resources, and the legal concept of fair use of information for public use should apply. It has been argued that digital librarians are well placed to help protect the rights of the public in securing fair access to information, while enabling providers to collect appropriate copyright fees (Posner, 2012; Vouttas, 2012). Posner (2010) contends that librarians must take an ethical standpoint in this area and if necessary challenge laws that violate the principles of good librarianship.

Since most people do not have such highly developed information retrieval skills as digital librarians, there is also a need for these information professionals to be extra vigilant when advising individuals on the use of digital information. Sometimes digital librarians may be unable to stop an executive from using information incorrectly, but they should not stand on the excuse that “they were following orders” and should certainly voice their objection if information is to be used unethically.

**ETHICAL DECISION-MAKING IN DESIGN, IMPLEMENTATION AND EVALUATION OF DIGITAL LIBRARIES**

Information ethics is another vital area of responsibility for digital librarians, who have the responsibility to keep information confidential if necessary and to ensure that it is used only in appropriate and professional ways. Digital information professionals have the responsibility to abide by the four principles of information ethics as described by Severson (1997): principles of respect for user’s Intellectual Property, privacy, fair representation, and principles of non-maleficence to daily information dissemination to users. While designing, implementing and evaluating the usage of digital information, digital library professionals need to consider customer protection as a top priority ethical obligation.

In the Information Age, information security and privacy are very important issues. Digital librarians have an ethical responsibility to protect the information that individuals and organizations took the time to collect, record or create. Having appropriate regulations for the
use and evaluation of information resources is necessary to safeguard the interests of all those affected by copyright issues or the distribution of information in digital format. The digital librarian should regard personal intellect in non-print materials, artworks, music, and other creative ideas as personal property. As such, digital information professionals should make efforts to preserve the privacy of these valuable resources and safeguard them from misuse.

PRIVACY, ANONYMITY AND IDENTITY

The American Library Association’s Code of Ethics states that librarians should “protect each library user’s right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted” (ALA, 1995). This and similar codes and standards developed in other countries have protected library users’ privacy for many decades in the conventional library context, where their searching and borrowing activities have not generally been monitored over time by library staff.

In contrast, digital libraries and especially the new Library 2.0 developments often require the recording of personal information including bank account details (for subscription-based services) and track search activities in detail (Kuzma, 2010; Zimmer, 2013). In this context, digital librarians have the new responsibility of ensuring this data is held in confidence, used only for the stated purpose and protected from hackers, criminals and other parties wishing to secure information about the library users for their own gain (Bowers, 2006). The privacy-related concerns of digital libraries are to prevent patrons’ information from being disseminated among other users and organizations in unethical manner. Digital librarians cannot give out information to parties not associated with the patron, and must not violate the patron’s privacy. They should be especially cautious when disseminating information in sensitive areas such as healthcare, to protect the privacy and identity of patients. Furthermore, in a university setting, digital information professionals should prevent the sharing of student information and should uphold their rights to privacy.

FUTURE TRENDS OF SECURITY AND PRIVACY IN DIGITAL LIBRARIES

As Zimmer notes, now that many services formerly provided by libraries are being made available online in other forms such as web search engines, the traditional roles and expertise of librarians in “collecting, filtering and delivering information” are being threatened (Zimmer). Digital libraries offer the possibility for librarians to retain and expand on their important roles, if they can develop new skills and become experts in all aspects of digital data collection, storage, preservation and retrieval. Especially pertinent are security and privacy-related expertise.

Recent research indicates that, despite the ongoing expansion in digital libraries around the world, there are serious shortcomings in addressing privacy and security related issues, and low levels of awareness of the issues among librarians. Though many laws and standards are in place that relate to information security and data protection, there is evidence that these are not always being observed in relation to digital libraries. For example, Kuzma (2010) conducted research with 80 European libraries and found evidence that 65% had serious security flaws in their web applications. In the non-western world, survey research with library managers has revealed very low levels of awareness of how to develop digital libraries and the security issues involved, and little or no training for librarians in these areas (Mohsenzadeh & Isfandyari-Moghaddam, 2011; Sarchami, & Mohsenzadeh, 2012).

Digital libraries form an important component of the emerging Library 2.0 developments, in which users actively participate in the ongoing design of both physical and virtual library services (Casey & Savastinuk, 2010).
Library 2.0 initiatives are expected to expand, including the use of social media to engage with patrons and seek their input into the development of library services. However, Zimmer (2013) found that though there is considerable professional interest in Web 2.0, which is seen as a significant new way of delivering library services and information content, very little attention is being paid to the privacy implications and how to address these. As a result little training or education is being developed for library and information specialists in this area (Zimmer, 2013), and there is a need to redress this situation. Moreover, Library 2.0 developments offer valuable opportunities to educate users about the need to protect themselves and their personal information in this environment and on the appropriate use of digital resources, and the library profession should therefore also develop guidance and materials for this purpose.

CONCLUSION

As Kuzma (2010) highlights, digital library security is not just a technical endeavor but “a multi-dimensional approach with a combination of both technical and managerial solutions”. This article has discussed the main security and privacy related issues facing digital libraries and has highlighted the ways that these must be addressed to protect the integrity of the digital library environment and the security of its users. Inevitably there are considerable costs involved: it will be important for digital library managers to allocate adequate resources not only for technical solutions, but also for the training of library professionals and the education of users. Collaboration of library professionals both within countries and internationally can help improve the efficiency and cost-effectiveness of relevant initiatives and help standardize approaches to digital library development and the security and privacy issues involved.

REFERENCES


