Volume 44 Number 3 October 2018

IFLA

Contents

Special Issue: Privacy

Guest Editor: Louise Cooke

Guest Editorial

Articles

Aims and Scope

IFLA Journal is an international journal publishing peer reviewed articles on library and information services and the social, political and economic issues that impact access to information through libraries. The Journal publishes research, case studies and essays that reflect the broad spectrum of the profession internationally. To submit an article to IFLA Journal please visit: journals.sagepub.com/home/ifl

IFLA Journal
Official Journal of the International Federation of Library Associations and Institutions
ISSN 0340-0352 [print] 1745-2651 [online]

Published 4 times a year in March, June, October and December

Publisher

SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC and Melbourne.

Annual subscription (4 issues, 2018) Free to IFLA members. Non-members: full rate (includes electronic version) £321/$592. Prices include postage. Full rate subscriptions include the right for members of the subscribing institution to access the electronic content of the journal at no extra charge from SAGE. The content can be accessed online through a number of electronic journal intermediaries, who may charge for access. Free e-mail alerts of contents listings are also available. For full details visit the SAGE website: sagepublishing.com

Student discounts, single issue rates and advertising details are available from SAGE, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP, UK. Tel: +44 (0) 20 7324 8500; e-mail: subscriptions@sagepub.co.uk; website: sagepublishing.com. In North America from SAGE Publications, PO Box 5096, Thousand Oaks, CA 91359, USA.

Please visit journals.sagepub.com/home/ifl and click on More about this journal, then Abstracting/indexing, to view a full list of databases in which this journal is indexed.

Printed on acid-free paper by Page Bros, Norwich, UK.

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 167–169

DOI: 10.1177/0340035218789601
journals.sagepub.com/home/ifl
SAGE

Privacy, libraries and the era of big data

Louise Cooke
Loughborough University, UK

This special issue of *IFLA Journal* concerns itself with one of the key ethical and legal concerns of our time, namely that of privacy. In addition to playing an important role in political and social thought more broadly (Tavani, 2008), privacy has particular significance to the role and operation of the library and information sector. However, it is a value that is currently facing significant threats. Scott McNealy, co-founder and former CEO of Sun Microsystems, is often quoted as having commented in 1999 that 'You have zero privacy anyway. Get over it!' (Sprenger, 1999). Although much challenged at the time (and since), this statement bears resonance in an era of big data, social media and the rapid growth of many technologies that afford high levels of surveillance and data storage and manipulation. To most of us, both within and beyond the library and information science (LIS) community, privacy is still seen as a vital human right, enshrined as it is within the *Universal Declaration of Human Rights* (United Nations, 1948) and subsequent human rights conventions. However, social values, norms and perspectives change over time, cultures and geographical locales and now seems the right time to take stock of what is happening with regard to privacy in the LIS domain and beyond. This is the purpose of this special issue.

Privacy has been described by Moor (2006) as an evolving concept that is shaped by the political and technological characteristics of the society in which we live. Multiple definitions of the concept exist, but it is typically understood as concerning itself with notions such as secrecy, solitude, security and confidentiality (Tavani, 2008). In a classic, influential articulation of the right to privacy back in the 19th century, Warren and Brandeis (1890) described privacy as the condition of 'being free from intrusion' and having 'the right to be let alone'. This aligns with more recent definitions from Alfino (2001) who considers it as being concerned with the right to personal space and to being able to lead a rational, autonomous life. Increasingly, however, it is seen primarily to be concerned with the ability to control the extent to which others have access to personal information about ourselves – our 'informational privacy' (Floridi, 2005). This is, in part at least, an outcome of the increasing ease with which personal information can be stored, transmitted and manipulated using modern information and communication technologies.

For libraries and librarians the concept of privacy holds special importance. As Witt (2017) shows us, the idea of privacy developed within LIS along with the growing concerns about technology-driven intrusion, described by Warren and Brandeis. Defining privacy (somewhat narrowly) in the context of librarianship as 'The freedom to access whatever materials an individual wishes, without the knowledge or interference of others', Gorman (2000) included it as one of his eight 'core values' and recognised the importance of the (private) bond of trust between librarians and their clients. Clarke (2006) recognises the need to balance the right to privacy against the competing interests of other individuals and groups in society: this is particularly pertinent in a library context, as privacy can either work in the interests of freedom of access to information (i.e. confidence in the ability to read or access information in private promotes a willingness to explore more controversial sources) or against such interests (e.g. the ability of government to keep certain sources private acts against open access to information).

Professional bodies in the LIS sector usually act to defend the importance of privacy within their professional codes of practice and codes of ethics. The IFLA *Code of Ethics for Librarians and Other Information Workers* (IFLA FAIFE, 2012) highlights the confidential nature of the relationship between library and

Corresponding author:
Louise Cooke, Professor of Information & Knowledge Management, School of Business & Economics, Room BE 1.31a, Loughborough University, Loughborough LE11 3TU, UK.
Email: L.Cooke@lboro.ac.uk

information personnel and their users, and the importance of not sharing data beyond the needs of the immediate transaction. At the same time, it advocates for transparency in government and declares that 'it is in the public interest that misconduct, corruption and crime be exposed by what constitute breaches of confidentiality by so-called "whistleblowers"' (IFLA FAIFE, 2012: Clause 3), thus recognising that in some contexts privacy can work against the public interest.

The complex – and sometimes, contentious – issues that privacy concerns raise for library and information personnel form the backbone of the content of the papers in this Special Issue. To begin with, Affonso and Sant'Ana highlight the importance of privacy policies in the digital era, drawing on the context of collection of data from the National Digital Libraries of South America. Their research used a data-mining tool, Wireshark, to demonstrate that data from interactions between users and digital libraries can be collected without the users' awareness, and that there is a need to make this possibility more explicit through well-crafted and transparent privacy policies available to all users. This is a good example of how new technologies enable collection, aggregation, and dissemination of information in ways that were not previously possible, and are possibly still not understood, thereby highlighting a need for stronger normative protection of privacy rights.

From a somewhat different perspective, Kritikos calls for librarians and information professionals to engage openly in the debate and discussion around issues of the Right To Be Forgotten (RTBF) and delisting of web content, arguing that these, alongside the use of Internet filtering software are disrupting the information ecosystem and ethical norms around freedom of access to information. This is a good example of the clash of values between two competing rights, both worthy in their own intentions but sometimes misguided in their implementation.

Maceli's paper reviews the literature around the role of public libraries and librarians in educating patrons about the importance of privacy, the existence of many, diverse threats to their own privacy in the new technological era, and the availability of tools and techniques to enhance and protect this privacy. She recognises the complexity of this role when, despite the long-standing commitment of the library profession to the privacy of their users, it has not generally been seen as the role of the librarian to educate users about privacy protection. Education regarding privacy protection is also relevant to the paper by McGuinness and Simon, in this case in the context of students' use of social networking sites (SNS). Their mixed-methods study indicated that young people *are* concerned about privacy, and they do modify their online behaviour and use privacy settings to protect themselves according to the context in which they are posting content; however, the protective measures taken are fallible as a result of both human and system errors.

Context is also key to the next paper, in which Inoue discusses privacy and libraries in Japan. She describes how privacy with regard to reading matter is highly prized in the country, and then goes on to discuss specific relevant legislative attempts to protect the privacy of personal information. The relevance of this legislation to libraries is highlighted, and then illustrated via two case studies.

And finally, ending on a provocative note, Doyle picks up on McNealy's declaration of the death of privacy. His argument focuses on the use of big data analytics and the ways in which even aggregated and anonymised data can be used to detect patterns, and subsequent predictions of our own behaviour and lifestyles may be (often erroneously) inferred, in ways that can be damaging to our own interest. The paper argues that two of what he describes as 'the most promising means' of protecting ourselves from this misuse of data, obfuscation and the propertisation of personal information, are both doomed to failure. Thus he concludes that privacy is indeed a lost cause and trying to defend it from a moral point of view is no longer a viable cause. Whether this is a viewpoint that is palatable to a library profession long committed to the defence of patrons' privacy is a matter of contention: certainly, it is not a battle that IFLA is yet ready to regard as lost. It is, however, a critical matter for debate and we hope that all the papers in this Special Issue provoke similar food for thought around this important topic.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Alfino M (2001) Information ethics in the workplace: Misplacing privacy. *Journal of Information Ethics* 10(2): 5–8.

Clarke R (2006) Introduction to Dataveillance and Information Privacy and Definition of Terms. Australian National University. Available at: http://www.cse.unsw.edu.au/~cs4920/resources/Roger-Clarke-Intro.pdf (accessed 26 June 2018).

Floridi L (2005) The ontological interpretation of informational privacy. *Ethics and Information Technology* 7(4): 185–200.

Gorman M (2000) *Our Enduring Values: Librarianship in the Twentieth Century*. Atlanta, GA: ALA.

IFLA FAIFE (2012) Code of Ethics for Librarians and Other Information Workers. Available at: https://www.ifla.org/publications/node/11092 (accessed 26 June 2018).

Moor JH (2006) Using genetic information whilst protecting the privacy of the soul. In: Tavani HT (ed.) *Ethics, Computing and Genomics*. Sudbury, MA: Jones and Bartlett, pp. 109–120.

Sprenger P (1999) Sun on privacy: 'Get over it' *Wired*, 26 January 1999. Available at: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ (accessed 25 June 2018).

Tavani HT (2008) Informational privacy. In: Himma K and Tavani HT (eds) *The Handbook of Information and Computer Ethics*. Hoboken, NJ: Wiley, Ch. 6.

United Nations (1948) Universal Declaration of Human Rights. Available at: http://www.un.org/en/universal-declaration-human-rights/ (accessed 25 June 2018).

Warren S and Brandeis L (1890) The right to privacy. *Harvard Law Review* 4(5):193–220.

Witt S (2017) The evolution of privacy within the American Library Association, 1906–2002. *Library Trends* 65(4): 639–657.

Article

International Federation of Library Associations and Institutions
2018, Vol. 44(3) 170–182

DOI: 10.1177/0340035218777275
journals.sagepub.com/home/ifl

Privacy awareness issues in user data collection by digital libraries

Elaine Parra Affonso
São Paulo State University (UNESP); Faculdade de Tecnologia (FATEC), Brazil

Ricardo César Gonçalves Sant'Ana
São Paulo State University (UNESP), Brazil

Abstract

This work has the objective of investigating privacy aspects in the collection of data by the National Digital Libraries of South America. Country-specific digital libraries were examined using an exploratory research method to identify data these libraries collected both with the user's awareness and in the explicit presence of privacy policies within their environments. Brazil's National Digital Library environment was also examined by using the Wireshark tool to identify possible data collected implicitly during user interaction. We identified that only two of the examined digital libraries provide privacy guidance, and in relation to the collection process, the data that are collected without the knowledge of the user stand out more than the data that the user makes available consciously. It is concluded that privacy issues can be influenced by low user awareness of when, how and where data collection takes place, and the availability of privacy policies becomes essential in digital libraries to raise awareness about this process.

Keywords

Abstraction layers, awareness, data collection, privacy

Submitted: 18 September 2017; Accepted: 14 February 2018.

Introduction

With the increased use of technological devices, activities that realize data collection increase, reaching all segments of society. As such, it becomes necessary to better understand this process which often does not occur in a perceptible way to the user who has low awareness about when, how, and where it occurs. Since data relating to such actions may reveal individuals' personal information, threats to privacy emerge. Tanenbaum and Wetherall (2011) point out that due to rapid technological growth, the differences between data collection, storage, and processing are rapidly disappearing, making issues in this process intangible to the user.

The effect that information technology has on privacy causes new concerns and can be analyzed from four factors: the amount of information collected by digital devices and environments; the speed with which information can be shared; length of storage time; and the type of information that can be collected (Tavani, 2008).

Threats to privacy extend from the moment that the user transfers their activities to the digital medium and leaves traces of interactions in those environments. According to O'Hara and Shadbolt (2014) each time a new technology emerges that allows communication and interaction without the need for physical presence, a new level of abstraction is created, because as long as there is no physical presence, the individual leaves representations in the environment making it harder to hide their interactions.

In addition to the data collection performed in digital environments explicitly, there are data that

Corresponding author:
Elaine Parra Affonso, São Paulo State University, Hygino Muzzi Filho Avenue 737, Marília, São Paulo State, Brazil.
Email: elainepff@gmail.com

circulate silently in computer networks. Silent data circulation results in lack of awareness into the data collection process, causing informational asymmetry[1] between data holders and users. It is emphasized that information asymmetry provides more power for those who hold the data, especially when it comes to personal data, and increases the lack of control over the collection. According to Mayer-Schönberger (2011), the loss of control is rarely transparent to the user since it occurs without the individual perceiving. In this way, when the individual loses control, others gain in the power of information.

In the digital libraries scenario, data collection can occur at the moment of user interaction when performing a search or when filling in registers to request information – including data traffic in computer networks. These environments must provide measures and guidelines regarding data collection issues that can identify individuals. According to Klinefelter (2016), digital libraries, while providing free access to information, also imply new privacy risks. This form of access often requires the user to identify themselves and their own interaction with the environment that leaves digital traces sufficient enough to be used in the commercial environment or by government agencies (Klinefelter, 2016).

In libraries, privacy is essential as it allows the user to choose and access information without fears, judgments, or punishments. The right to read can be compromised if the individual's privacy is threatened, and true freedom of choice in libraries requires both a variety of materials and the assurance that interaction and choices are not being monitored (ALA, 2017).

This study aims to investigate the privacy aspects in the data collection phase using the National Digital Libraries of South America as a basis. The following questions guide this study:

1. What data are collected during user interaction with the digital library site?
2. Are the data that is collected perceptible to the user? Or does the very interface of this process diminish the perception about the data collected?
3. Does the collected data imply privacy threats?
4. Are there privacy policies that explain to the user what data are collected during interactions on digital library sites?

Methodology

The methodology used in this study was based on: (1) identification of National Digital Libraries of South American countries through the Google search engine with the term national digital library descriptor and country name; (2) exploratory research on digital library sites to identify the following issues: explicit provision of privacy policies; communication protocol used; identification of data collected with the user's awareness; (3) identification of possible data collected implicitly in the user's interaction with digital environments, specifically with Brazil's National Digital Library.

In order to identify and demonstrate the possible data implicitly collected, and the elements involved in the data collection phase during the user's interaction with Brazil's National Digital Library, the Wireshark[2] tool was used. Through the Wireshark tool, it is possible to analyze each data packet that the user received and sent to the destination, verifying the source IP and destination IP data, number of ports, date and time of the request. When the page does not use encryption, it is possible to check the data sent from the user to the digital environment.

In this study, the Wireshark version 2.4.0 was installed and executed in the author's own equipment so that it was possible to initiate the capture and identification of traffic data packets when searching in the digital collection of Brazil's National Digital Library website, which consisted typing the title of the book "o cortiço" in the search field. The packets trafficked during access to the website were collected and a package was selected for analysis and exemplification of possible collection performed by the data holders during the data collection phase.

Subsequently, the main data present in the package were correlated with the layers of the Open System Interconnection (OSI) model, including verification whether the data are identifiers, quasi-identifiers, or sensitive.

The collection of data on the website of Brazil's National Digital Library was carried out through a notebook with the Windows operating system, with the wireless connection. It should be emphasized that the collection performed during the user's interaction with the digital library website was done by the authors' equipment and using the home network. Only the data resulting from this interaction have been viewed and analyzed. The data collection of this research was carried out in July 2017.

This text is divided into the following sections: Collection phase and privacy issues; Open System Interconnection (OSI) model and abstraction in the collection phase; Tool for data collection in computer networks; Results and discussions, and Considerations.

The main contribution of this article is to highlight the phase of data collection in the web environment,

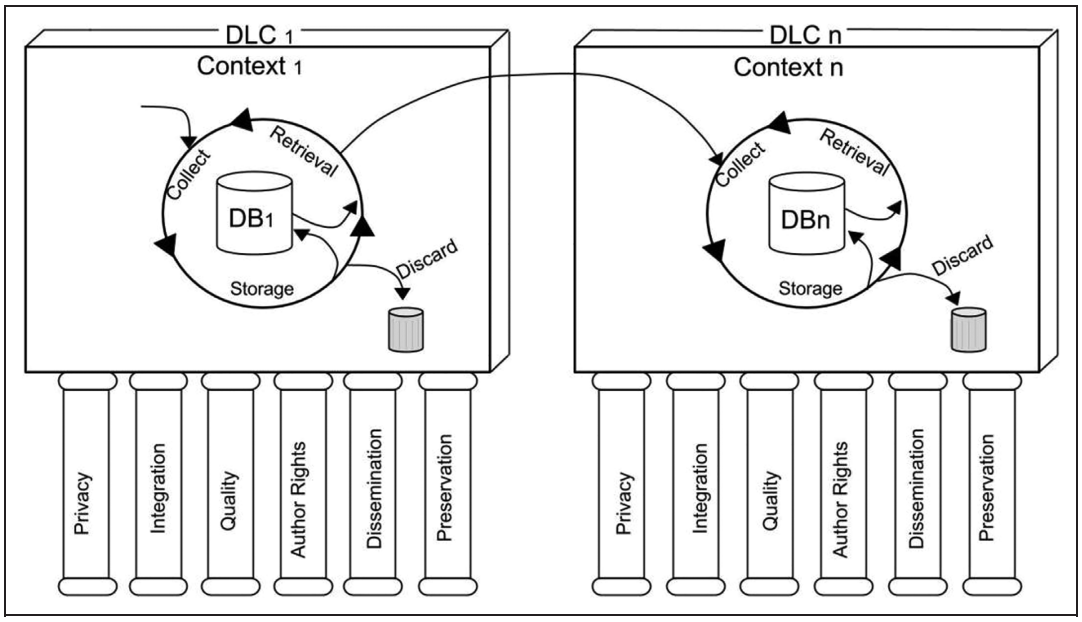

Figure 1. Data life cycle for information science.
Source: Sant'Ana (2016: 123)

explicitly in digital libraries, in order to demonstrate that the collection of data exceeds the data made available by the user, and the architecture of the communication networks themselves contributes to making this process more distant from the user. As a consequence, privacy threats increase.

Collection phase in the data life cycle and the privacy aspects

As a way to highlight the different moments and objectives present in the access and use of data, Sant'Ana (2013) proposes the Data Life Cycle for Information Science (DLC-IS). DLC-IS is a theoretical framework delimited in four phases: collection, storage, retrieval, and disposal. The phases are permeated by the factors privacy, integration, quality, author rights, dissemination, and preservation (Figure 1). This model seeks to contribute to a better understanding of these phases and involved resources.

The collection phase delimits the moment in which the purpose is to obtain data and in which the planning and execution of several activities occurs, among them: identification of the need for collection; definition of the data to be collected; procedures for collection; data format; and treatment necessary for the intended purpose of the collection (Sant'Ana, 2016). In the DLC, the collection phase is permeated by the factors privacy, integration, quality, copyright, dissemination, and preservation of data (Sant'Ana, 2016).

Among these factors, the collection of data can cause threats to the privacy of the individuals who participate in the collection context. In the case of this research, the user's privacy issues are taken into account in relation to the collection made by the data keeper, in the case of digital libraries. Regarding data quality, origin, collection, reliability, utility, and physical and logical integrity guarantees, these are fundamental at this stage of the data life cycle.

Regardless of the factors involved, digital environments such as digital libraries, social networks, search engines, mobile applications and the most diverse applications collect data with the justification of providing better results for users who make use of these environments. However, it is necessary to make users aware of the data collected and the privacy implications of individuals interacting with these environments.

The World Digital Library (2017) describes in its privacy policy that the environment offers a better service through the collection and storage of non-personally identifiable information and cookies. Their privacy policy also states that it only collects personal information the user voluntarily provides, and the use is intended only for the service. In addition, there is mention of the implementation of safeguards to protect any information collected.

The social network Facebook (2017) describes in its privacy policy that it collects data regarding the activities of the users and the information made available by said activities, including data about people and groups with which it connects. In addition to interactions and information, Facebook also collects data from payments, devices, sites and applications that use Facebook services, as well as information from external partners and companies of this social network.

Data collection can happen in two ways: directly involving the user, and collections that do not directly involve the user. When the user fills out a form on a website, he is aware that the collection is happening and understands that this activity brings benefits even though they do not understand the privacy implications. On the other hand, when browsers send cookie information back to the site or when surveillance cameras record activities in an environment, the collection occurs without user involvement (Spiekermann and Cranor, 2009).

Information that may seem harmless can be linked to new contexts., and it becomes difficult to get a sense of when privacy has been violated. As such, the Web becomes an environment that gathers more information about the user than other environments making it possible to construct an image of the user using the Web (Nissenbaum, 2011: 36).

When the user is interacting in a digital environment, a set of personal data is revealed to the data keeper. This personal data can be classified as: identifiers that uniquely identify the individual; quasi-identifiers that, when combined with other databases, allow the identification of the individual; sensitive data that reveal confidential information and, where disclosed, may place the data subject in situations of constraints; or non-sensitive data – the collection or dissemination of which does not imply privacy threats (Samarati, 2001).

Furthermore, according to the new Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data, personal data may be defined as:

> information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (GDPR, 2016: 33)

The problems related to the collection of user data and privacy are numerous and with consequences that are not yet estimated or perceived by individuals. Consequences may include issues of discrimination, induction in the choice of products and services, and correlation of data for the construction of user profiles. Fabian et al. (2010) point out that due to the repression imposed by some political regimes, in which copyright, freedom of expression and, in particular, free access to information are restricted, the various possibilities of data collection by various means can lead to the pursuit of individuals if their identity is revealed.

Through the dissemination of privacy policies, these environments are designed to offer users an awareness of data collection. However, the perception of the user may be linked to the description that the company makes available in these documents or in the data that the user makes available during the use of the service, such as username, passwords, field fields, search terms, among others. Thus, awareness about data collection involves the user's knowledge about how their data will be collected. The purposes of privacy policies should be to make information about data collection more clear and accessible and to broaden the user's perception of this process.

In these digital environments, computer networks are essential (specifically the Internet, attracting myriads of new users) and make it possible to configure several pages of information containing texts, figures, sounds, and video with embedded links to other pages (Tanenbaum, 2003).

To minimize the complexity involved in the operation of these communication networks, they are organized into layers of abstraction whose purpose is to provide services to the upper layers, isolating these layers from the implementation details (Tanenbaum and Wetherall, 2011). The concept of abstraction is common in computer science, receiving various names such as information hiding, abstract data types, and encapsulation (Tanenbaum and Wetherall, 2011).

In this way, the digital environments, when collecting data using computer networks, rely on a layered model of abstraction with the purpose of hiding from the user technical details of the activities and data collected. The most important abstraction principle in the field of communication in computer networks is the OSI reference model.

With this in mind, the layered approach proposed by the OSI reference model becomes relevant to hide details that are not operationally important to the user. Although it visualizes the communication process in the computer networks in a generalized way and with reduction of complexity, the layers specified in the model facilitate the understanding of moments and elements involved in this process, including data collection.

OSI reference model

The OSI reference model is a layered structure whose purpose is to inform the function of each layer and to keep software or hardware details hidden when

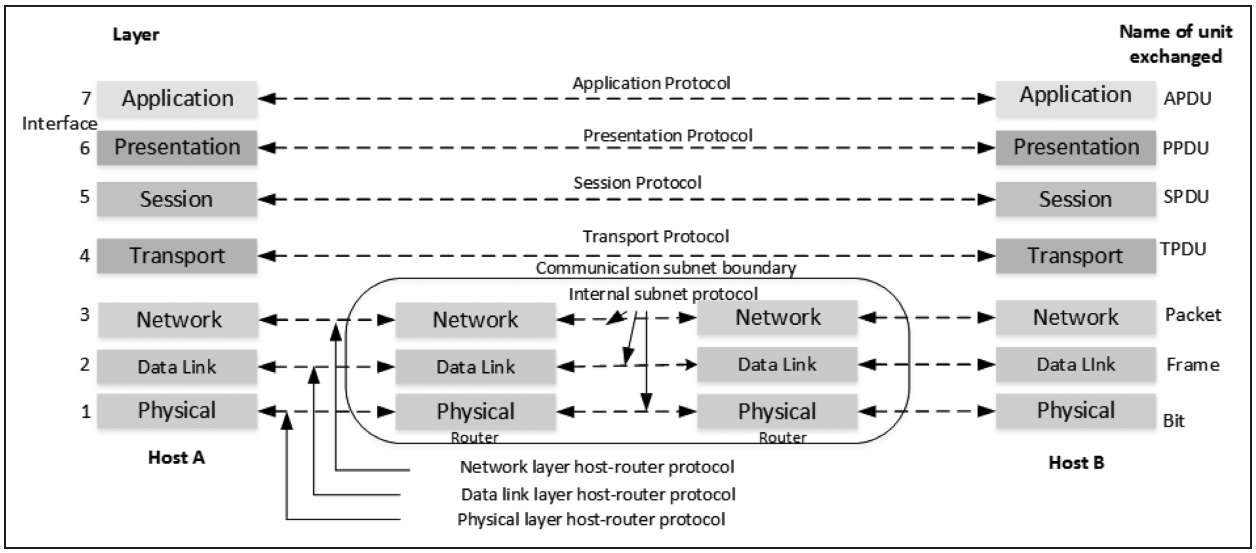

Figure 2. Layers of abstraction OSI reference model.
Source: Tanenbaum (2003: 41)

providing service to users (Tanenbaum and Wetherall, 2011). This model presents three concepts: services, interface, and protocol, making their differences explicit. The OSI model, through each layer, performs services for higher layers, which, in turn, determine what the layer accomplishes by defining the semantics of the layer. The interface informs how the upper layer processes can be accessed and the protocols make the work feasible, that is, they provide the services (Tanenbaum and Wetherall, 2011). This model was developed by the International Standard Organization (ISO) as a means to internationally standardize the protocols that are used in the layers: physical, link, network, transport, session, presentation and application (Tanenbaum, 2003) (Figure 2).

The OSI layered model helps to organize and simplify the understanding of operational concepts that might otherwise be unnecessarily detailed and complex, simplifying the complexity of computer network protocols and technologies by abstracting them from each other in multiple tiers (Nikkel, 2005).

Abstraction is fundamental in dealing with complexity. Its purpose in the network environment is to ignore small differences between the elements and processes of communication networks by considering only their similarities. An efficient abstraction is one that highlights important details for the user without considering those that are irrelevant to interaction (Sclavos et al., 1994).

The abstraction provided by the OSI model in communication networks can have an effect on the privacy of individuals interacting in the network environment by hiding different types of data collected during this interaction such as: the result of access to social networks, search engines, to service sites, such as loans and book searches in digital libraries.

Sniffers/Wireshark

One way to verify the functioning of computer networks is by means of tools capable of monitoring the flow of data passing through networks at various levels of the OSI model in real time, such tools being called packet analyzers of communication networks or sniffers. These tools run on some networked device that passively receives all data packets from the link layer. After capturing the data that is addressed to the machine, these can be saved for later analysis (Asrodia and Patel, 2012).

Sniffers can be used to convert binary data into a human-readable format, analyze network performance, detect network intrusion, detect spyware, and learn about protocol performance in computer networks (Orebaugh and Ramires, 2004). According to Asrodia and Patel (2012), in addition to the use of sniffers for traffic monitoring and analysis, this use provides several solutions for problems with computer networks. However, they can be a security threat to the individual, because of their ability to capture all incoming and outgoing network traffic, including passwords and usernames or other sensitive data.

In this study, we used Wireshark, free software based on the General Public License (GPL), which captures and analyzes network packets in real time, displaying in detail the data that is circulating in the computer network. Wireshark is primarily used by: network administrators, to troubleshoot computer networks; security engineers, when they need to examine

problems related to network security; developers, who seek to debug protocol implementations; students and other network professionals who use the tool to learn about internal network protocols (Wireshark, 2017). This tool was used during interaction with Brazil's National Digital Library to verify the possible data collected by the digital environment.

Results

The analysis included the identification of digital libraries in South America, based on the collection phase with the Privacy factor of the DLC of the libraries. As a result, nine countries that have National Digital Libraries were found. However, it was not possible to access the websites of the National Digital Libraries of Bolivia and Guiana because they were not found on server, and the National Digital Libraries of Suriname and French Guiana were not found.

Analysis of digital library sites

It can be seen in Table 1 that only the National Digital Library of Brazil's website and the National Digital Library of Colombia's website present some orientation regarding privacy. Most of the libraries use HTTP (HyperText Transfer Protocol), configuring issues with data security and consequently threats to privacy and protection of personal data, except Argentina and Brazil. Three libraries (Argentina, Brazil, and Chile) request some type of registration to reserve documents and, this broadens the set of data about the user and possible implications in the privacy of individuals.

The collected data that are explicit to the users are those requested at the time of registration, authentication to access a service or the search term for retrieval of documents or books.

Data collection using Wireshark

When using the Web, the user requests service based on the client-server model, in which the user requests information and the server responds. Between the lines of this process, the data collection is present, passing through the layers of the OSI reference model. Evidences of privacy threat and levels of abstraction are presented in the next topics in the data collection phase, through access to the National Digital Library of Brazil's website.

To demonstrate the process, the National Digital Library of Brazil page was requested through a query to retrieve a particular book; this activity does not require the user to be logged into the system. In this way, the only data that the user makes available consciously and voluntarily is the search term. The user must log into the site if they wish to reserve books or documents.

This process was accompanied by the Wireshark software and resulted in the collection of 498 packages, of which 267 were directly identified as user interaction packets with the library site. Of this total, 117 packets sent from the originating machine (user) to the server (library page) and 187 packets sent from the server to the user's machine.

To perform this study, package 68 was selected, corresponding a POST method, whose purpose is to allow the user to send data to the server, in this case, to perform the search in the digital collection. The description of the fields obtained during capture with the Wireshark tool follows.

In the Frame field, the metadata of the selected packet relative to capture information, time variables (such as the date and time the packet was captured and the time at which the packet was collected), package size, and protocols are specified acted in this package. In this layer, a GUID (Globally Unique Identifier) is defined in the field "interface id", value generated by the operating system in order to create a unique reference number for the resource (Figure 3).

The Ethernet II field, (Figure 4), is related to the proposal of the data link layer, in order to be the path understood between the origin and the destination, transporting data packets through protocol.

For identification of the source and destination device, the MAC address (Media Access Control), a unique address of the board, is collected. In this case, the MAC address of the Src user card: HonHairPr_f8: b1:51 (xx: xx: xx: x: xx: xx) and the destination MAC address Tp-LinkT_15: e5: 66 (xx: xx: xx: xx: xx: xx).

The Internet Protocol Version 4 field (Figure 5) represents the network layer, through which it selects paths, so that data packets can travel. To do this, it uses the IP (Internet Protocol) address, and in this way, the packets are identified through the source and destination IP address. Geolocation data is also specified for the source and destination, using the Source GeoIP and Destination GeoIP fields.

The Transmission Control Protocol (TCP), Figure 6, refers to the transport layer of the OSI model, in order to allow communication between programs or processes through the port number. Note the presence of the TCP, which carries out the communication through the Src Port: 55498 (55498) and the destination port Dst Port: us-cli (80).

The HTTP is related to the application layer of the OSI model, the only layer typically perceived by the user, which, through the HTTP, allows communication between browsers and servers. Therefore, HTTP

Table. 1. National Digital Library – Countries of South America.

Name	Country	Privacy Policy (Explicit)	Protocol	Collected data (Explicit)	Need of requests registration for download or preview
Bibliotec Nacional Mariano Moreno[1] (Digital Collections)	Argentina	No	https[2]	Contact information (name, email, subject, destination, message) Reservation (login and password) Search term	No However, request login for material reservation
Biblioteca Nacional Digital Brasil [3]	Brazil	No The solely available policy is provided by Disqus service, referring to the data collected in the comments about the document	https	Contact us (Name, email, subject, message) To receive updates (email) Search term	No However, request login for material reservation
Biblioteca Nacional Digital de Chile[4]	Chile	No	http	Contact data (Name, last name, gender, region, occupation, email, action, comment)	No However, it requests registration for the option "request copying" of images with better resolution
Biblioteca Nacional de Colômbia[5]	Colombia	It is presented in the link 'citizen Service' guidelines on personal data	http	Material reservation (email and password) Subscribe citizen service (Type of application, Preferential attention, First name, Second name, Surname, Second surname, Document type, Document number, Address, Optional fixed phone, Cell phone number, Optional cell number, Email, Optional email, country, Department, City, Description of the request), Search term	No
Biblioteca Nacional del Ecuador Eugenio Espejo[6]	Ecuador	No	http	Subscribe to the repository (email and password) Search term	No
Biblioteca Nacional Paraguay[7]	Paraguay	No	http	Search term	No
Biblioteca Nacional del Perú[8]	Peru	No	http	Contact data (name, email, message) Search term	No
Biblioteca Nacional D Uruguay[9]	Uruguay	No	http	Email and password Search term	No
Biblioteca Digital de Venezuela[10]	Venezuela	No	http	Data for Comments (name, subject, comment) Search term	No

1.Available at: https://www.bn.gov.ar/ (accessed 3 July 2017).

2.It is secure HTTP, security principles are added, so clients send confidential information to servers (Belshe and Peon, 2015).

3.Available at: https://bndigital.bn.gov.br/ (accessed 3 July 2017).

4.Available at: http://www.bibliotecanacionaldigital.cl/bnd/612/w3-channel.html (accessed 5 July 2017).

5.Available at: http://catalogoenlinea.bibliotecanacional.gov.co/client/es_ES/bd. (accessed 6 July 2017).

6.Available at: http://repositorio.casadelacultura.gob.ec/ (accessed 6 July 2017).

7.Available at: http://bibliotecanacional.gov.py/bibliotecadigital/ (accessed 10 July 2017).

8.Available at: http://bdigital.bnp.gob.pe/Bvirtual/Home (accessed 10 July 2017).

9.Available at: http://bibliotecadigital.bibna.gub.uy:8080/jspui/ (accessed 10 July 2017).

10.Available at: http://bibliotecadigital.bnv.gob.ve/ (accessed 12 July 2017).

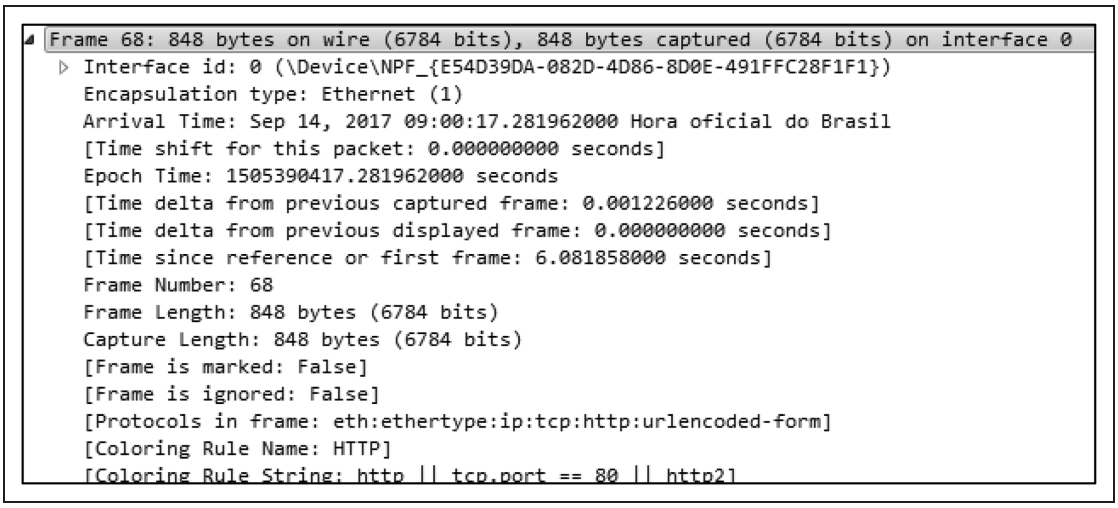

Figure 3. Trimming the Frame field in Wireshark.

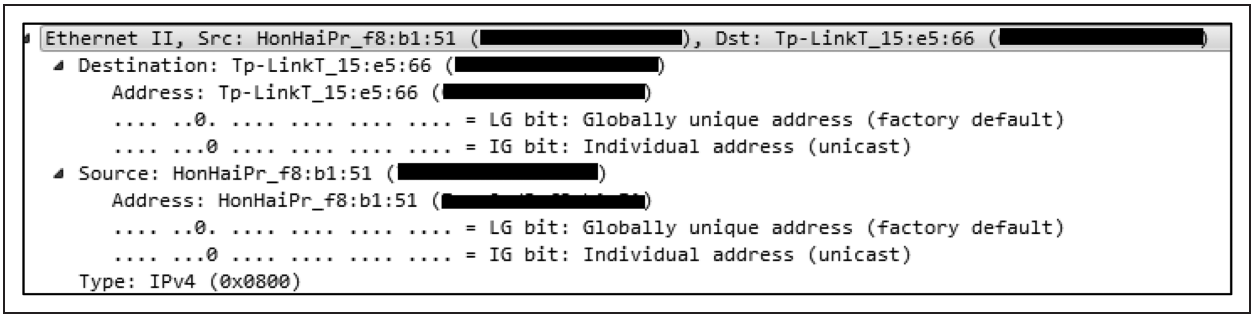

Figure 4. Trimming the Ethernet II field in Wireshark.

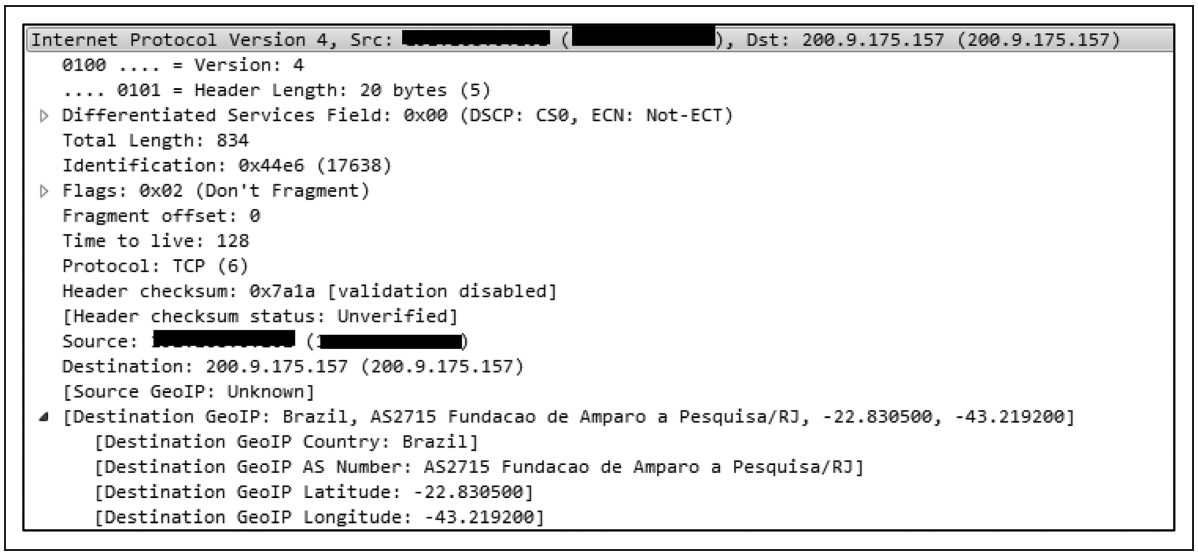

Figure 5. Trimming the Internet Protocol Version 4 field in Wireshark.

is used to send application-layer commands between client and server.

Using the POST command, the client (user) sends a package to the server. This command is used, when the user fills some form in the page (in this case, text to perform the search). Among the information specified in the POST method are: the Uniform Resource Identifier (URI) of the library site, the address to which the data is being sent; user-agent header,[13] with browser and operating system information; referrer,

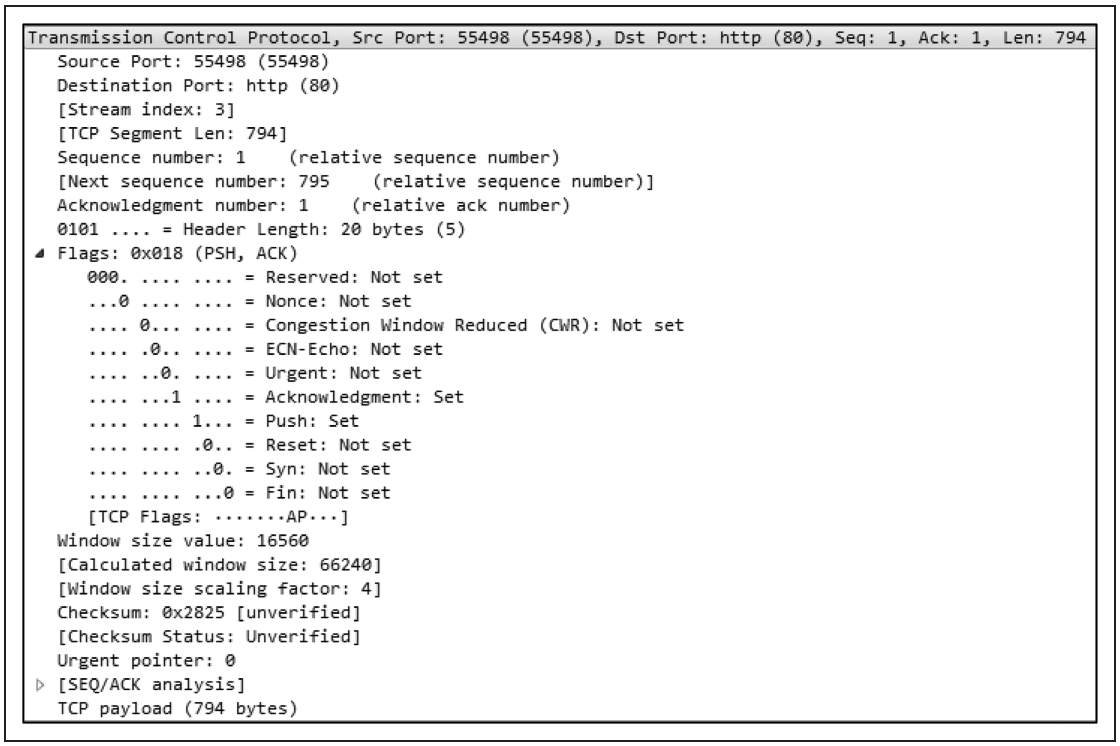

Figure 6. Trimming the Transmission Control Protocol field in Wireshark.

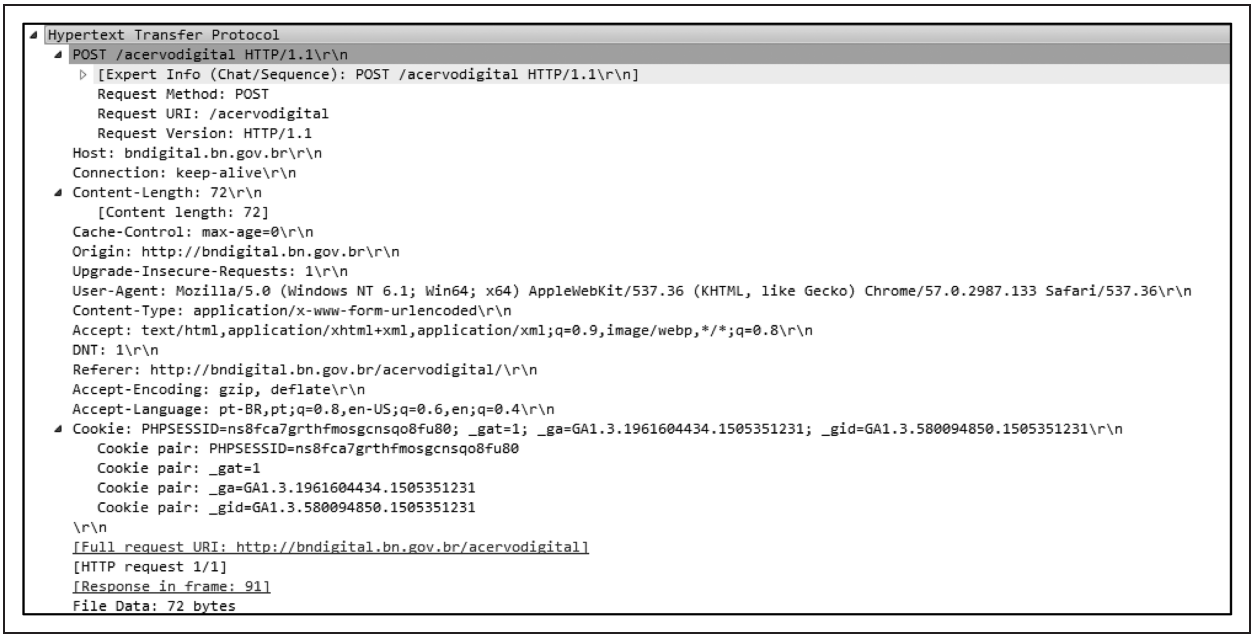

Figure 7. Trimming the HyperText Transfer Protocol field in Wireshark.

which indicates the URL (Uniform Resource Locator) requested, and the accept-language header, which informs the server the language the client machine will be using (Figure 7).

Subsequently, the search terms sent to Brazil's National Digital Library are displayed, explicit in the HTML Form URL Encoded field of the package (Figure 8). It is observed in Figure 8 that the data presented are the ones that the user made available in the search field, data that are in the application layer, the one closest to the user, allowing awareness and apparently do not cause privacy threats when used alone.

Discussions

We analyze possible data collected by the National Digital Libraries sites in two ways: through the

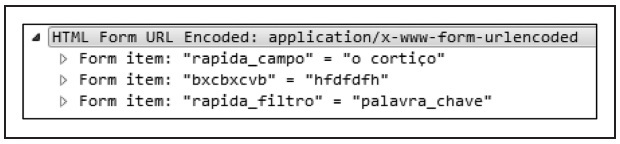

Figure 8. Trimming the HTML Form URL Encoded field in Wireshark.

exploration of the sites and identification of which data can be collected, and analysis of a package of traffic data referring to the user interaction Brazil's National Digital Library website. In the exploration of the sites it was observed that the availability of privacy policies in digital libraries, which are essential to promote the user's awareness about the data collection process, is limited. Additionally, most sites operate under the HTTP which does not provide guarantees regarding the confidentiality and privacy of the data.

Regarding data collection with the use of Wireshark, it is possible to verify data that are present during the user interaction with the digital environment. The data were collected in only one package range from the request date and time, IP address, location data, browser and operating system information, cookies, and machine MAC address and number of ports for communication. These data are not perceptible to the user at the moment of interaction with the environment, confirming the asymmetry of information between the holder and user. The perceptible data are only those that are reported by the user, such as e-mail, registration data, and search term, as shown in Table 1.

Regarding privacy threats in the data collection phase, Table 2 presents a summary of the main data present in the user-server interaction packet when accessing Brazil's National Digital Library site. Each data attribute is classified by its privacy type (Identifiers, Quasi-Identifiers, Sensitive and Not Sensitive).

The MAC address represents a unique and immutable value that allows the identification of the user's machine. The search term and cookies are considered sensitive data, since they store information that refers to something particular to the individual, and that if used improperly can put the subject referenced in these data in situations of embarrassment. However, although IP data, geolocation data, accept-language header, source port, destination port, user-agent are not data that allow uniquely identifying the individual, when correlated with other databases, the examination may result in the identification of the individual.

Through the user-agent header, each time the user interacts with digital environments, this type of data reveals exactly the browser that the user is using and some more data. This information when combined, for example, with location data, can help distinguish users from each other's Internet, making it easier to fingerprint to track on the Web.

Figure 9 illustrates the data collection process and abstraction levels, represented by the layers of the OSI model. This process starts at the time of the client's request (source) to an HTTP page or to an HTTPS page, in which the interaction of the user with the environment depends on the data it provides for the application (conscious interaction process). The architecture of computer networks, divided through the layers of the OSI reference model, determines the interfaces where abstraction is present. This abstraction occurs through the encapsulation of the data collection effected by the protocols that provide the transition of data between the layers, in which is circulated an amount of data that can threaten the privacy of the user, as shown in Table 2. Thus, the very interface of computer networks can contribute to decreasing the user's perception of data collection, making privacy issues more tense and complex.

This research sought to emphasize the possible data collected by digital environments during user interaction. In the case of digital libraries, it was observed that the data collection refers to the data of registers and search term – a situation that is explicit to the user during the interaction with the pages of the digital libraries. However, with the analysis of network packets, it is noted that many other data can be collected and are not perceptible to the user, such as IP address, user-agent header, geolocation, and cookies.

Thus, the user's perception about data collection is based on the data made available. It is not explicit that, encapsulated in the network layers, other data are collected and can threaten privacy, increasing the abstraction for the user about this process. From a different perspective, the data keeper's knowledge of the data across the network layers is increased. However, through this process, other data subjects are intercepted resulting in new or even unwanted collections and emerging privacy threats for individuals.

Most environments do not provide privacy policies, which can contribute to minimizing user insight on the data collection phase. Digital environments should in their content make explicit not only the collection of data that are easily noticeable to the user but also the data that are present in the flow of communication through computer networks.

Considerations

In this study, we have highlighted the privacy issues in the collection phase in digital library sites,

Table. 2. Synthesis of the main data present in the user-server package.

Access with http protocol					
Field	OSI Layer	Atributte	Value	Data	Awareness
Ethernet II	Data link	Source MAC	HonHairPr_f8: b1 (xx: xx: xx: xx: xx)	I	Low
		Destination MAC	Tp-LinkT_15: e5:66 (xx: xx: xx: xx: xx: xx)	I	
Internet Protocol	Network	Sorce IP	IP xxx.xxx.x.xxx	QI	Low
		Destination IP	IP 200.9.175.157	QI	
		Source GeoIP	*Unknown*	QI	
		Destination GeoIP	Brazil, AS2715 Fundação de Amparo à Pesquisa, Latitude: - 22.830500, Longitude: - 43.219200	QI	Low
Transmission Protocol Version	Transport	Source Port	Src Port: 52368(52368)	QI	Low
		Destination Port	Dst Port: us-cli (80)	QI	
Hypertext Transfer Protocol	Application	User-Agent	Mozilla/5.0 (Windows . . . .)	QI	Low
		Accept-Language	Pt-BR\r\n	QI	Low
		Cookies	PHPSESSID . . .	S	Low
		Form item: rápida_campo	o cortiço	S	High
		Form item: rápida filtro	Keywords	NS	

I: identifier; QI: Quasi-Identifier; S: Sensitive; NS: Not Sensitive.

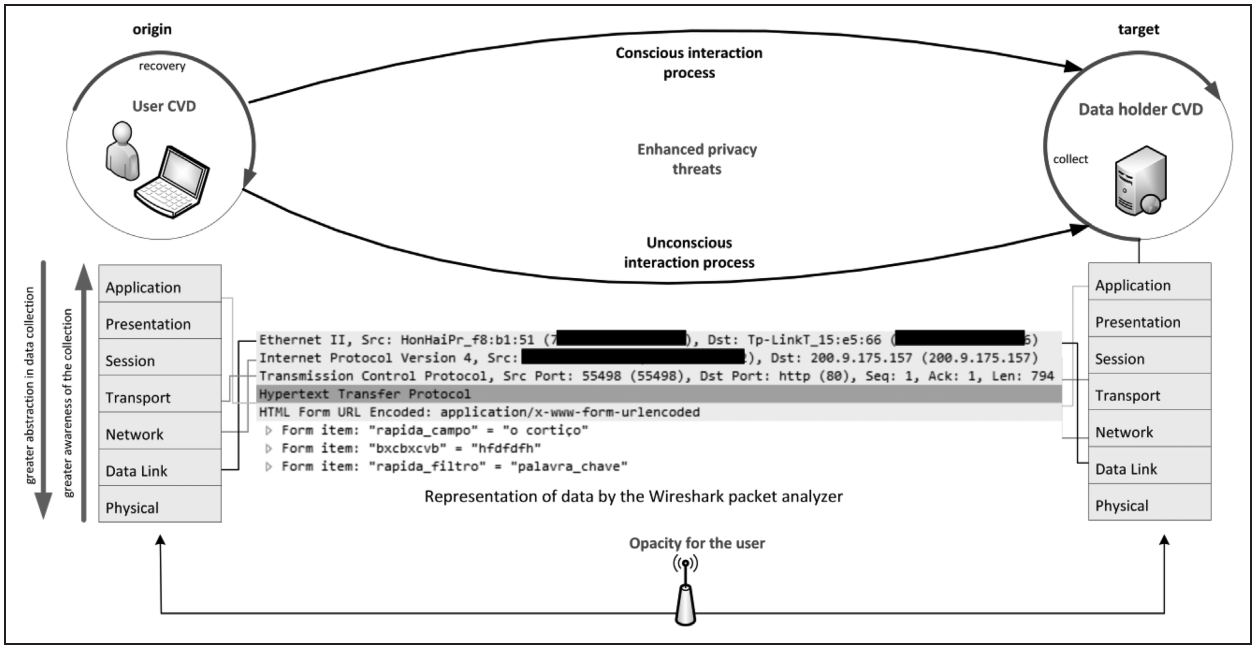

Figure 9. Data collection process.

analyzing the data that are collected both explicitly and implicitly. For this, an exploratory research was carried out in the sites of the National Digital Libraries of South America, and in the analysis from the traffic data resulting from the interaction of the user with Brazil's National Digital Library. By organizing and simplifying their complex context, abstraction layers encapsulate details of communication in computer networks, generating hidden details about collection flows to which users are unknowingly inserted, and increase the privacy-related issues of individuals referenced in sets of data.

Thus, it is observed that the opacity in this scenario goes beyond the low awareness of the user about the collection process and may imply threats in privacy issues since data processed in the networks can result in the identification of the individual. Other aspects can also be of concern, such as the possible correlation of the data with other databases, forming user profiles and increasing the knowledge of the data holders regarding the user.

In conclusion, privacy issues can be influenced by the user's low awareness of when, how and where data collection takes place. Digital libraries need to make privacy policies available for the purpose of guiding users in relation to data collection ensuring that these policies not only specify data that users voluntarily provide, but also data that is abstracted into the layers of computer networks.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Elaine Parra Affonso http://orcid.org/0000-0002-3953-462X

Ricardo César Gonçalves Sant'Ana http://orcid.org/0000-0003-1387-4519

Notes

1. A concept based on the asymmetric information theory developed by Akerlof (1970), which analyzes the implications of asymmetric information in used car markets, in which the seller of a car knows more than the buyer about the quality of that product.
2. Download available at: https://www.wireshark.org/download.html
3. Identifies the user's browser and provides certain operating system details to the servers that host the sites that the user visits (MICROSOFT, 2017).

References

Akerlof G (1970) The market for 'lemons': Quality uncertainty and the market mechanism. *Quarterly Journal of Economics* 83(3): 488–500.

ALA (American Library Association) (2017) Privacy. Available at: http://www.ala.org/advocacy/privacy (accessed 15 July 2017).

Asrodia P and Patel H (2012) Network traffic analysis using packet sniffer. *International Journal of Engineering Research and Applications* 2(3): 854–856.

Belshe MPR and Peon R (2015) Hypertext Transfer Protocol Version 2 (HTTP/2), RFC7540. Internet Engineering Task Force (IETF). Available at: https://tools.ietf.org/html/rfc7540 (accessed 3 August 2017).

Facebook (2017) Políticas de privacidade do Facebook. Available at: https://www.facebook.com/privacy/explanation?pnref=lhc (accessed 8 May 2017).

Fabian B, Goertz F and Kunz S et al. (2010) Privately waiting: A usability analysis of the Tor anonymity network. In: *Sustainable e-business management: 16th Americas conference on information systems, AMCIS 2010*, Lima, Peru, 12–15 August 2010, pp. 63–75. Available at: https://www.researchgate.net/publication/220893134_Privately_Waiting_-_A_Usability_Analysis_of_the_Tor_Anonymity_Network (accessed 16 June 2017).

GDPR (General Data Protection Regulation) (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (accessed 3 July 2017).

Klinefelter A (2016) Reader privacy in digital library collaborations: Signs of commitment, opportunities for improvement. *I/S: A Journal of Law and Policy for the Information Society* 13(1): 199–244. UNC Legal Studies Research Paper. Available at: http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1027&context=faculty_publications (accessed 8 July 2017).

Mayer-Schönberger V (2011) *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

Microsoft (2017) User agent. Available at: https://msdn.microsoft.com/en-us/library/hh920767(v=vs.85).aspx (accessed 3 June 2017).

Nikkel BJ (2005) Generalizing sources of live network evidence. *Digital Investigation* 2(3): 193–200.

Nissenbaum H (2011) A contextual approach to privacy online. *Daedalus* 140(4): 32–48.

O'Hara K and Shadbolt N (2014) *The Spy in the Coffee Machine: The End of Privacy as We Know It*. London: Oneworld.

Orebaugh AD and Ramirez G (2004) *Ethereal Packet Sniffing*. Syngress.

Samarati P (2001) Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering* 13(6): 1010–1027.

Sant'Ana RCG (2013) data life cycle for Information Science (DLC-IS). In: *Encontro Nacional De Pesquisa Em Ciência Da Informação*, 14, 2013, Florianópolis. Anais . . . Florianópolis. Available at: http://enancib.sites.ufsc.br/index.php/enancib2013/XIVenancib/paper/viewFile/284/319 (accessed 3 January 2017).

Sant'Ana RCG (2016) Data life cycle: A perspective from the Information Science. *Information & Information* 21(2): 116–142.

Sclavos J, Simoni N and Znaty S (1994) Information model: From abstraction to application. In: *IEEE network operations and management symposium*, Orlando, Florida, USA, 14–17 February 1994, p. 183. IEEE.

Spiekermann S and Cranor L F (2009) Engineering privacy. *IEEE Transactions on Software Engineering* 35(1): 67–82.

Tanenbaum AS (2003) *Computer Networks*. 4th edn. [translated edition]. Rio de Janeiro: Pearson.

Tanenbaum A S and Wetherall J D (2011) *Computer Networks*. 5th edn. Rio de Janeiro: Pearson.

Tavani H T (2008) Informational privacy: Concepts, theories, and controversies. In: Himma KE and Tavani HT (eds) *The Handbook of Information and Computer Ethics*. Hoboken, NJ: John Wiley & Sons, pp. 131–164.

Wireshark (2017) User Manual. Available at: https://www.wireshark.org/docs/ (accessed 8 July 2017).

Word Digital Library (2017) Warnings from the World Digital Library. Available at: https://www.wdl.org/pt/legal (accessed 8 September 2017).

Author biographies

Elaine Parra Affonso is a doctorate student in Information Science at São Paulo State University (UNESP), School of Philosophy and Sciences, Marília, São Paulo State, Brazil. She has a Master's in Computer Science and is Professor in the Technology School of Presidente Prudente (FATEC), São Paulo State, Brazil.

Ricardo César Gonçalves Sant'Ana is Doctor in Information Science at São Paulo State University (UNESP). He is Adjunct Professor at UNESP, Campus Tupã and Professor in the Post-Graduate Program in Information Science at UNESP School of Philosophy and Sciences, Marília, Brazil.

Article

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 183–194

DOI: 10.1177/0340035218773783
journals.sagepub.com/home/ifl

Delisting and ethics in the library: Anticipating the future of librarianship in a world that forgets

Katie Chamberlain Kritikos
University of Wisconsin-Milwaukee, USA

Abstract
Traditional librarian ethics protect privacy and promote information access. The right to be forgotten and delisting have the potential to create a new online information ecosystem that disrupts ethical norms and redefines the role of librarians. Along with Internet filtering, the right to be forgotten and delisting are the harbingers of coming changes to content regulation and information access online. Librarians should engage with right to be forgotten F and delisting issues now to prepare for possible future disruptions of information flow in the library and shifts in information policies and laws around the world. This paper articulates the legal and ethical issues associated with delisting, lays the foundation for an international dialogue on delisting, and signals the need for future research. The international librarianship community needs a larger discussion about the issues related to the right to be forgotten and delisting, particularly on laws and policies on free speech and privacy.

Keywords
Delisting, ethics, information access, librarianship, privacy, right to be forgotten

Submitted: 5 September 2017; Accepted: 31 January 2018.

Introduction

Imagine that on the Internet, personal information about you that is embarrassing, such as a mortgage foreclosure that occurred many years before, appears in Internet search results for your name (Google Spain, 2014). Or that even more sensitive and delicate personal information, such as intimate photographs taken in privacy and shared in the confidence of a relationship, now appear in the search results (Citron and Franks, 2014; Laird, 2013). Or, worse yet, that these intimate images of your body are not only online without your consent, but appear alongside other personally identifiable information (PII) like your real name, address, and phone number (Laird, 2013: 45–47). What recourse do you have to remove this personal information from very public, very accessible Internet search results?

The right to be forgotten (RTBF) offers a solution by delisting (not deleting) from search results embarrassing, outdated personal information (Google Spain, 2014), as in the first example, or "revenge pornography" (Citron and Franks, 2014: 346), as in the second. After the groundbreaking 2014 ruling of the Court of Justice of the European Union (CJEU) in *Google Spain v. Costeja*, European Union (EU) law requires that at the data subject's request, an Internet search engine "delist" personal information that is embarrassing, inflammatory, or irrelevant from the search results for her name (CJEU, 2014; Google Spain, 2014). (The CJEU, the EU's chief judicial authority that manages the uniform interpretation and application of EU law (CJEU, n.d.), should not be confused with the European Court of Human Rights (ECHR), the international court established by the European Convention on Human Rights (ECHR, n.d.). The *Google Spain v. Costeja* decision affirming the legality of the RTBF and delisting is a signal light

Corresponding author:
Katie Chamberlain Kritikos, School of Information Studies, University of Wisconsin-Milwaukee, Milwaukee, WI 53217, USA.
Email: kchambs@gmail.com.

on the coming train of change for content regulation and information access on the Internet.

Fueled by different views of privacy and free speech in the European Union and United States, the scholarly debate over the RTBF often focuses on whether delisting protects human dignity (European Commission, 2012, 2014), as in the former, or sanctions the removal or blockage of information access tantamount to censorship (Fleischer, 2011, 2015; Rosen, 2012), as in the latter. The idea that an individual has agency over search results has also sparked international treatment in the news and in the courts (Alba, 2017), from France (CNIL News, 2015) to Japan (Umeda, 2017) and from Brazil (Sganzerla, 2016) to India (Bhattacharya, 2017), to name a few. Overall, the RTBF and delisting have the potential create a new online information ecosystem, one where certain information may not be accessible (Jones, 2013, 2016). While this changing information landscape certainly implicates international law and policy, it also may create a new ethical conundrum for librarians, who are committed to information access and free speech as part of the provision of library services.

Traditional librarian ethics protect patron privacy and promote information access in the library context (Zimmer, 2013). Along with Internet filtering, the RTBF and delisting are the harbingers of continued challenges to content regulation and information access online. While much library and information science (LIS) literature addresses how Internet filtering implicates librarian ethics and information access (see, for example, US v. ALA, 2003; ALA Council, 2015; Jamali and Shahbaztabar, 2017), little research considers the effects of delisting on what Nissenbaum (2004: 137) calls the "norms of information flow" in the library. Because the RTBF and delisting have the potential to disrupt information access in the library, librarians should engage with the issues now to prepare for possible shifts in information policies and laws around the world. Potential issues for librarians to consider discussed further below include how the RTBF disrupts information flow in the library and whether helping a patron delist her personal information online falls within the context of privacy in the library, which traditionally pertains to patron records and reading behavior.

The RTBF and delisting are international issues that require an international conversation. This paper frames the legal and ethical issues associated with the RTBF and delisting and initiates a conversation about their potential future disruption of librarian ethics and the provision of library services. The following sections introduce the RTBF phenomenon, parse the differing privacy and free speech laws in the EU and US, and highlight examples of recent international RTBF cases.

The right to be forgotten phenomenon

Understanding the legal and ethical issues related to the RTBF and delisting has important implications not just for individuals, lawmakers, and search engine operators, but for librarians the world over. This section presents some general information on the RTBF phenomenon, including the CJEU's decision in *Google Spain v. Costeja* and the different reactions to the RTBF and delisting in the EU and the US.

Privacy and forgetting in the European Union

In the EU, the RTBF is based on personal privacy and agency over personal information flows (Castellano, 2012: 6; Rosen, 2012: 88). The very terminology for the RTBF comes from the French legal concept of *le droit à l'oubli*, or "right of oblivion" (Rosen, 2012: 88). Thus, being forgotten is a fundamental part of the longstanding norms of EU information law and policy. Indeed, the RTBF is in line with theories of forgetting as necessary to move forward and survive in modern society (see, for example, Augé, 2004).

1995 Data Protection Directive. At the time of the European Commission's 2012 Data Protection Regulation, discussed below, the lynchpin of existing EU legislation on personal data protection was Directive 95/46/EC3 (1995 Data Protection Directive) (European Parliament, 1995). The 1995 Data Protection Directive has two goals: (1) to uphold the fundamental right to personal data protection, and (2) to guarantee the free flow of personal data between EU member states (European Parliament, 1995: 1). Additionally, Council Framework Decision 2008/977/JHA protects personal data for the purposes of police and judicial cooperation in criminal matters (European Council, 2008). These goals attempt to balance individual privacy protection with the free flow of information.

While the 1995 Data Protection Directive provides "basic regulation of the protection of personal data" (Chelaru and Chelaru, 2013: 4), it does not provide an explicit RTBF. Some privacy law scholars, however, interpret parts of the data protection framework as a diluted version of forgetting and the RTBF (Ambrose and Ausloos, 2013: 6–7). For example, Article 12, Right of Access, covers a data subject's right to access her data and creates legal protection for personal data online (European Parliament, 1995: Article 12; Mantelero, 2013: 6). In particular, Article 12(b)

declares that each data subject has the right to "the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data" (European Parliament, 1995: Article 12(b); European Commission, 2014: p. 2).

2012 Data Protection Regulation. As the Explanatory Memorandum of the 2012 Data Protection Regulation states, "Rapid technological developments have brought new challenges for the protection of personal data" (European Commission, 2012: 1). The Internet and the social web have created a new digital world where users share their lives – and their data: "Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life" (European Commission, 2012: 1). The 2012 Data Protection Regulation thus recommends a new legal framework, proposing a regulation to protect the processing and free movement of individual personal data and a directive to protect the processing and free movement of individual personal data by legal authorities (Ambrose and Ausloos, 2013: 11; European Commission, 2012: 1).

In particular, Article 17 provides an explicit RTBF and references the "erasure" in Article 12(b) of the 1995 Data Protection Directive. Under Article 17, a data subject may request a "controller" (e.g. a search engine operator) to delist her personal information, transforming public information into private information (Jones, 2013: 371). Additionally, the controller must then inform third parties of the data subject's request to erase any links to or copies of the data, subject to certain limitations (European Commission, 2012: Article 17(a)-(d)).

Delisting removes personal information from online search results and prevents the future accessibility of that information via search engine searches. It is worth noting that *delisting* information from search results is not the same as permanently *deleting* this information from the Internet altogether (see Ash, 2016: 307; Edwards, 2017: 13). As Chelaru and Chelaru (2013: 7) note, Article 17's "remarkable novelty" comes from its placement of the burden of proof on the *controller* to show the necessity of keeping the information in search results, not on the *data subject* to show the necessity of delisting. This provision ensures that a data subject has the right to delisting; as a result, delisting has become a popular legal mechanism in the EU for protecting personal information in the name of privacy.

The RTBF case and the "man who wished to be forgotten"

Ultimately decided in 2014 by the CJEU, the seminal RTBF case to date is *Google Spain v. Costeja*. The plaintiff, a Spanish citizen, filed complaints with the Spanish data protection agency against *La Vanguardia*, a Spanish newspaper, and Google Spain and Google, Inc. when a link to the 1998 auction notice for his foreclosed home appeared in Google search results for his name (Ash, 2016: 307). Because the debt and foreclosure proceedings were resolved years ago, Costeja argued that listing the notice in search results was irrelevant and infringed his privacy rights (European Commission, 2014: 1) – even though the auction notice is part of the public record.

The issues before the CJEU were the:

- **Applicability of law**, or whether the 1995 Data Protection Directive applies to search engine operators like Google;
- **Territoriality of law**, or whether the 1995 Data Protection Directive, a European law, applies to Google Spain and Google even though the data processing server was in the United States; and
- **Right to be forgotten**, or whether individuals have the right to request the removal of links to their personal information from search engine results (European Commission, 2014: 1).

In its groundbreaking ruling in favor of the RTBF (Stupariu, 2015: 1, 37–44), the CJEU cited the two notable objectives of the 1995 Data Protection Directive: "protecting the fundamental rights and freedoms of natural persons (in particular the *right to privacy*) when personal information is processed, while removing obstacles to the *free flow of such data*" (CJEU, 2014: 1, emphasis added). In its balance of the right of personal privacy with information flow, the court ruled in favor of Costeja, holding that regarding the:

- **Applicability of law**, the 1995 Data Protection Directive applies to search engine operators (here, Google) as "controllers of personal data";
- **Territoriality of law**, the 1995 Data Protection Directive applies to search engine operators (here, Google) with subsidiaries operating in an EU member state (here, Google Spain), even though it may process data outside of Europe; and
- **Right to be forgotten**, individuals have the right, *subject to limitations*, to request the

> removal of links to their personal information from search engine results (European Commission, 2014: 1-2).

Thus, Google was required to comply with the 1995 Data Protection Directive, establishing the precedent that a search engine operator is responsible for processing personal information that appears on third-party websites and that a data subject may ask the operator to delist said information from search results for her name (CJEU, 2014: 1).

The ruling created what Peter Fleischer (2015), Global Privacy Counsel for Google, calls a "right to delist", or the right to have certain information removed from Internet search results. EU citizens may ask search engine operators to delist information that is "inaccurate, inadequate, or irrelevant or no longer relevant, or excessive" (CJEU, 2014: Para. 94; European Commission, 2014: 5). The CJEU took care to note that delisting is not an absolute right; requests are handled on a case-by-case basis, and:

> the right to get your data erased is not absolute and has clear limits . . . It only applies when personal data storage is no longer necessary or is irrelevant for the original purposes of the processing for which the data was collected. (European Commission, 2014: 4)

Thus, search engine operators handle delisting requests from EU citizens on a case-by-case basis.

As noted above, to *delist* information from search results does not permanently *delete* it from the Internet (see Ash, 2016: 307; Edwards, 2017: 13). According to the Advisory Council to Google on the Right to Be Forgotten:

> Once delisted, the information is still available at the source site, but its accessibility to the general public is reduced because search queries against the data subject's name will not return a link to the course publication . . . *only the link to the information has been removed, not the information itself*. (Floridi et al., 2015: 4, emphasis added)

The Advisory Council to Google also suggests criteria by which the search engine operator should evaluate delisting requests (e.g. the data subject's role in public life; the nature, source, and timing of the information) (Floridi et al., 2015: 7–14) and advises on implementing delisting procedures (Floridi et al., 2015: 15–20).

On its very first day of court-ordered compliance with the 1995 Data Protection Directive in 2014, Google received 12,000 delisting requests (EuropeNews.net, 2014). By the following summer of 2015, it had received over 300,000 requests and delisted 40% of the 1.1 million web addresses evaluated (Ash, 2016: 308). And as of January 2017, Google had received over 670,000 requests and delisted 43% of the 1.8 million web addresses evaluated (Edwards, 2017: 13). Ironically enough, "In trying to restore his privacy, [Costeja] made himself not merely a public figure but a historic one. He would forever be remembered as the man who wished to be forgotten" (Ash, 2016: 308). The man who wanted to protect his privacy via delisting his personal information became the very poster child for forgetting.

2015 reform of EU data protection rules

The European Commission prioritized the RTBF when it began reforming EU data protection laws in 2012 (Jones, 2013: 371). As Viviane Reding (2012), then the European Commission's Vice President, declared: "If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system".

In December 2015, the European Parliament, Council, and Commission agreed on new data protection rules that created a "modern and harmonised data protection framework across the EU" (European Commission, 2015; Edwards, 2017). The goals to "make Europe fit for the digital age" and to generate a digital single market (European Commission, 2015) resulted in:

- **Regulation (EU) 2016/679**, which repeals the 1995 Data Protection Directive and focuses on personal data processing and the "free movement" of such personal data (European Commission, 2015). Regulation 679 was approved on May 24, 2016, and will become effective on May 25, 2018 (European Commission, 2016a; European Commission, 2015); and
- **Directive (EU) 2016/680**, which repeals Council Framework Decision 2008/977/JHA, mentioned above, and focuses on personal data processing by police and judicial cooperation in criminal matters. Directive 680 was approved on May 5, 2016, and EU member states must adopt it into their national laws by May 6, 2018 (European Commission, 2016b; European Commission, 2015).

Criticism of delisting in the United States

Because the *Google Spain v. Costeja* decision created a legal RTBF in the European Union, a new kind of content regulation in addition to, for example, Internet

filtering exists on the Internet that removes information from search engine results. Now a data subject who is an EU citizen may request that a search engine operator delist certain personal information about her from Internet search results for her name. The legal removal of content from the Internet via delisting in certain jurisdictions around the world could create a new online information ecosystem, one where some information may not be accessible (Jones, 2013, 2016). Delisting also disrupts the norms of information law and policy in the United States, including traditional conceptions of the rights to free speech and privacy.

Right to free speech in the United States

The First Amendment of the US Constitution states that "Congress shall make no law . . . abridging the freedom of speech . . . ." Critics view the RTBF and delisting as "rewriting history" at best and "censorship," or the removal or blockage of access to certain information and infringes free speech and free expression, at worst (Jones, 2013: 371).

Other scholars argue that delisting undermines the constitutional right to free speech (Rosen, 2012) and dilutes the quality of the Internet (Mayes, 2011). Due to the challenge of defining the RTBF's exact meaning, scope, and applicability (Richards, 2015: 90), some critics also contend that only personal information put online by the data subject herself qualifies for delisting (Walker, 2012).

Right to privacy in the United States

As with free speech, the RTBF and delisting can also conflict with US views of the right to privacy (Mayes, 2014). While the EU laws discussed above protect personal information, the US Constitution does not explicitly protect privacy, though many state constitutions do so (Ambrose and Ausloos, 2013: 8). Rather, privacy is an "evolving concept" in the United States (Jones, 2013: 374), and there is no "coherent, homogenous federal legal system of data and privacy protection . . . U.S. privacy protection is scattered and spread across a variety of state and federal laws that typically apply to specific groups of people" (Stupariu, 2015: 52). Consequently, many US critics of the RTBF do not view delisting as part of the right to privacy (Bennett, 2012; Bolton, 2014; Rosen, 2012). When viewed alongside US information law and policy norms, the RTBF is thus not what former European Commission Vice President Viviane Reding (2012) called a "modest expansion of existing data privacy rights", but as a "sweeping new privacy right" that is "the biggest threat to free speech on the Internet in the coming decade" (Rosen, 2012: 88).

Cross-border application of delisting

Based on the different norms of privacy and free speech in the European Union and United States, "Europeans and Americans have diametrically opposed approaches to the [RTBF] problem" (Rosen, 2012: 88). Some believe that the RTBF may exist in Europe, but not in the United States. For example, a recent report of the Advisory Council to Google on the RTBF indicated that the right should only apply within *European* jurisdictions (Floridi et al., 2015: 19–20). Limiting the RTBF to EU jurisdictions, however, does not solve the problems of delisting. The digital world, and the personal information shared, collected, and disseminated online, transcends the physical borders of countries and continents.

To truly protect privacy, information scholars urge international law- and policymakers to reach a unified understanding of the RTBF and its cross-border application and implementation (see, for example, Ausloos, 2012: 151; Bennett, 2012: 192–193; Richards, 2015: 90–92). The RTBF and delisting are international issues without borders or boundaries, appearing in the news of countries such as Canada (Alba, 2017; Blanchfield, 2016), Indonesia (Halim, 2016), and Ireland (Carolan, 2017), among others, and in the courts. The following provides a sample of countries with recent judicial decisions on the RTBF.

France

French law and policy treats privacy as a matter of dignity and human rights. As mentioned above, the RTBF terminology comes from the *droit à l'oubli*, the French legal concept of the "right of oblivion" (Rosen, 2012: 88). The Commission nationale de l'informatique et des libertés (CNIL), the regulatory body overseeing the enforcement of data privacy laws, received many delisting requests in the wake of the *Google Spain v. Costeja* decision in 2014. To manage these requests, a 2015 CNIL order requires Google to delist a data subject's personal information across *all* of its domain names (e.g. .fr, .uk, .com) (CNIL, 2015). A press release stated that, "In accordance with the CJEU judgement, the CNIL considers that in order to be effective, delisting must be carried out on all extensions of the search engine and that the service provided by Google search constitutes a single processing" (CNIL, 2015).

Outcry erupted from free speech traditionalists, among them Peter Fleischer, Global Privacy Council for Google, who argues for a European but not a

global RTBF: "We believe that no one country should have the authority to control what content someone in a second country can access" (Fleischer, 2015). The case between the CNIL and Google is currently pending before the European Court of Justice, one of the three courts that comprises the CJEU, as Case C-507/17 (ECJ, n.d.; Hern, 2017). The implications of a high court order limiting the RTBF to EU jurisdictions remain to be seen.

Japan

In contrast with the EU view of privacy in *Google Spain v. Costeja* and the French CNIL order, Japan's Supreme Court rejected a data subject's request that Google delist the search results for his 2011 arrest for child prostitution and pornography (Heisei, 2017; Umeda, 2017). Though the lower court had recognized the data subject's rights to privacy and to be forgotten, and ordered Google to delist these search results (Kyodo, 2016), the Tokyo High Court reversed the ruling and the Supreme Court affirmed it on the basis that the RTBF was not yet a ripe (i.e. timely) issue to adjudicate alongside the right of personal privacy (Umeda, 2017).

Brazil

Like the high court in Japan, Brazil's Superior Court of Justice (STJ) ruled unanimously against the imposition of the RTBF on Google and other search engine operators due to concerns over search engine authority, censorship, and information access (Sganzerla, 2016; STJ, 2016). According to a report on the ruling, "forcing search engines to adjudicate removal requests and remove certain links from search results would give too much responsibility to search engines, effectively making them into *digital censors*" (Sganzerla, 2016, emphasis added). An appeal is pending in Brazil's Supreme Court (Sganzerla, 2016).

India

Unlike the courts in Japan and Brazil, the Karnataka High Court in India approved and applied the RTBF to the case of a young woman seeking to delist search results for a prior marriage annulment to protect her privacy and reputation (Bhattacharya, 2017). Seeking harmony with western privacy law and acknowledging the need for sensitivity to women, the Court found that its ruling is: "in line with the trend in Western countries of 'right to be forgotten' in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned" (Bhattacharya, 2017). That the Karnataka High Court looked to the West for guidance on how to interpret the RTBF and privacy indicates a possible growing global consensus to prioritize the protection of privacy over the provision of information access.

Delisting disrupts the norms of information flow and librarian ethics

The interplay between information access and delisting disrupts not just international law and policy, but librarian ethics as well. Traditionally, libraries are the cornerstone of intellectual freedom and information access (ALA Council, 1996, 2008, 2014; IFLA, 1999) and librarians have a professional imperative to protect patrons' rights to privacy and to receive information in the library (Givens, 2014). The RTBF and delisting, however, alter the norms of information flow in libraries and create the potential for a new online information ecosystem, one where some information may not always be accessible (Jones, 2013, 2016).

Before considering some of the unintended consequences of delisting for patron privacy and information access in the library, the next section provides a brief overview of librarian ethics. Due to considerations of space, it focuses on the ethical standards of the American Library Association (ALA) and International Federation of Library Associations (IFLA).

US approaches to privacy and ethics in the library

While librarians typically must balance ethical principles with legal obligations, a potentially disruptive new legal regime like the RTBF and delisting could disrupt the ethical foundations of librarianship. To address privacy issues in US libraries, a set of "librarian ethics" that exist alongside librarians' legal obligations emerged from documents and ethical frameworks that the ALA has refined and codified over time (Magi and Garnar, 2015). This section first introduces the concept of contextual integrity before highlighting some of the ALA's official statements on privacy and ethics.

Contextual integrity and information flow in the library. As guardians of privacy and free speech, librarians preserve what Nissenbaum (2004,2009) calls contextual integrity of patron privacy while providing information access. "Contextual integrity" refers to the sharing of personal information in different spaces, or *contexts*, that have their own norms and expectations, from the home to the workplace to the library: "Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which

governs its various aspects such as roles, expectations, actions, and practices" (Nissenbaum, 2004: 137). According to Zimmer (2013: 45), "the context of the library brings with it specific norms of information flow that protect patron privacy". Librarians traditionally manage information flows in the library context by providing information access and by protecting patron privacy (for example, patron reader records are private and patron PII is confidential). Based on this understanding of privacy in the library, librarians must safeguard patron information in library records, but are not responsible for privacy outside of the library context.

Code of Ethics. Initially adopted in 1939, the ALA's *Code of Ethics* establishes general policies to guide ethical decision making in libraries, focused on the principle that, "We have a special obligation to ensure the free flow of information and ideas to present and future generations" (ALA Council, 2008). Indeed, "ensuring free and unfettered information access is a cornerstone of the librarian profession and the ALA's Code of Ethics. Librarians have a rich history of protecting patron privacy . . . " (Zimmer, 2013: 51). Considering the RTBF and delisting under this ethical framework, how can librarians "ensure the free flow of information and ideas" while respecting patrons who no longer want certain personal information to be searchable online?

Library Bill of Rights. The ALA also adopted the *Library Bill of Rights* in 1939, creating a formal policy statement on intellectual freedom that entitles everyone to free thought and expression and to the free access of library materials (ALA Council, 1996; Magi and Garnar, 2015). In particular, Article III states that, "Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment" and Article IV states that, "Libraries should cooperate with all persons and groups concerned with resisting abridgment of free expression and free access to ideas" (ALA Council, 1996: Articles III and IV). The RTBF creates a problem for librarian ethics: Is delisting censorship (the removal or blockage of access) of information? Does it prevent librarians from "resisting abridgment of free expression and free access to ideas"?

2014 Interpretation of the Library Bill of Rights. Despite the ALA's longstanding commitment to librarian ethics, patron privacy is perennially challenged, such as through government attempts to gain access to patron records via the USA PATRIOT Act (Foerstel, 2004). More recently, the ALA issued *Privacy: An Interpretation of the Library Bill of Rights*, which notably affirms that, "Everyone . . . who provides governance, administration or service in libraries has a responsibility to maintain an environment respectful and protective of the privacy of all users" (ALA Council, 2014). In a world that delists, how do librarians protect privacy? Are they responsible just for patron information in library records, or for any personal information pertaining to that individual?

ALA statement on the RTBF. At the time of this writing, the ALA has not issued a formal statement on the RBTF (Freeman, 2016). The issue, however, has been discussed and debated at formal ALA meetings (see, for example, Carlton, 2016).

IFLA approaches to privacy and ethics in the library

IFLA also promotes librarian ethics through a set of documents and frameworks that address privacy and information access (IFLA, 1999, 2015, 2016b).

1999 Statement on Libraries and Intellectual Freedom. Prepared by the Freedom of Access to Information and Freedom of Expression (FAIFE) Committee and approved by IFLA's Executive Board in 1999, the *Statement on Libraries and Intellectual Freedom* (1999 Statement) states that IFLA "defends and promotes intellectual freedom as defined in the United Nations Universal Declaration of Human Rights" and "asserts that a commitment to intellectual freedom is a core responsibility for the library and information profession" (IFLA, 1999). IFLA finds that privacy is an essential component of intellectual freedom. As such, libraries and library staff must ethically "adhere to the principles of intellectual freedom, uninhibited information access and freedom of expression and to recognize the privacy of library use" (IFLA, 1999). But the RTBF creates a conundrum for the "uninhibited information access and freedom of expression" and "privacy of library use": Is delisting the censorship of information?

The 1999 Statement's list of 11 intellectual freedom principles includes the affirmation that, "Library users shall have the right to personal privacy and anonymity. Librarians and other library staff shall not disclose the identity of users or the materials they use to a third party" (IFLA, 1999). But in a world that delists, how do librarians protect privacy? Based on the 1999 Statement, it seems that librarians are ethically required to protect only a patron's privacy in the library as it pertains to her identity or materials used.

2015 Statement on Privacy in the Library. Prepared by the FAIFE Committee and approved by the Governing Board, IFLA's recent *Statement on Privacy in the Library* (2015 Statement) notes that Article 12 of the United Nations' *Universal Declaration of Human Rights* defines privacy as human right: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation" (ILFA, 2015: 1, quoting *Universal Declaration on Human Rights*). It also cites IFLA's *Code of Ethics*, which "identifies respect for personal privacy, protection of personal data, and confidentiality in the relationship between the user and library or information service as core principles" (IFLA, 2015: 1, quoting *IFLA Code of Ethics for Librarians and Other Information Workers*).

Considering the human rights element of personal privacy and the ethical obligation of librarians to protect patrons' privacy again raises the challenge of delisting. The norms of information flow in the library context protect privacy from unwanted infringement by third parties, which librarians can achieve by "decid[ing] what kind of personal data they will collect on users and consider[ing] principles of data security, management, storage, sharing and retention" (IFLA, 2015: 2). But the 2015 Statement also recommends that: "Data protection and privacy protection should be included as a part of the media and information literacy training for library and information service users. This should include training on *tools to use to protect their privacy*" (IFLA, 2015: 2, emphasis added).

The call for better information literacy training for library patrons seems to extend beyond traditional library protection of reader records and PII to "tools to protect their privacy." Does this training include using Google's delisting request tool, or just internal library tools? Does helping a patron access and complete a delisting request amount to sanctioning censorship that violates librarian ethics?

2016 Statement on the Right to Be Forgotten. Like the Statement on Privacy in the Library, IFLA's Statement on the Right to be Forgotten (2016 Statement) also cites the United Nation's Universal Declaration of Human Rights and IFLA's Code of Ethics in its discussion of concerns related to delisting, which include:

- **Integrity of and access to the historical record**. IFLA dedicates itself to protecting information access, including the preservation of the historical record. Notably, IFLA "sees information on the public Internet as published information that may have value for the public or for professional researchers and so should, in general, not be intentionally hidden, removed or destroyed" (IFLA, 2016b);
- **Free information access and free expression**. IFLA also dedicates itself to protecting the freedoms of expression and information access. The RTBF and delisting violate these ideals; for example, "[t]he ideal of freedom of access to information cannot be honoured where information is removed from availability or is destroyed . . . When links to information are removed, for many, this results in a loss of access to information" (IFLA, 2016b); and
- **Privacy of the individual**. IFLA dedicates itself to protecting personal privacy in libraries, which, "as upholders of the public good, are sensitive to concerns around personal privacy in the context of the Internet" (IFLA, 2016b). Regarding the RTBF and delisting, "The degree to which libraries and librarians will find a particular application of RTBF to be acceptable, in the context of the more general library concern for access to information, will depend upon the particular circumstances of the application" (IFLA, 2016b).

The 2016 Statement concludes by exhorting librarians to participate in policy discussions about the RTBF and a list of professional imperatives that preserve information access, such as opposing removal of links from the results of name searches of public figures and advocating transparent criteria and processes for search engines' RTBF determinations. But the list also suggests that librarians should: "Support individuals who request assistance in finding more information on the application of the right to be forgotten to their individual circumstances," indicating that at least under IFLA's interpretation of ethical norms and information flows in the library, librarians should educate patrons about the RTBF and delisting.

2013 and 2016 Trend Reports. In addition to the official statements described above, the IFLA Trend Report included the redefinition of the boundaries of data protection and privacy as one of five major factors that will influence the future of the international information ecosystem (IFLA, 2013). The 2016 update revisited the paramount importance of privacy, data protection, and information security (IFLA, 2016a). The update also specifically mentions the RTBF, noting that "unanticipated side effects of our online activities [leave] behind a permanently visible digital footprint" (IFLA, 2016a: 7).

Delisting considerations for librarians

As described above, librarians traditionally protect and defend patron privacy in the library context, but delisting may change the norms of information flows and privacy in the library. The RTBF's disruption of contextual integrity in the library may require a redefinition or expansion of patron privacy protection.

Though yet to receive extensive treatment in the LIS literature, the RTBF has not gone unnoticed by the domain's professional organizations, such as the ALA and IFLA, or its scholars. For example, Edwards (2017: 14) identifies the RTBF as a possible "conflict in the making" for the professional imperatives of librarianship like information access and preserving the historical record, echoing the ALA and IFLA statements discussed above. Because the RTBF and delisting can alter the norms of information flow and librarian ethics in the future, the following lists possible issues that librarians around the world should consider now in preparation.

- **Information flows**. How does the RTBF disrupt information flow in the library? Delisting revokes access to certain information in search engine results, implicating the rights to read and to receive information in libraries. But delisting also can protect the privacy of the data subject, which can include sensitive PII. Recall that delisting is not the same as permanently deleting information from the Internet.
- **Personal information**. Does it matter whether the personal information that the patron wants to delist is public and factual, such as the mortgage foreclosure in *Google Spain v. Costeja*, or is sensitive and embarrassing, such as revenge pornography? What if the patron seeks to delist PII?
- **Intellectual freedom**. Does helping a patron delist information online protect that patron's privacy and maintain confidentiality, or does it undermine free speech and unfettered information access?
- **Patron privacy**. Does helping a patron delist her personal information online fall within the context of privacy in the library, which traditionally pertains to patron records and reading behavior?
- **Delisting requests**. Delisting can alter the norms of information flow in the context of the library by removing certain information online from availability and accessibility. What if patron asks a librarian for help with a delisting request? Can the librarian refuse to help a patron locate a delisting request form or to fill it in? Or is the librarian now obliged to help protect this patron's privacy? Based on IFLA's *Statement on the Right to be Forgotten* (IFLA, 2016b), it appears that librarians are ethically bound to educate patrons about the RTBF tools available to them.

Conclusion and future research

The relationship between privacy, free speech, and delisting is critical for the future of librarianship worldwide. This paper anticipates the RTBF and delisting's potential disruption of librarianship and seeks to initiate an international dialogue between librarians, scholars, and advocacy groups. Delisting, while legally applicable only in EU jurisdictions at the time of this writing, nevertheless implicates privacy and information access in libraries around the world. It might also create a new role for librarians, who must educate themselves and patrons about the RTBF and delisting and may create and implement new polices that reflect the evolving online information ecosystem.

Going forward, librarians should engage with RTBF and delisting issues now to prepare for possible future disruptions of information flow in the library and shifts in information policies and laws around the world. Some of the considerations for librarianship are the possible effects of delisting on patron privacy and free speech in the library and the possible new responsibilities of the librarian in a new online information environment. Future research is needed on the potential of delisting and the RTBF to disrupt librarian ethics and the provision of library services. Possible projects include cross-cultural studies of librarianship norms and practices around the world and formulation to formulate best practices to guide the management of delisting in the library.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Alba D (2017) The world may be headed for a fragmented 'splinternet'. *Wired*, 7 July. Available at: https://www.wired.com/story/splinternet-global-court-rulings-google-facebook/ (accessed 2 February 2018).

ALA (American Library Association) Council (1996) Library Bill of Rights. ALA.org. Available at: http://www.ala.org/advocacy/intfreedom/librarybill (accessed 2 February 2018).

ALA (American Library Association) Council (2008) Code of Ethics. ALA.org. Available at: http://www.ala.org/tools/ethics (accessed 2 February 2018).

ALA (American Library Association) Council (2014) Privacy: An Interpretation of the Library Bill of Rights. ALA.org. Available at: http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy (accessed 2 February 2018).

ALA (American Library Association) Council (2015) Privacy: An Interpretation of the Library Bill of Rights. ALA.org. Available at: http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/internet-filtering (accessed 2 February 2018).

Ambrose M L and Ausloos J (2013) The right to be forgotten across the Pond. *Journal of Information Policy* 3: 1–23.

Ash T G (2016) *Free Speech: Ten Principles for a Connected World*. New Haven, CT: Yale University Press.

Augé M (2004) *Oblivion*. Trans. de Jager. M. Minneapolis, MN: University of Minnesota Press.

Ausloos J (2012) The 'right to be forgotten' – worth remembering? *Computer Law & Security Review* 28(2): 143–152.

Bennett SC (2012) Right to be forgotten: Reconciling EU and US perspectives. *Berkeley Journal of International Law* 30(1): 161–195.

Bhattacharya A (2017) In a first, an Indian court upholds the 'right to be forgotten'. *Livelaw*. Available at: http://www.livelaw.in/first-indian-court-upholds-right-forgotten-read-order/ (accessed 2 February 2018).

Blanchfield M (2016) Google, B.C. firm duel over free speech, copyright in Supreme Court battle. *Toronto Star*, 6 December. Available at: https://www.thestar.com/business/2016/12/06/google-bc-firm-duel-over-free-speech-copyright-in-supreme-court-battle.html (accessed 2 February 2018).

Bolton R (2014) The right to be forgotten: Forced amnesia in a technological age. *John Marshall Journal of Information Technology and Privacy Law* 31(2): 133–144.

Carolan M (2017) Google argues 'right to be forgotten' ruling is unworkable. *Irish Times*, 18 May. Available at: https://www.irishtimes.com/news/crime-and-law/courts/high-court/google-argues-right-to-be-forgotten-ruling-is-unworkable-1.3088145?mode=amp&ref=yfp (accessed 2 February 2018).

Carlton A (2016) Should there be a right to be forgotten? Librarians debate EU privacy laws at Midwinter. *American Libraries Magazine*. Available at: https://americanlibrariesmagazine.org/blogs/the-scoop/should-there-be-a-right-to-be-forgotten/ (accessed 2 February 2018).

Castellano PS (2012) The right to be forgotten under European law: A constitutional debate. *Lex Electronica* 16(1): 1–30.

Chelaru E and Chelaru M (2013) Right to be forgotten. *Annales Universitatis Apulensis – Series Juriprudentia* 16: 1–8.

Citron D and Franks M A (2014) Criminalizing revenge porn. *Wake Forest Law Review* 49(2): 345–392.

CNIL (Commission Nationale de l'informatique et des libertés) (2015) CNIL orders Google to apply delisting on all domain names of the search engine. *CNIL News*, 12 June. Available at: http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/ (accessed 2 February 2018).

CJEU (Court of Justice of the European Union) (2014) Press Release No. 70/14, Judgment in Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (Luxembourg). *Curia*. Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (accessed 2 February 2018).

CJEU (Court of Justice of the European Union) (n.d.) General presentation. *Curia*. Available at: https://curia.europa.eu/jcms/jcms/Jo2_6999/ (accessed 2 February 2018).

Edwards E (2017) Libraries and the right to be forgotten: A conflict in the making? *Journal of Intellectual Freedom and Privacy* 2(1): 13–14.

European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *European Parliament*. Available at: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf (accessed 2 February 2018).

European Commission (2014) Fact sheet on the 'right to be forgotten' ruling (C 131/12). *Europa.eu*. Available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (accessed 2 February 2018).

European Commission (2015) Press release: Agreement on Commission's EU data protection reform will boost Digital Single Market. *Europa.eu*, 15 December. Available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm (accessed 2 February 2018).

European Commission (2016a) Regulation of the European Parliament and of the Council of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Regulation (EU) 2016/679. *EurLex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC (accessed 2 February 2018).

European Commission (2016b) Directive of the European Parliament and of the Council of on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Directive (EU) 2016/680. *EurLex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC (accessed 2 February 2018).

European Council (2008) Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. *Official Journal of the European Union*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977 (accessed 2 February 2018).

ECHR (European Court of Human Rights) (n.d.) The court in brief. *European Court of Human Rights*. Available at: http://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf (accessed 2 February 2018).

ECJ (European Court of Justice) (n.d.) *Google*, Case C-507/17. *Curia*. Available at http://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17 (accessed 2 February 2018).

European Parliament (1995) Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *EurLex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (accessed 2 February 2018).

EuropeNews.net (2014) Removal of Google personal information could become work intensive. *EuropeNews.net*, 1 June. Available at: http://www.europenews.net/index.php/sid/222490797 (accessed 2 February 2018).

Fleischer P (2011) Foggy thinking about the right to oblivion. In: *Privacy . . . ?* Available at: http://peterfleischer .blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html (accessed 2 February 2018).

Fleischer P (2015) Implementing a European, not global, right to be forgotten. In: *Google Europe Blog*. Available at:http://googlepolicyeurope .blogspot.com/2015/07/implementing-european-not-global-right.html (accessed 2 February 2018).

Floridi L et al. (2015) The advisory council to Google on the right to be forgotten. Google Advisory Council, 6 February. Available at: http://www.cil.cnrs.fr/CIL/IMG/pdf/droit_oubli_google.pdf (accessed 2 February 2018).

Foerstel H (2004) *Refuge of a Scoundrel: The Patriot Act in Libraries*. Westport, CT: Libraries Unlimited.

Freeman M (2016) Google embraces version of right to be forgotten. In: Intellectual Freedom Blog, 18 March. Available at: http://www.oif.ala.org/oif/?p=6258 (accessed 2 February 2018).

Givens C (2014) *Information Privacy Fundamentals for Librarians and Information Professionals*. New York: Rowman and Littlefield.

Google Spain [*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C 131/12] (2014, 13 May) (Spain). Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doc&mode=lst&dir=&occ=first&part=1&cid=133613 (accessed 2 February 2018).

Halim H (2016) Press exempt from right to be forgotten. *The Jakarta Post*, 6 December. Available at: http://www.thejakartapost.com/news/2016/12/06/press-exempt-right-be-forgotten.html (accessed 2 February 2018).

Heisei 28 (Kyo) 45 (2017) *Courts in Japan*. Available at: http://www.courts.go.jp/app/hanrei_jp/detail2?id=86482 (accessed 2 February 2018).

Hern A (2017) ECJ to rule on whether 'right to be forgotten' can stretch beyond EU. *The Guardian*, 20 July. Available at: https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (1999) Statement on libraries and intellectual freedom. IFLA.org. Available at: https://www.ifla.org/publications/ifla-statement-on-libraries-and-intellectual-freedom (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (2013) IFLA trend report. IFLA.org. Available at: http://trends.ifla.org/http:// (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (2015) Statement on privacy in the library environment. IFLA.org. Available at: https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (2016a) IFLA trend report 2016 update. IFLA.org. Available at: https://trends.ifla.org/files/trends/assets/trend-report-2016-update.pdf (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (2016b) Statement on the right to be forgotten. IFLA.org. Available at: https://www.ifla.org/node/10272 (accessed 2 February 2018).

Jamali HR and Shahbaztabar P (2017) The effects of Internet filtering on users' information-seeking behaviour and emotions. *Aslib Journal of Information Management* 69(4): 408–425.

Jones ML (2013) It's about time: Privacy, information life cycles, and the right to be forgotten. *Stanford Technology Law Review* 16(2): 369–422.

Jones ML (2016) *Ctrl + Z: The Right to Be Forgotten*. New York: NYU Press.

Koops B-J (2011) Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten' in big data practice. *SCRIPTed* 8(3): 229–256.

Kyodo (2016) Japanese court recognizes 'right to be forgotten' in suit against Google. *Japan Times*, 27 February. Available at: http://www.japantimes.co.jp/news/2016/02/27/national/crime-legal/japanese-court-recog

nizes-right-to-be-forgotten-in-suit-against-google/#.WOVE99IrI2w (accessed 2 February 2018).

Laird L (2013) Victims are taking on websites for posting photos they didn't consent to. *ABA Journal* 99: 44–50.

Magi T and Garnar M (eds) (2015) *Intellectual Freedom Manual*. 9th edn. Chicago, IL: American Library Association.

Mantelero A (2013) The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Computer Law and Security Review* 29(3): 229–235.

Mayes T (2011) We have no right to be forgotten online. *The Guardian*, 21 May. Available at: https://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet (accessed 2 February 2018).

Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79(1): 119–157. Available at: https://www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf (accessed 2 February 2018).

Nissenbaum H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Reding V (2012) EU data protection reform 2012: Making Europe the standard setter for modern data protection rules in the digital age. Speech given at: *Innovation conference digital, life, design*, Munich, Germany, 22 January. Available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (accessed 2 February 2018).

Richards N (2015) *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. New York: Oxford University Press.

Rosen J (2012) The right to be forgotten. *Stanford Law Journal Online* 64(1): 88–92.

Sganzerla T (2017) Brazil superior court rules in Google's favor, against 'right to be forgotten'. *Global Voices*, 21 November. Available at: https://globalvoices.org/2016/11/21/brazil-superior-court-rules-in-googles-favor-against-right-to-be-forgotten/ (accessed 2 February 2018).

STJ (Brazil Superior Court of Justice) (2016) Request for right to forget cannot be directed to Google. *Migalhas*, 16 November. Available at: http://www.migalhas.com.br/Quentes/17, MI248798,51045-Pedido+de+direito+ao+esquecimento+nao+pode+ser+direcionado+ao+Google (accessed 2 February 2018).

Stupariu I (2015) *Defining the right to be forgotten: A comparative analysis between the EU and the US*. LLM Short Thesis, Central European University, Hungary. Available at: http://www.etd.ceu.hu/2015/stupariu_ioana.pdf (accessed 2 February 2018).

Tene O and Polonetsky J (2013) Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property* 11(5): 242–273.

Umeda S (2017) Japan: Google does not have to delete search results related to arrest. *Library of Congress Global Legal Monitor*. Available at: http://www.loc.gov/law/foreign-news/article/japan-google-does-not-have-to-delete-search-results-related-to-arrest/?loclr=eaglm (accessed 2 February 2018).

United States v. American Library Association, Inc., 539 US 194 (2003) Available at: http://caselaw.findlaw.com/us-supreme-court/539/194.html (accessed 2 February 2018).

Walker RK (2012) The right to be forgotten. *Hastings Law Journal* 64(1): 257–286.

Zimmer M (2013) Patron privacy in the '2.0' era: Avoiding the Faustian bargain of library 2.0. *Journal of Information Ethics* 22(1): 44–59.

Author biography

Katie Chamberlain Kritikos is a doctoral candidate at the School of Information Studies and research assistant at the Center for Information Policy Research at the University of Wisconsin-Milwaukee. She researches issues related to information law and policy including privacy, technology, and digital civil rights. Katie received her B.A. (2006) in English from the University of Alabama and J.D. (2009) and M.L.I.S. (2010) from the University of Illinois.

Article

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 195–202

DOI: 10.1177/0340035218773786
journals.sagepub.com/home/ifl

Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries

Monica G. Maceli
Pratt Institute, New York, USA

Abstract

Threats to our patrons' privacy have been a long-standing concern in libraries, though our responsibilities were largely bounded by the physical library space. Today, fueled by novel technologies, the landscape is vastly different, with patrons' privacy threatened by an ever-increasing number of entities. In this complexity, libraries have continued their commitment to privacy, with public libraries now seeking to educate patrons about privacy threats, protective measures, and tools that they might employ. This review of literature seeks to identify challenges to United States public libraries in educating and advocating for patron use of privacy-protection technology tools, drawing from research in a variety of allied fields, while suggesting future research directions. Issues identified include: substantial technology-related knowledge gaps in our patrons, librarians, and library staff; the need to support a vast number of technology tools and techniques; as well as building our understanding of the perspective of the tools' underlying creators.

Keywords

Librarian education, literature review, patron training, privacy-protection technologies, privacy threats, public libraries, United States

Submitted: 13 January 2018; Accepted: 26 March 2018.

Introduction

Libraries' commitment to patron privacy has been a core value of the field since its earliest days. Previous generations of librarians and library staff crafted policies and procedures to mask the information trail patrons left behind them within the physical library space, be it from browsing the Web on public access computers or from checking out materials. Today's public libraries have taken on a much greater challenge: that of advising and educating patrons as to how to protect their privacy within the vast online landscape. A common focus of such educational efforts is introducing patrons to privacy-protection technology tools and encouraging their use. These initiatives are becoming increasingly common within public libraries, as will be the focus of this work.

Privacy-protection technology tools consist of a variety of specialized software. These include: web browser plugins that thwart behavioral tracking and data collection, tools to protect the user's data in transit, e.g. virtual private networks (VPNs), or to obfuscate one's location (e.g. the Tor browser), and encrypting various data in storage, such as one's emails or multimedia. Table 1 summarizes some of the most common types of privacy-protection tools as well as their function (for further reading, see Maceli, 2018). Along with the necessary software is the needed knowledge and ability to effectively customize, configure, and wield such tools, as well as the technical literacy needed to avoid social engineering attacks.

In recent years, notable projects originating in public libraries have focused on educating our patrons on privacy-related tools and potential threats. Several large-scale projects in United States public libraries,

Corresponding author:
Monica G. Maceli, Pratt Institute School of Information, 144 West 14th St, 6th Floor, New York, NY, 10011, USA.
Email: mmaceli@pratt.edu

Table 1. Summary of popular privacy-protection technology tools.

Privacy-protection technology tool	Function	Example
Privacy-protecting web browser plug-ins	Thwart behavioral targeting and data collection during the user's web browsing session; block ad-delivery and potentially malicious scripts.	Privacy Badger (www.eff.org/privacybadger)
Incognito or private browsing mode	Protect against later users of the same local computer viewing your stored browsing data.	Private Browsing in Firefox (https://www.mozilla.org/)
Encryption	Protect data from snooping as it travels networks or when stored on computers.	Hypertext Transfer Protocol Secure (HTTPS) for encrypting web content; VeraCrypt (www.veracrypt.fr) utility for encrypting stored data
Virtual private networks (VPNs)	Provides encrypted protection while traversing an open wireless network or from ISPs snooping into one's traffic; change visible origination IP address.	OpenVPN (https://openvpn.net/)
Tor (The Onion Router)	Hide user's identity and obfuscate the destination and origin of traffic by routing their traffic through a series of computers running Tor, known as Tor relays.	Tor Project (https://www.torproject.org/)

currently supported by the Institute of Museum and Library Services (IMLS) and other influential library and information science organizations, seek to train librarians and library staff in this area, with the goal of reaching thousands of practitioners. These include: NYU's partnership with the Library Freedom Foundation (IMLS, 2017) and the City of New York's initiative to train library staff across the city (Marden, 2017), as well as less formal projects such as the growth in the number of libraries offering Tor to their users, sparked by the Kilton Public Library's efforts (Library Freedom Project, 2015). The coming years will reveal the impact of these (and future) projects, with an anticipated sharp increase in the number of librarians and public library staff that can confidently educate, train, and advise their patrons on privacy-protection technology.

Complementing the formal training opportunities in this area for librarians and library staff, numerous pragmatic guides to privacy threats, protective actions and relevant technology tools exist, both in the research literature (e.g. Fortier and Burkell, 2015) and in web-based resources (such as the Library Freedom Project's (2018) "Privacy toolkit for librarians"). The American Library Association (ALA) provides a wealth of privacy-related guidelines, checklists, and toolkits for library staff and librarians (ALA, 2014, 2016). However, such resources focus on mitigating privacy threats while fulfilling the need for "libraries to collect user data and provide personalized services" (ALA, 2016) within the context of the libraries' physical space and resource offerings, and less about guiding patrons in protecting their privacy in the context of their broader lives.

Public libraries are not the only organizations taking on the challenge of privacy-protection tool education, many human rights non-profits are active in this area as well. The highly influential Electronic Frontier Foundation (EFF) is a United States-based non-profit organization that tackles the numerous legal issues arising from the need to protect civil liberties in the digital era. The EFF maintains an extensive body of privacy-related literature and resources on their website and conducts activities ranging from litigating court cases, to developing novel software, such as privacy-protecting web browser plugins (Electronic Frontier Foundation, 2018). In fact, the aforementioned Library Freedom Project's "Privacy toolkit for librarians" includes several pointers to EFF resources. Many other non-profits educate user groups on privacy topics, including: Freedom of the Press Foundation which trains journalists and at-risk groups on digital privacy-protection, internationally, the Tactical Technology Collective and Front Line Defenders work to protect human rights advocates protect their privacy when using digital communication tools.

Public libraries have an advantage over the human rights groups working in this area, given that public libraries have an existing physical presence in many communities across the United States. Privacy-related work within public libraries therefore stands to

complement the efforts of other human rights organizations. Privacy and technology have been historically well studied within the field of library and information science; a great deal of previous work has explored our roles and responsibilities in providing technology services to our patrons in a privacy-sensitive fashion, be it public Internet access (such as Nijboer, 2004) or digital library resources (e.g. Sturges et al., 2003). However, though significant effort has been focused on librarian education around privacy-protection technology tools (e.g. Fortier and Burkell, 2015; Noh, 2014), relatively little work in the information science field has looked directly at the barriers and issues surrounding users' adoption and use of such tools. These challenges have the potential to lessen the impact of librarians' work in educating and encouraging patrons in using privacy-related technologies. Libraries have historically emphasized protecting their users' privacy at all costs, but this focus has been largely bounded by the physical library space, with less attention to broader protections as users browse the Web, use mobile devices or other common technology tools, across all aspects of their lives.

This research literature review seeks to explore the work of allied fields studying and designing privacy protection tools, such as computer science and security researchers, with the goal of identifying the potential challenges to patron adoption that our librarians and library staff may face in the future. To that end, this work explores the following questions through a review of existing literature:

- What challenges to the use and adoption of privacy-protection technology tools by public library patrons in the United States are suggested by research literature?
- What potential implications do these challenges have for public libraries' educational initiatives in this area?

The next section will provide a review of related research literature, which will then be contrasted against the stated research questions in the subsequent Discussion section.

Review of related research work

Research assessing the use, understanding, and impact of privacy-protection technology tools on end users has attracted attention from researchers in a variety of security and computing-related fields. To identify and collect such work for the purpose of this literature review, the author and a graduate assistant independently searched both library-specific publications with a technology focus (such as Library Hi Tech, Information Technology & Libraries, and Association for Information Science and Technology (ASIS&T) Annual Meeting Proceedings) and broader general-purpose computing digital libraries (such as the ACM Digital Library). A total of 52 papers were then assessed to identify the purpose and findings of the work, and to determine its relevance in the context of libraries. Though, as stated earlier, the main focus of this literature review was work within the United States, several international publications were included that had particular relevance.

Many studies revealed surprising or paradoxical findings that were very sensitive to contextual factors. Notable work exploring the public's baseline privacy concerns, the impact of their technical knowledge on their actions, and their general use of privacy-protection technology tools will be summarized next.

Baseline privacy concerns

Advising and training our patrons in the use of privacy-protection technology tools is a goal much easier to achieve if patrons have pre-existing concerns about their privacy in the digital world. Though one might assume widespread privacy concern in communities, given the many recent and dramatic privacy-related news stories (e.g. the Equifax hack, NSA spying), the reality of where and when those concerns are felt and acted upon is much more nuanced.

Many researchers have studied users' privacy concerns and their perceptions of control in this area. Efforts to understand the public's privacy concerns and categorize these accordingly have taken place for decades. Starting in the 1970s, Westin conducted a number of surveys (for example – privacy concerns on the growing "Net" (Freebies and Privacy: What Net Users Think, 1999), consumer privacy issues (Consumer Privacy and Survey Research, 2003) and many others) aiming at assessing and tracking privacy worries over time through construction of privacy indexes. Kumaraguru and Cranor (2005) provide a concise survey of Westin's corpus of findings, which notably include grouping of consumers into the categories of: privacy *fundamentalists* (who are greatly protective of their privacy), *pragmatics* (who weight the personal benefits of revealing their information), and the *unconcerned* (who are generally trusting of data-collecting organizations).

Over the many decades and many studies Westin conducted, the pragmatics consistently formed the largest percentage of those studied, ranging from 55% to 63% of respondents. Bergmann (2009), in a large-scale international survey to assess users'

privacy awareness based on exposure to a website's privacy policy, found privacy fundamentalists represented 34% of participants, pragmatists were 48%, and unconcerned users 18%. Though users may be easily categorized in interacting with a particular system or scenario, as in the Bergmann study, other research suggests that users' privacy concerns are highly context dependent and variable, with users fluctuating from extreme concern to apathy about privacy depending on contextual and environmental cues (Acquisti et al., 2015). On a more general level, the 2015 Pew Internet survey (Madden and Rainie, 2015) found that 93% of American adults feel it is important to control who can acquire information about them, and 90% of adults find controlling what information is collected about them to be important, so these are clearly widespread values.

Privacy-protection actions

Though the previous work indicates that the majority of the public is at least somewhat (or intermittently) concerned with their privacy, much smaller portions of the population are taking significant measures to protect their privacy in digital environments. Bashir et al. (2015) aptly term this the "privacy paradox", noting the incongruity between people's stated desire for privacy and their actions (or rather – their inactions). In 2015, American survey respondents reported a range of reasons they did not take privacy-protection actions including: the perceived difficulty it would entail, feeling they have nothing to hide, lacking the time and/or technical expertise, the fear of attracting greater scrutiny, and valuing the perceived safety afforded by surveillance (Rainie and Madden, 2015).

Research work emphasizes that those who do take privacy-protecting actions are in the minority, and their actions may be relatively ineffective (e.g. Aldhafferi et al., 2013; Daniel et al., 2014; Madden and Rainie, 2015; Wills and Zeljkovi, 2011). Wills and Zeljkovic (2011) found that simple website privacy measures, such as removing browser history, are done by less than 20% of users. Of users that take action to protect their privacy, the previously mentioned survey of American adults found that 59% cleared cookies, 34% disabled cookies, 15% reported using a search engine that does not track users' search history, 9% of participants added a privacy-enhancing browser plugin, and 9% used anonymizing technologies, e.g. Tor, VPN, proxy server (Madden and Rainie, 2015). One of the simplest means of controlling privacy on an application-by-application basis is changing the default privacy settings; a substantial body of privacy research in the context of social media sites estimates that very few users do so (e.g. Aldhafferi et al., 2013; Daniel et al., 2014), even in response to life changes such as entering the job market (Hargittai and Litt, 2013).

Furthermore, significant struggles were noted in those users that do attempt to take action to protection their privacy. Users that do modify their privacy settings often end up with incorrect settings that do not match their original sharing intentions (Madejski et al., 2012) or are confused by the interfaces and jargon presented (Leon et al., 2012). A 2016 study exploring digital literacy among African American young adult Internet users, found that a large percentage struggled with privacy and safety-related tasks and less than half could complete simple privacy-protection actions, such as adjusting the web browser's security settings or clearing cookies (Park and Jang, 2016). Trepte et al. (2015) suggest that a lack of "privacy literacy" prevents users from effectively taking action to assuage their privacy-related concerns.

Privacy-protecting technology tools

The use of privacy-protecting technology tools themselves also raises many troubling issues and questions. For participants that were studied while using privacy-protection tools, the impact of such technologies was often paradoxical. In exploring a variety of privacy-related browser plugins, Schaub et al. (2016) found that the use of such tools in fact *increased* users' privacy concerns, instead of allaying their fears. A notable emergent concern of participants was sharing information with the privacy tool itself, as their data was visibly processed and intercepted by such technologies.

Though privacy fears were increased, there was little impact noted on users' underlying understanding of what data might be collected and why. Privacy tools increase awareness of privacy-threatening techniques, such as third-party tracking; however, when using personalized logged-in sites, the users' privacy worries often increased and their trust in privacy tools decreased (Schaub, 2016). Additionally, findings indicate that simply becoming aware of a potential privacy issue does not increase the user's underlying comprehension of how such violations may occur (Bergmann, 2009; Schaub, 2016).

As noted earlier, contextual cues play a large role in the users' trust of the technology tool and the perceived information gathered. The users' expectations and the purpose of why sensitive resources are used have a major impact on users' subjective feelings and their trust decisions (Lin, 2012). Tools that offered

greater perceived control over the data collected or revealed to others were observed to make users more likely to disclose riskier sensitive information (Brandimarte et al., 2012). And the more confident users felt in their ability to manage their privacy with a particular tool or setting, then the less they would consider revealing personal information to be a privacy risk at all (Chen and Chen, 2015).

Technical knowledge and privacy choices

Many researchers have questioned the role of users' technical knowledge in the privacy choices and actions that they take, with the assumption that technological novices may behave quite differently than those with more expertise. Users' technical knowledge has been assessed through a variety of research means, including eliciting mental models of technical concepts, such as asking users to explain or sketch how the Internet (Kang et al., 2015) or home computer security works (Wash, 2010), and surveying users on their use and experience with technology tools and techniques (e.g. Kang et al., 2015). Here too, results are surprising and the "privacy paradox" (Bashir et al., 2015) is similarly evident.

Malandrino et al. (2013) found that users with greater levels of technology knowledge had a better understanding of privacy-related threats; however, all users generally expressed a concern for privacy but less effort to take any protective actions. Kang et al. (2015) found no clear relationship between users' technical background and knowledge, and their privacy-protection actions. Less technology-savvy users reported greater concerns about their privacy but were generally unwilling to modify settings, change their behaviors, or install privacy-protection technologies, particularly if there was a perceived personal benefit to revealing their information (Malandrino, 2013).

Discussion

Overall, the body of research in this area suggests a significant percentage of the public (which encompasses the public library patron base) are concerned with their privacy, but lack the motivation, knowledge, and digital literacy necessary to consistently and effectively act on these concerns. Privacy-protection technology tools are by no means a panacea, with prior research suggesting they may increase privacy concerns or be used ineffectively. And concern alone would appear to have little impact on users' underlying understanding of what data might be collected, why, and through what technical means (e.g. Bergmann, 2009; Schaub, 2016). The current trend in public libraries, towards providing privacy-related guidance for their patrons and communities, means that library staff and librarians will be directly impacted by the findings of the research reviewed here. The review of literature yields several issues of relevance to the first research question – What challenges to the use and adoption of privacy-protection technology tools by public library patrons in the United States are suggested by research literature? These challenges will be explored next, and presented in the context of the second research question –What potential implications do these challenges have for public libraries' educational initiatives in this area?

Bridging the (many) knowledge gaps

The findings highlighted above clearly illustrate numerous knowledge gaps preventing patrons (and likely library staff and librarians themselves) from effectively adopting, understanding, using, and explaining privacy-protection technologies. Bashir et al. (2015) describe several key knowledge gaps in users' understanding of Internet infrastructure and function, emphasizing a deep problem of information asymmetry (in this case between Internet service providers and their customers) making it difficult for the users to truly comprehend and give consent for their information's collection and use.

These knowledge gaps create serious problems woven throughout all aspects of protecting one's privacy in a digital world, from the initial step of giving consent, to deciding to use, and attempting to customize, privacy-protection tools. The lack of privacy literacy identified by Trepte et al. (2015) is a challenging issue and one that libraries are uniquely positioned to tackle. Wissinger (2017: 380) emphasizes the distinction between *privacy literacy* and *digital literacy*, with privacy literacy focused on the "understanding of the responsibilities and risks associated with sharing information online", while digital literacy focuses on "the task-based use of information in a digital environment." Framed in this way, privacy literacy becomes a deeply personal and challenging critical thinking activity (Wissinger, 2017: 380). Rotman (2009) presents a privacy literacy framework consisting of: *understanding* how personal information is used online, *recognizing* where information may be shared, *realizing* the consequences of sharing, *evaluating* the benefits or drawbacks to sharing online, and *deciding* when it is appropriate to share information. This framework illustrates the many dimensions that must be considered in managing one's information sharing in online environments.

The knowledge gaps preventing users from fully understanding the digital world's impact on their privacy and information are quite daunting, in particular the technological aspects facilitating the underlying ability of information to be shared, as it traverses networks, storage locations, and data collectors.

Nearly every day brings a novel privacy-threatening exploit to the news, requiring constant vigilance and shifting of protective techniques and tools over time. Though it may be relatively simple to advocate for and train users in the use of, say, a particular tracking-blocking browser extension, this clearly does not endow users with a deeper understanding of the function of such tools and the flexibility to apply this knowledge in future novel scenarios. A one-time workshop or infrequent training series is likely not enough to both instill deeper knowledge and encourage the addition of privacy-protection technology tools into one's daily life, particularly given the many reasons users cite for their privacy inactions.

Supporting the vast range of tools and techniques

The literature shows the extensive set of techniques, tools, and actions needed to fully protect one's privacy in today's digital environments. Actions such as reading a privacy policy or running the Tor browser require very different levels of technical knowledge and skill yet may be equally important in protecting one's privacy. The necessarily complementary nature of tools and techniques creates many barriers to use, namely in requiring the users' time and effort to customize the tools to fit their individual needs, as well as the related time and effort on the libraries' side in educating users in these areas. An individual instruction session, which might involve assisting the user in customizing their sharing settings on each social media site, and perhaps installing a series of privacy-related software tools, could be very time-intensive and not scale well to serving larger communities.

The implication for library educators, as is the focus of the several large funded projects mentioned earlier, are that deep technical knowledge, flexibility, and confidence are required to navigate the numerous tools and systems, which we ourselves may or may not be users of. Reference sessions may require the ability to elicit a patron's particular concerns (for example – ads that track them from webpage-to-webpage), suggest a tailored set of privacy-protection tools, as well as bring additional privacy concerns to the user's attention, which they may not have been aware of.

Researching our recommendations

Many of the privacy technology guidelines and toolkits provided by library-related organizations focus on the *how to*, with relatively little explanation of the mission and goals of the software tools' creators or maintainers. The research detailed above demonstrates that privacy tools may in fact increase users' privacy concerns, without giving them insight into the underlying functionality or purpose of the tools. In educating their patrons, libraries must take care to (as much as possible) convey why specific tools should or should not be trusted; this assessment of authenticity and trustworthiness falls under the larger need for digital literacy.

Given the low barrier to software creation and distribution on the Web and mobile app environments, users may mistakenly employ technology tools that have malicious intent. In recent years, this was seen on a wide scale when highly-publicized current events about government surveillance and corporate data breaches drove many people to employ virtual privacy networks (VPNs) for the first time. However, subsequent reviews of the myriad of VPN mobile app options available to users found that many offered little robust protection, threatened the users' privacy by collecting their data, or even contained malware (Ikram et al., 2016). So simply advocating for the use of a general technology, such as VPNs or ad-blocking plugins, may lead users to make personally damaging technology choices, all the while thinking they are taking action to protect themselves. As mentioned earlier, the pace of technological change makes this a particularly difficult issue to keep pace with as new tools enter the market on a near-daily basis.

Future educational and research efforts

It is striking that little of the research presented above, exploring the use of privacy-protection technology tools, assessed library patrons or librarians directly, though the general themes can be extrapolated to this group. Prior research on the technology skills employed by librarians in practice indicates a lack of engagement with deeply technical tasks (e.g. Maceli and Burke, 2016) and it is reasonable to assume that a similar problem of information asymmetry and the privacy paradox of inaction exists for librarians and library staff, mirroring the general population findings. These findings are therefore of interest both in our own educational practices, as well as in educating our patrons and communities, and numerous questions for future research efforts emerge. On the educational front, the Masters of Library Science (MLS) and allied degrees likely need deeper coverage

of the underlying technical infrastructure and data flow of the Internet, related directly to privacy threats and vulnerabilities. For practicing librarians and library staff, this knowledge may need to be disseminated through continuing education or professional development opportunities; as the funded privacy-related projects mentioned earlier come to fruition, these opportunities will likely increase.

Relatively little is known of librarians' existing use of privacy-protection technology tools, and this area could benefit from further study. Current work of the author's is exploring librarians' current personal use of privacy-protection tools and how that relates to their technical knowledge and experiences, to close this gap. On the patron side, as the large-scale funded projects mentioned earlier continue to progress, there will be a need to assess the success of patron education efforts and their rate of privacy-protection tool adoption.

Conclusion

There is a clear need for library and information science practitioners, researchers, and organizations to take a larger role in building the corpus of research knowledge about the public's privacy concerns, actions or inactions, and use of privacy-protection tools. The review of literature presented in this article poses several challenges to existing projects training librarians to educate patrons in privacy threats, as well as protective tools and techniques. These challenges include: significant technical knowledge gaps in our patrons (and librarians and library staff as well), the need to support a staggering number of technology tools and techniques, as well as taking care to understand the underlying mission and goals of the suggested tools' creators. Further work is needed to integrate privacy-protection technology topics more deeply into the Masters of Library Science (MLS) and its allied degrees, study librarians' and library staff's current use and understanding of privacy-protection tools, and evaluate the effect of ongoing patron education efforts in this area.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Acquisti A, Brandimarte L and Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* 347(6221): 509–514.

Aldhafferi N, Watson C and Sajeev AS (2013) Personal information privacy settings of online social networks and their suitability for mobile Internet devices. *International Journal of Security* 2(2).

American Library Association (2014) Privacy Tool Kit. Available at: http://www.ala.org/advocacy/privacy/guidelines (accessed 10 December 2017).

American Library Association (2016) Library Privacy Guidelines. Available at: http://www.ala.org/advocacy/privacy/toolkit (accessed 2 March 2018).

Bashir M, Hayes C, Lambert AD, et al. (2015) Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology* 52(1): 1–10.

Bergman M (2009) Testing privacy awareness. In: Matyáš V, Fischer-Hübner S, Cvrček D, et al. (eds.) *The Future of Identity in the Information Society*. Vol. 298. Berlin,Heidelberg: Springer, pp. 237–253.

Brandimarte L, Acquisti A and Loewenstein G (2012) Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* (4)3: 340–347.

Chen HT and Chen W (2015) Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking* 18(1): 13–19.

Daniel WK, Xu X, Bai M, et al. (2014) Privacy issues in online social networks: User behaviors and third-party applications. In: *PACIS 2014 Proceedings* 42. Available at: http://aisel.aisnet.org/pacis2014/42/ (accessed 24 April 2018).

Electronic Frontier Foundation (2018) About EFF. Available at: https://www.eff.org/about (accessed 19 March 2018).

Fortier A and Burkell J (2015) Hidden online surveillance: What librarians should know to protect their own privacy and that of their patrons. *Information Technology & Libraries* 34(3): 59–72.

Hargittai E and Litt E (2013) New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy* 11(3): 38–45.

Ikram M, Vallina-Rodriguez N, Seneviratne S, et al. (2016) An analysis of the privacy and security risks of android VPN permission-enabled apps. In: *Proceedings of the 2016 ACM internet measurement conference*, Santa Monica, CA, USA, 14–16 November 2016, pp. 349–364. New York: ACM.

Institute of Museum and Library Services (2017) New York University & Library Freedom Project: Privacy in Libraries. Available at: https://www.imls.gov/grants/awarded/re-95-17-0076-17 (accessed 14 December 2017).

Kang R, Dabbish L, Fruchter N, et al. (2015) 'My data just goes everywhere': User mental models of the Internet and implications for privacy and security. In: *Symposium on Usable Privacy and Security (SOUPS)*, Ottawa, Canada, 22–24 July 2015. Available at: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf (accessed 24 April 2018).

Kumaraguru P and Cranor LF (2005) *Privacy Indexes: A Survey of Westin's Studies*. Pittsburgh, PA: Institute for Software Research International, School of Computer Science, Carnegie Mellon University.

Leon P, Ur B, Shay R, et al. (2012) Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In: *Proceedings of the SIGCHI conference on human factors in computing systems*, Austin, TX, USA, 5–10 May 2012, pp. 589–598. New York: ACM.

Library Freedom Project (2015) Tor exit relays in libraries: A new LFP project. Available at: https://libraryfreedomproject.org/torexitpilotphase1/ (accessed 10 December 2017).

Library Freedom Project (2018) Privacy toolkit for librarians. Available at: https://libraryfreedomproject.org/ (accessed 12 January 2018).

Lin J, Sadeh N, Amini S, et al. (2012) Expectation and purpose: Understanding users' mental models of mobile App privacy through crowdsourcing. In: *14th ACM Ubicomp*, Pittsburg, PA, USA, 5–8 September 2012, pp. 501–510. New York: ACM.

Maceli M (2018, forthcoming) Privacy-protection technology tools: Libraries and librarians as users, participants, and advocates. In: Varnum KJ *The Top Technologies Every Librarian Needs to Know: A LITA Guide*. Chicago, IL: ALA TechSource.

Maceli M and Burke J (2016) Technology skills in the workplace: Information professionals' current use and future aspirations. *Information Technology and Libraries* 35(4): 35–62.

Madden M and Rainie L (2015) Americans' attitudes about privacy, security and surveillance. Available at: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (accessed 2 December 2017).

Madejski M, Johnson M and Bellovin SM (2012) A study of privacy settings errors in an online social network. In: *Pervasive computing and communications workshops (PERCOM Workshops)*, Lugano, Switzerland, 19–23 March 2012, pp. 340–345. IEEE.

Malandrino D, Scarano V and Spinelli R (2013) How increased awareness can impact attitudes and behaviors toward online privacy protection. In: *Proceedings of the 2013 international conference on social computing (SOCIALCOM'13)*, Washington, DC, USA, pp. 57–62. IEEE.

Marden W (2017) Brooklyn, Queens, and New York Public Libraries launch a new digital privacy initiative. Available at: http://www.oif.ala.org/oif/?p=11782 (accessed 10 January 2018).

Nijboer J (2004) Big Brother versus anonymity on the Internet: Implications for Internet service providers, libraries and individuals since 9/11. *New Library World* 105(7): 256–261.

Noh Y (2014) Digital library user privacy: Changing librarian viewpoints through education. *Library Hi Tech* 32(2): 300–317.

Park YJ and Jang SM (2016) African American Internet use for information search and privacy protection tasks. *Social Science Computer Review* 34(5): 618–630.

Rainie L and Madden M (2015) Americans' privacy strategies post-Snowden. Available at: http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/ (accessed 3 December 2017).

Rotman D (2009) Are you looking at me? Social media and privacy literacy. Poster presentation. In: *iConference*, Chapel Hill, NC, USA, 8–11 February 2009.

Schaub F, Marella A, Kalvani P, et al. (2016) Watching them watching me: Browser extensions' impact on user privacy awareness and concern. In: *USEC'16: NDSS workshop on usable security*, San Diego, CA, USA. DOI: 10.14722/usec.2016.23017.

Sturges P, Davies J, Dearnley J, et al. (2003) User privacy in the digital library environment: An investigation of policies and preparedness. *Library Management* 24(1/2): 44–50.

Trepte S, Teutsch D, Masur PK, et al. (2015) Do people know about privacy and data protection strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS). In: De Hert P and Gutwirth S (eds) *Reforming European Data Protection Law*. Netherlands: Springer, pp. 333–365.

Wash R (2010) Folk models of home computer security. In: *Sixth symposium on usable privacy and security* (SOUPS), Redmond, WA, USA, 14–16 July 2010, pp. 1–16. New York: ACM.

Wills CE and Zeljkovic M (2011) A personalized approach to web privacy: Awareness, attitudes and actions. *Information Management & Computer Security* (19)1: 53–73.

Wissinger CL (2017) Privacy literacy: From theory to practice. *Communications in Information Literacy* 11(2): 378–389.

Author biography

Monica Maceli is Assistant Professor at Pratt Institute School of Information, focusing on emerging technologies in the information and library science domain. She earned her PhD and MSIS from the College of Information Science and Technology (iSchool) at Drexel University. She has an industry background in web development and user experience, having held positions in e-commerce, online learning, and academic libraries. Her research areas of interest include end-user development, human-computer interaction, and information technology education.

Article

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 203–222

DOI: 10.1177/0340035218785389
journals.sagepub.com/home/ifl

Information disclosure, privacy behaviours, and attitudes regarding employer surveillance of social networking sites

Deirdre McGuinness
William Fry Solicitors, Dublin, Ireland

Anoush Simon
Aberystwyth University, UK

Abstract

This paper explores the use of social networking sites amongst the student population of a Welsh university, with particular respect to information-sharing and privacy behaviours, and the potential impact of social networking site checks by employers on future use of these sites. A mixed-methods research design incorporating both quantitative and qualitative approaches was employed to investigate the research question. Results demonstrated that participants were concerned with maintaining privacy online, and were careful with regards to posting and protecting information on social networking sites; however, protective measures were imperfect due to human and system errors. Most respondents were aware of social networking site surveillance, with many noting that this would have an impact on their future use; however, users are active in protecting their privacy through a combination of use of privacy settings and varied levels of information disclosure dependent on context.

Keywords

Information and society/culture, Internet privacy, privacy, social media, social networking sites, surveillance

Submitted: 15 January 2018; Accepted: 9 May 2018.

Introduction

Over the past decade, with developments in social media, the Web has become increasingly social, with users actively creating their own content for dissemination across the internet. Social networking sites (SNSs) are one such means of sharing user-generated content, allowing users to disseminate content far beyond the borders of what was previously possible, and enabling them to 'become the stars of their own productions' (Pempek et al., 2009: 234).

SNSs have come under scrutiny regarding the security of online information. Changes to SNS infrastructure or security features have often been met with negative reactions from users concerned about losing control over personal information, but the behaviour of users has also attracted attention, with media reports indicating that people are disseminating information without thought of the possible consequences (Phipps et al., 2018).

In using SNSs, people are encouraged to share personal information with larger audiences and have grown accustomed to doing so. Research suggests that Internet users are comfortable sharing information within controlled environments, which is what makes SNSs (with password protection and privacy settings) attractive for information disclosure (Bateman et al., 2011). Many SNS users communicate in a manner that demonstrates their belief that these online communities are safe (Clemmitt, 2006). They post information with a specific audience in mind, and, with the

Corresponding author:
Anoush Simon, Information Studies, Aberystwyth University, Aberystwyth, Ceredigion, SY23 3AL, Wales, UK.
Email: ads@aber.ac.uk

availability of privacy settings, are able to define the parameters of their audience. However, online privacy is at risk when users underestimate the visibility of their profiles and fail to enforce adequate privacy measures, thereby leaving information open to unwanted viewers.

Employers take note of the wealth of information available on social media and may use them to gather information about current/prospective employees. Employers have always been able to conduct background checks on applicants but were rarely able to investigate the social aspects of a prospective employee's life. SNSs act as an additional source of personal data, enabling employers to conduct background checks at any stage of the hiring process and make decisions based on this information (Clark and Roberts, 2010).

SNS users are aware of possible privacy issues due to the frequent media reports on the topic. In particular, employer SNS checks are increasingly anticipated by prospective employees (Clark and Roberts, 2010). In recent years, various guidelines have been developed for and by employers (ACAS, n.d.) and upcoming, major changes to data protection (the General Data Protection Regulation (GPDR)) have also prompted further discussion and action (ICO, 2017).

It is possible that employer checks – even while limited and legitimate – could diminish the usefulness of social networking sites as a means of communication, as users fear judgement by current or prospective employers, and so alter their online behaviours (Clark and Roberts, 2010). Awareness of these risks may impact on how users employ SNSs. The practice of employer SNS checks, and its potential impact, was the focus of this study.

The aim of this research was to explore SNS use amongst students within a Welsh (UK) university, with regard to information-sharing and privacy behaviours, and to investigate the potential impact of employer scrutiny on their future SNS use.

The research was conducted in a medium sized university in Wales, United Kingdom. Both undergraduate and postgraduate students were included. The type of SNS studied was limited to a particular subset of social media websites. According to Keenan and Shiri (2009), there are two main types:

- people-focused, where social interaction involves the sharing of personal content centred on the user's profile/homepage (e.g. Facebook, Twitter, etc.);
- activity-focused, in which social interaction is based on site-specific content relating to a particular theme/subject (e.g. YouTube for video content, Flickr for photographs).

For this study, people-focused SNSs were the focus. Users of these sites may participate more actively and share more personal information with their online connection compared to users of activity-focused SNSs. Within this broad category, some sites are not primarily 'social' but more professionally-focused, e.g. LinkedIn. However, this site allows people to create networks (although professional rather than social) and generates a large volume of discussion, personal messaging and other content, therefore it was included in the broad 'people-focused' category. As will be seen later, participants were able to make a clear distinction between the aims of various sites and understood the need to adjust content and interactions accordingly.

The specific focus in this paper is a consideration of the results of the qualitative data (contextualised as appropriate with the findings of the quantitative element of the project), specifically perceptions, attitudes and reported behaviours in relation to privacy online, and particularly reactions to potential employer surveillance in this regard.

Literature

With the development of online communities, 'a more digital approach for maintaining and establishing relationships' (Madhusudhan, 2012: 100) has become the norm. Social media sites are possibly the most popular means of online communication, enabling users to share information to a selected online audience and allowing them to keep up to date with the lives of friends and family. While SNSs represent a popular and vibrant means of social communication, concerns have also been raised. The widespread practise of sharing personal information has stimulated debate about privacy online; when engaging with SNSs, users are encouraged to divulge personal details, and may do so without thought to maintaining privacy.

The debate regarding SNSs and privacy includes the professional environment. Employers are able to search profiles of potential job candidates and recruit those whose profiles demonstrate their suitability for the position (and indeed some sites, such as LinkedIn, exist for this purpose). However, the potential for employers to check non-professional SNS profiles has been the subject of contention, with job applicants arguing that this practise is an invasion of their privacy. SNS checks may have detrimental effects on future SNS usage, both from the

perspective of its users and for the SNS itself (Clark and Roberts (2010).

Information disclosure

Sharing information is an important part of using SNSs and is actively encouraged, with sites providing a number of disclosure categories, allowing users to input personal information, as well posting information on their own profiles and their Friends' profiles.

SNS users prefer to provide accurate self-presentations, and 'users often respond honestly and in the majority of disclosure categories' (Strater and Lipford, 2008: 2). Reasons for self-disclosure in online communities include peer pressure, desire to be portrayed in a particular manner, trust in the network and other members, perceived benefits vs. costs of sharing information, SNS interface, and relaxed attitudes to privacy (De Souza and Dick, 2007). Chen and Michaels (2012) note the importance of the online community in information disclosure, stating that users wish to identify within the community and desire feedback affirming their membership from other users. A focus of attention to information sharing on SNSs is the posting of potentially sensitive/controversial information. Users frequently update their profiles with highly personal information, using profiles 'as billboards about themselves while others use them as personal diary pages' (Clark and Roberts, 2010: 507). Included in this is information that could be construed as inappropriate. Foul language, sexist/racist comments, evidence of intoxication, sexually explicit material, and professional indiscretions have all been noted on SNS profiles (Go et al., 2012; Morgan et al., 2010).

Sharing information publicly is common practice among SNS users: Pempek et al. (2009) note that students are twice as likely to post information on each others' walls as send messages privately. However, some studies have noted that although some adolescents are posting personal/identifying information, it is not to the extent assumed. Nosko et al. (2010: 408) found that users exercise 'some discretion regarding what kinds of revealing information they are willing to share', or judge their disclosures based on the social norms of their network, suggesting the influential role of the user's audience (Strater and Lipford, 2008).

Social networking and privacy

The control of personal information is paramount, with Clark and Roberts (2010: 511) noting '. . . a general belief that there is a natural right to have some information about oneself kept from others'. The right to privacy is protected under Article 12 of the Universal Declaration of Human Rights, and many countries recognise the individual's right to privacy; it is restated in the UK Human Rights Act 1998 Article 8. Most recently, changes to Data Protection legislation in 2018 (leading from the rolling out of the GPDR) are likely to have an impact on how personal data is used and re-used, and discussions and guidelines about organisations' use of employee (and indeed prospective employee) data is currently widespread (ACAS, n.d.; ICO, 2017; Robles, 2017; Stacey, 2017).

Legally, there is no clear consensus over online privacy. SNS users have the right to privacy; however, they must be aware that information shared online may go public (Smith and Kidder, 2010). It is argued that information shared online loses its claim to privacy as what is posted online (or indeed in the public sphere, as in Twitter) has a lower 'expectation of privacy' (Barnes et al., 2009: 32), due to the potentially large audience and difficulties in controlling access to information. Posting information on SNSs can be considered self-publication, and 'a person's right to privacy ceases once the individual publishes the information' (Clark and Roberts, 2010: 512); discussions in the literature indicate that the public/private boundaries may be blurring, and this impacts on employment relations (McDonald and Thompson, 2016; Sánchez Abril et al., 2012).

Maintaining privacy

Maintaining privacy on SNSs is important due to the presence of personal/sensitive information, which, if made publicly available, could harm the user. SNS users manage their online privacy by controlling the amount/type of uploaded information, or controlling access to information by using privacy settings. Most, if not all, SNSs provide multiple privacy settings enabling users to limit the information that can be viewed by strangers (i.e. individuals not accepted as Friends/Followers), and some sites (e.g. Google+ and Facebook) have also introduced settings allowing users to control the spread of information amongst accepted Friends. However, privacy maintenance may fail due to individual and system errors (Strater and Lipford, 2008). Particular faults include weak default privacy settings (Byrnside, 2008), the tendency for settings to change without prior notification (Landman et al, 2010), and the difficulty in designing privacy settings to cover all possible outcomes (Chen and Michael, 2012). SNS users frequently make little use of available privacy settings, possibly due to poor interface design, lack of understanding, conforming to social group expectations, and trust in the online

community's security (Strater and Lipford, 2008). Users often underestimate their profiles' visibility (Acquisti and Gross, 2006; Byrnside, 2008) and vulnerability to risk (Cho et al., 2010). Although users are generally informed through privacy policies as to the visibility of their information, these are not always read (Arcand et al., 2007).

Employers and SNSs

Employers are gathering an increasing amount of information about job candidates 'to ensure the best fit between an applicant and the employer's organization' (Byrnside, 2008: 448), and now incorporate SNS checks into the decision-making process, viewing them as a convenient means of gathering information about prospective employees. Significant numbers of employers have reported that online information has influenced their decision, in most cases leading to the disqualification of the candidate over the presence of negative content (Clark and Roberts, 2010). Generally, employers will search for applicants using various SNSs and examine what information is made available. If applicants have privacy settings in place, HR managers may encourage them to join the company's SNSs as part of the recruitment process (Madera, 2012), or may add these applicants as Friends (Brandenburg, 2007). SNS profiles are attractive to employers in providing an easy and cost-effective way of gathering information about job applicants, compared to traditional background checks which were usually reserved for serious candidates (Branine, 2008). For employers, gathering information is necessary for making an informed decision regarding the right candidate (Brandenburg, 2007; Clark and Roberts, 2010). SNSs also serve as a useful means of confirming information given to employers by job applicants (Levashina, 2009).

UK recruitment has become increasingly person-orientated (Branine, 2008), and, although academic/professional achievements are still important for hiring decisions, 'non-academic qualities and "fit" are playing an increasingly significant role' (Go et al., 2012: 296). SNSs enable employers to gain a comprehensive view of the applicant, as well as providing insight into his/her standard behaviour. Traditional selection methods are frequently subject to bias; they 'include a certain element of self-presentation, reflecting "maximal" instead of "typical" work performance' (Kluemper and Rosen, 2009: 570). Personal profiles are less likely to highlight information aimed at employers, therefore possibly affording a more accurate insight into the applicant's personality/character. Applicants may argue that their personal/social life is no indication of their professional behaviour, but employers maintain that employees, in having access to sensitive company information, need to demonstrate careful judgement (Brandenburg, 2007). Decision making in sharing personal information may indicate how they might treat company data.

The accuracy of judgements based on SNS information has been questioned (Slovensky and Ross, 2012), and lack of objectivity in SNS checks may also be a problem. Decisions are based on subjective assessments of strangers' profiles in which little context is given, thereby easily leading to misinterpretation of posted content. Judgements made on this basis can be biased, especially without policies to guide this practice (Go et al., 2012; Clark and Roberts, 2010). SNS profile checks have the potential to invade the applicant's privacy, in accessing personal information without the owner's knowledge/consent (Byrnside, 2008), and impacting on 'the right to decide whether, and to whom, to disclose information in an atmosphere free from coercion' (Slovensky and Ross, 2012: 63).

The merits of employer SNS checks are discussed, justifying their use in selecting employees, whilst noting problems faced by profile owners and employers wishing to select the right applicant. Of interest were the potential implications of this practice. Employers must be aware that applicants may react negatively to the incorporation of SNS information into the decision-making process, which may perhaps lead to a negative perception of the organisation. SNSs themselves may also suffer as a result (Madera, 2012). Clark and Roberts (2010) argue that SNSs may be impacted adversely, with users modifying their online behaviour for fear of judgement or punishment by employers.

Themes identified in the literature have interesting implications for both employers and SNSs. In this context, this paper examines how students (a significant SNS user-group) react to the possibility of SNS checks in their future professional endeavours, and considers the possible impact employer surveillance will have on future SNS use.

Methodology

A mixed-methods approach was chosen as the most appropriate method for this study. While qualitative and quantitative research methods each offer numerous benefits, they are not without drawbacks. Both have underlying weaknesses, which may threaten the validity of the research. Quantitative methods are appropriate for describing what has happened, but

'they offer little insight into the social processes which actually account for the changes observed' (Clarke and Dawson, 1999: 55). They inform researchers about patterns of social interaction but fail to provide explanations as to how/why events have happened, and do not aid researchers in generating theory (Amaratunga et al., 2002).

Qualitative methods focus on 'lived experience' and seek to describe 'the meanings people place on the events, processes and structures of their lives' (Amaratunga et al., 2002: 22). They are useful for explorative research and for the development of hypotheses and can expand on quantitative data collected from the same setting (Amaratunga et al., 2002). However, there are important issues to be aware of (Pickard, 2007). Analysis of qualitative data is subjective, so results produced from such studies are dependent on the researcher's interpretation. Results are not readily applied to other similar situations, and there is difficulty in generalising data across the wider population. Questions of reliability and credibility are common with qualitative research.

The mixed-method approach involves utilising both qualitative and quantitative approaches in a single research study (Tashakkori and Creswell, 2007); this allows for methods triangulation, whereby the consistency of research findings can be checked by using different methods of data collection, potentially balancing or compensating for weaknesses in a single method. This may lead to increased validity and reliability of results. The mixed-method approach is also used in cases when a single approach fails to investigate the phenomenon thoroughly; results from one method are supported and enhanced by results of the other – researchers can seek explanations for quantitative results, or generalise qualitative results and test their validity (Fidel, 2008).

To gather both large-scale data and comprehensive insights, and to offset weaknesses in each method, a mixed-methods approach was chosen as the most appropriate method for this study. Participants were recruited online through a snowball sampling method.

The methods used included an online questionnaire consisting of 18 questions (including both open-ended and closed), and semi-structured interviews. Responses to closed questions were coded prior to the launch of the questionnaire and open-ended responses were coded manually. A series of semi-structured interviews (nine in total) were carried out to expand on some of the issues raised earlier in the research process. Interviews were recorded and transcribed for analysis, with codes assigned to the different themes established in each interview.

Participants were drawn from the student population of the university. Both undergraduate and postgraduate students were recruited for the survey to gain a more comprehensive view of online behaviour across the entire student population. For the interviews, the focus was exclusively on postgraduate students, to gain insight on views of privacy and employer surveillance amongst emerging professionals and to discuss changes in social media use and online behaviour throughout their university careers.

The sample gathered for this study compared to the entire student population is inevitably relatively small. As a result, the extent to which the findings of this research can be generalised to the wider population is limited. However, it does provide insights into student perceptions and responses to privacy online, which can contribute to our developing understanding of this area, and which is the focus of this paper.

Results

Questionnaire

The questionnaire response (n=108) consisted of 36 males (33.3%) and 72 females (66.7%). Respondents ranged in age from 18 to 61 years, with a mean age of 24.6 years. There were 64 undergraduates (59.3%) and 44 postgraduates (40.7%).

Most respondents identified themselves as frequent SNS users citing activity across a wide range of sites, including Facebook, Twitter and LinkedIn (Table 1), with 94 respondents (87%) visiting SNSs once a day or more (Table 1). Facebook, Twitter and LinkedIn were the most commonly used social networking sites amongst the participant base, and LinkedIn (being a professional-focused SNS) served as an interesting juxtaposition to the other sites, indicating how users are targeting employers with this information and so may be approaching it differently compared to more social, personal sites.

Participants reported multiple reasons when asked why they used SNSs. Frequently reported reasons were keeping in touch with people; including people met with only occasionally (92.6%), and people seen frequently (70.4%). SNSs were used to keep abreast with Friends' news (81.5%); however, only 38.9% of respondents reported using SNSs to keep their Friends up to date with *their* news. The disparity may indicate a preference amongst respondents to view others' information rather than posting their own.

Lesser reported reasons were meeting new people (12%) and self-promotion (12%). Social use of SNSs was predominant; only 24.1% used SNSs for professional networking. However, 55.6% reported

Table 1. Frequency of SNS use.

0	Answer	Response	%
1	Less than once a week	2	1.90
2	Once a week	1	0.90
3	A couple of times a week (2–3 days)	3	2.80
4	Most days during the week (4–6 days)	8	7.40
5	Once a day	13	12.00
6	More than once a day	26	24.10
7	Many times throughout the day	55	50.90
Total		108	100%

Table 2. Availability of information posted on SNS profile.

	General public	Friends and their friends only	Friends only	Myself only	Not certain who can view	Unavailable/unsure if available
Screen name/pseudonym/nickname	50	7	14	1	2	23
Full name	54	12	26	5	4	7
Date of birth	20	6	46	25	4	4
Hometown	30	11	39	12	4	8
Current address	7	3	27	33	1	32
Education history	15	15	59	5	6	6
Employment history	7	10	46	15	4	21
Family information	6	6	53	15	5	19
Friends list	28	19	42	9	5	4
Relationship status	14	7	44	18	4	17
Sexual orientation	13	8	31	20	3	27
Political views	7	6	35	15	3	37
Religious views	8	7	36	15	3	34
Email address	4	4	46	26	8	15
Contact number	1	1	24	36	4	36
Personal website	5	0	20	14	7	56
Full address	1	0	8	34	3	55
Interests	11	14	55	2	7	15
Posted photographs	6	16	74	2	5	1
Photographs in which you are tagged	7	25	61	5	5	2
Posted videos	5	11	63	3	5	15
Videos in which you are tagged	5	19	54	5	6	12
Wall posts on own wall	9	11	72	4	7	1
Notes/Blogs	8	8	46	1	4	32
Events you have created	4	12	61	2	6	16
Events you are attending	5	19	58	2	11	7
Communities/Networks/Groups	13	16	52	6	12	5

sharing university coursework information and/or employment-related information.

Information sharing on SNSs. Respondents were asked to identify the information posted on their profiles, and to indicate to whom it was available (Table 2).

Much of the information posted on SNS profiles was available to Friends only, excluding full name and screen name (pseudonym/nickname) with most respondents (50% and 46.3% respectively) making this public. Additionally, respondents' Friends lists were generally shared beyond the respondent.

Although 38% of respondents shared their hometown beyond their Friends, respondents were more cautious when sharing their full addresses, with many (50.9%) believing this information to be unavailable, and 31.5% reporting it as viewable only by the respondent himself/herself. Only one respondent

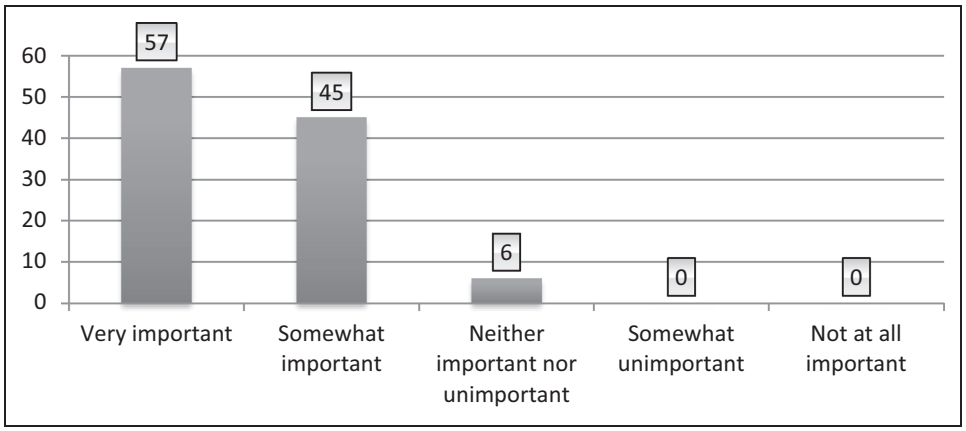

Figure 1. Importance of online privacy.

made their full address available to the public. Contact numbers were mostly omitted from profiles (33.3%) or made viewable to respondent only (33.3%). However, 22.2% made this information available to their friends. Very few (1.9%) made this information available to a wider audience.

Information regarding relationship status, political stance, religious views and sexual orientation were generally shared with Friends only, or were omitted altogether. Less than 20% of respondents reported sharing this information publicly. Information regarding employment history and education history was generally shared with Friends only (42.6% and 54.6% respectively); only a few respondents (6.5% and 13.9%) made this information public. Photographic/video media were generally restricted to Friends; however, media in which respondents were tagged were more often available to Friends of Friends. Created/attended events were also usually restricted to Friends, with low numbers reporting that this information was made available to the public. Respondents generally appeared to be aware of the audience for their online content, with a minority (11.1% and less) reporting uncertainty over who could view each piece of content.

Privacy. Survey respondents were asked about their attitudes to privacy online. The majority of respondents placed some importance in having privacy when using SNSs (Figure 1), reporting it as 'somewhat important' (41.6%) and 'very important' (52.8%).

An open-ended question asked respondents to note down privacy concerns experienced when using SNSs (Table 3). The 96 responses given were coded for analysis.

The most frequently reported concern was unwanted people/groups accessing personal information (18.5%) with possible consequences such as identity theft/identity fraud (14.8%), hacking (10.2%), cyber-bullying (0.9%) and stalking (3.7%) noted.

Table 3. Reported privacy concerns amongst respondents.

No response	12	11.1
No concerns	6	5.6
Damage to reputation	3	2.8
Lack of trust in SNS	1	0.9
Loss of privacy	7	6.5
Identity theft/Fraud	16	14.8
Cyber-bullying	1	0.9
Employers checking profiles	8	7.4
Monitoring of online activities	2	1.9
Data-mining	8	7.4
Understanding privacy settings and keeping up with policy changes	4	3.7
Strangers/Unwanted parties accessing personal information	20	18.5
Inappropriate/Unauthorised use/dissemination of personal information by other people	17	15.7
Hacking	11	10.2
Stalking	4	3.7

Several respondents were concerned over their information 'getting into the wrong hands' and being used without permission (15.7%), and the potential loss of privacy (6.5%) and damage to reputation (2.7%):

> Some information I might be tagged in might not be appropriate for others to see.

A small proportion of respondents (7.4%) reported concern over employers gaining access to online information not intended for their viewing, as 'some activity that may jeopardise your career'.

Some respondents had problems with SNSs themselves, with one indicating that they did not trust their SNS, and another four reporting difficulty in keeping

Table 4. Reported methods of protecting personal information.

#	Answer	No.	%
1	Using strict privacy settings	74	68.5
2	Blocking content from members of the public (i.e. people you are not friends with)	84	77.8
3	Limiting the amount of information you upload to your profile	79	73.1
4	Only uploading information you deem appropriate for a wide audience	77	71.3
5	Limiting the amount and availability of important personal information (e.g. contact details, descriptive information such as date of birth, address, employment, etc.)	70	64.8
6	Using a pseudonym or nickname instead of your full name to make it more difficult for members of the public to find your profile.	19	17.6
7	Using private messaging to communicate information you do not want to make available to a wider audience	87	80.6
8	Controlling what content you are tagged in (e.g. requiring website to ask for confirmation before you are tagged in a photograph)	45	41.7
9	Keeping your password secret	99	91.7
10	Reading the privacy policy for information on how your information is used	28	25.9
11	Keeping your accounts across different social networking sites separate (i.e. not linked)	55	50.9
12	Only accepting friend/follower requests from people you already know	84	77.8
13	Other (please specify)	3	2.8

up to date with privacy changes. Also noted was the possible monitoring of online activities (1.9%) and data-mining (7.4%):

> Selling personal information to third parties without consent. My life should not be a commodity to be sold without my knowledge or approval.

Respondents selected from multiple choices their preferred methods of protecting their information (Table 4).

Controlling access to information was widely implemented: blocking content from the public (77.8%); granting access only to known Friends (77.8%); and using strict privacy settings (64.8%). The vast majority (91.7%) kept their password secret.

Most respondents also restricted what they shared: 73.1% limited the amount of information uploaded to their profile, with 64.8% limiting identifying information; 41.7% of respondents reported controlling information posted about themselves by their Friends; 71.3% only uploaded information appropriate for wide audiences, while 80.6% used private messaging to share information unsuitable for larger audiences; 50.9% reported keeping their different SNS accounts separate, thereby maintaining separate online identities.

Some privacy measures were less frequently employed. Only 17.6% employed a pseudonym to protect their identity or prevent strangers from finding them, and only 25.9% reported reading the Privacy Policy for information about controlling their content.

Most respondents were confident in protecting their information (Figure 2), reporting that they were 'very confident' (18.5%) and 'somewhat confident' (50%). Only 10.2% reported self-doubt in protecting their information.

Employer surveillance. Respondents were aware of the potential of SNS surveillance by employers (Figure 3), reporting that it was very likely (27.8%) and somewhat likely (42.6%). Very few respondents considered the likelihood of employer surveillance to be low, with only two respondents (1.9%) replying 'probably not'.

Responses were mixed regarding the possible effects of SNS checks on future use (Figure 4). While 30.6% of the sample reported that their SNS use

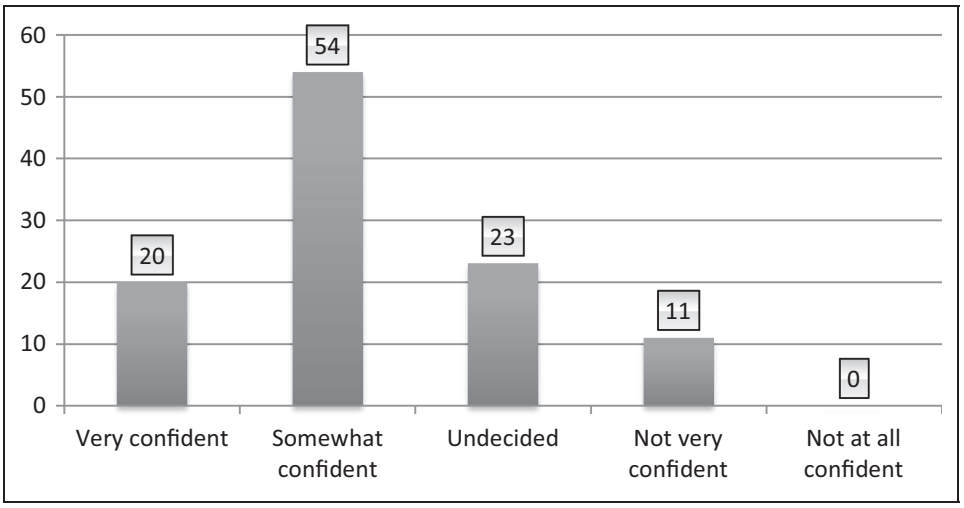

Figure 2. Reported confidence in ability to protect personal information.

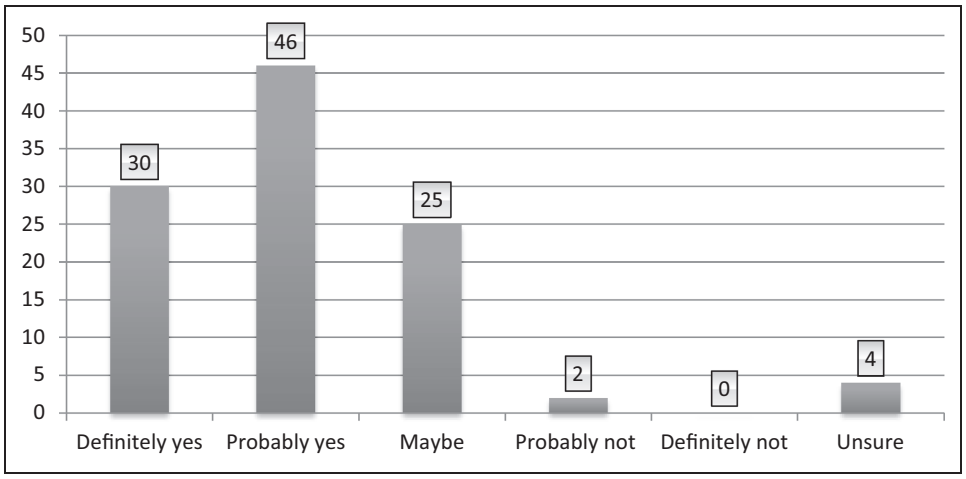

Figure 3. Perceived likelihood of SNS checks.

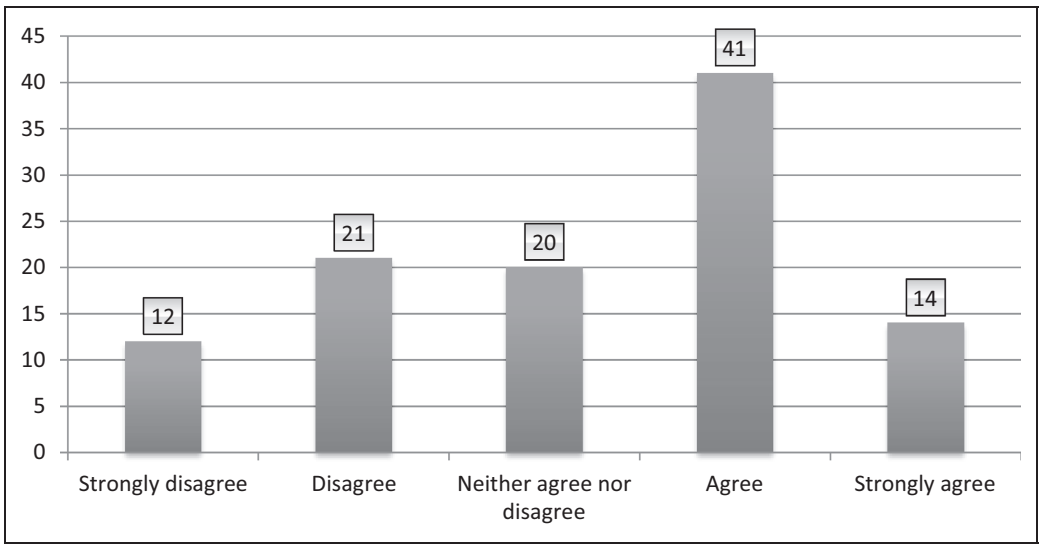

Figure 4. Perceived likelihood of employer surveillance affecting personal use of SNSs.

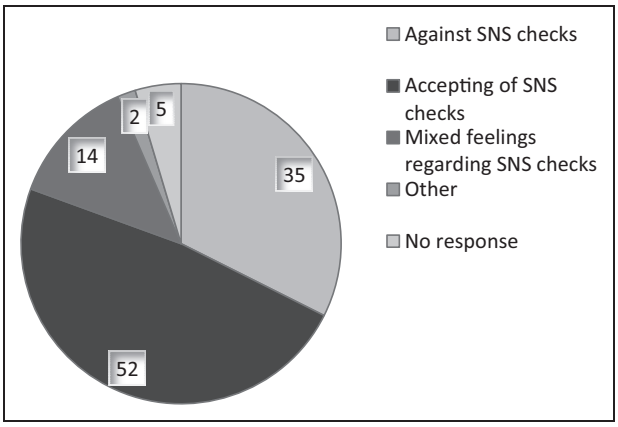

Figure 5. Respondent reactions to SNS checks.

would not change, a greater proportion (50.9%) reported that it would. 18.5% remained unsure.

An open-ended question was used to ascertain attitudes towards employer SNS checks (Figure 5). Out of the 108 respondents, 103 provided an answer, which were coded for analysis. Three groups were established; those against SNS checks (n=35, 32.4%), those accepting of the practice (n=52, 48.1%), and those with mixed feelings (n=14, 13%). Two respondents did not give a direct opinion.

Those against the idea claimed it to be 'invasive and unethical', 'inappropriate', and 'stalker-ish'. Many were concerned with information being misinterpreted, arguing that SNSs were not an accurate representation of their lives. They expressed concern over being judged on this information, particularly if it were to overshadow their educational/professional achievements:

> The true person is usually misconstrued on social networking sites
>
> I hope they'd see any information they found in context, and be tactful about how they used it.

Although satisfied with employers checking professionally-orientated profiles, respondents were unhappy with sharing information regarding their personal lives, questioning its relevance in hiring decisions. They preferred to keep separate their professional and personal lives:

> What I choose to do in my spare time doesn't indicate the type of individual I will be on the job.
>
> Work should be separate from personal life.

Other respondents reported mixed feelings, considering employer surveillance 'annoying but understandable'. Although some disliked their profiles being checked, they could understand the employer's decision to do so:

> I don't think it's right that they should do it, but then again if I was employing someone I'd find social networking sites a good way of gaining an idea of how the potential employee is.

A significant proportion (48.1%) reacted more positively. Several were unconcerned with profile checks due to privacy settings in place, while others ensured that their information was appropriate for employers. Also noted was the possibility of making a favourable impression:

> If people are just a little smart about it, they will use things like Twitter and LinkedIn to enhance their employable image . . . Therefore being checked online by employers can actually be an advantage.

Others argue that employers have the right to look at available online information, arguing that if a user fails to hide information from the public, they cannot expect privacy:

> If I'm stupid enough to place incriminating statuses or photos for all to see then it's my own fault.

Future use. An open-ended question required respondents to discuss their expected future SNS use: 95 responses were returned with mixed reactions (Figure 6).

Most respondents (n=47, 43.7%) indicated that their SNS use would remain unchanged, primarily for social interactions. Another 13.9% reported that they would use also SNSs for social purposes in the future; however, they did not indicate whether this differed from current use. A small number (n=7, 6.5%) anticipated using SNSs for professional reasons due to their potential for marketing themselves and networking with other professionals. Eight respondents (7.4%) indicated that their use of SNSs would likely decrease in the future, citing 'less time on my hands' and lack of interest. Only one participant (0.9%) claimed a possible increase, stating 'it's going to become even more important'.

Thirteen respondents (12.0%) predicted that they would be more cautious with what they make available online. Even users planning to continue using SNSs as they do now noted the necessity of caution when posting content, particularly to avoid jeopardising their professional endeavours:

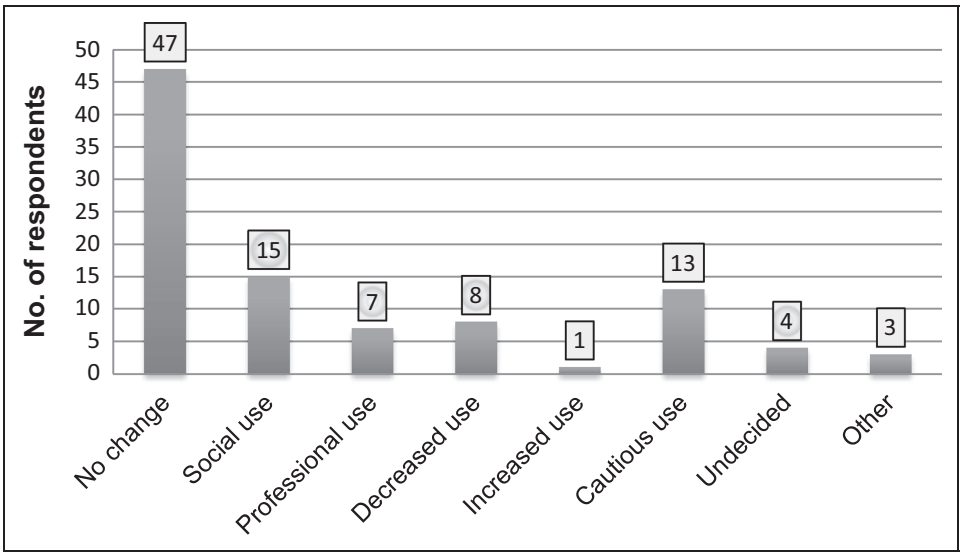

Figure 6. Expected future use of SNSs.

> I definitely feel that I couldn't vent about a bad day at work, even to friends, in case it would get back to my workplace somehow.

Employer surveillance will possibly affect SNS use amongst all respondents. Respondents indicated that they were willing to take measures to ensure that online content did not negatively affect their professional lives:

> Carry on the same, until I get a serious job, and then I'll recreate a new one, with appropriate pictures and stricter privacy settings.

The intention expressed here, to actively make use of the possibility of employer monitoring of SNS profiles to benefit the user, and indeed make them a more attractive potential employee, perhaps underscores a sense of being able to remain in control of personal information posted on SNS through a combination of privacy settings, experience, common sense and regular profile maintenance.

Interviews

Interviews were conducted with nine postgraduate students (7 females, 2 males, aged 22–32); four were UK residents and five international students, and were studying in different departments within the University. Interviewees used Facebook, Twitter, LinkedIn and YouTube, with Facebook being the most popular, and in all but one case, the most frequently used. Interviewees attributed specific purposes for different SNSs. Facebook was predominantly used for social interactions. Desire to stay in touch with people was a common reason for joining Facebook and was reported as its main benefit. Professional/educational use of Facebook was less common, though two interviewees used Facebook to share and gather information relating to their profession. The research did not specifically focus on differences between UK and international students. However, cultural background and context can have an impact – Kim et al. (2011) noted that although broad motivations for SNS use many be consistent, the weight placed on these, e.g. seeking entertainment or using social media for support, varies across countries.

Unlike Facebook, with its predominantly social focus, Twitter was not used for contacting friends. Instead, it was useful as a news feed, and for discussing and keeping informed about professional topics. Its value in allowing interviewees to promote themselves professionally and to network with other professionals was also highlighted:

> It's an easy way to show [employers] you are interested in issues to do with your future career, so it might just put you a little bit ahead.

LinkedIn was also employed by interviewees to facilitate professional networking and to seek information related to their future careers.

Information disclosure on SNSs. Different information was posted on interviewees' separate profiles, generally sharing day-to-day activities and pastimes on Facebook, while restricting LinkedIn and Twitter content to academic/professional achievements and interests. Although interviewees posted a wider variety of information on Facebook, they reported reluctance to share certain information, preferring to keep

personal information (e.g. regarding family, relationships, etc.) amongst close friends:

> People who are in my actual circle will know that about me, but stuff I consider too personal to share online, I don't post.

Interviewees were also reluctant to share highly detailed identifying information, and in particular, information about their location or contact details for fear of stalking, identity theft or harassment. Some interviewees reported a preference not to discuss work-related matters on Facebook:

> I've never talked about my employment, or if I've had a bad day at work, I never say any of that.

Interviewees made conscious efforts to restrict information disclosure and reported that they were more cautious in online interactions, citing the potentially large audience and permanency of this content. Several interviewees tried not to post too much information about their lives:

> I don't want everyone to know what I'm doing everyday . . . it can be a bit intrusive in that way.

However, the trend of posting considerable amounts of information was noted, and participants considered that such information disclosure is, in part, influenced by the SNS itself. Users can share information that they would have no opportunity to do in real life, and many may be influenced to disclose information due to the website's culture of sharing:

> Before, it would just ask you a bunch of your general likes, so you would mention sport, films etc. But now they have them separated into different fields so it encourages you to expand on it.

In this context it is possible to think about user-generated but SMS-facilitated content, which may differ considerably between networks depending on aim and scope of SNS. Feedback regarding the extent to which one can learn about people from their profiles was mixed. Much can be learnt in some cases, 'because some people are inclined to post everything on Facebook'. However, people are selective with their disclosures, therefore it is difficult to determine what they are really like:

> I don't think you get to know everything about someone . . . they choose what they put up there . . . You can make yourself sound a certain way.

Posted information is selected to portray the user in a certain manner, something which may be largely influenced by their perceived audience. Awareness of the audience can cause Facebook users to be more selective when posting information:

> People judge you when you post something, so you tend to think first 'should I post this, is this appropriate?'

This links to findings in the survey highlighting an awareness of employer presence on SNS sites but also the possibility that information can be presented selectively to promote oneself to this perceived audience.

Privacy. In general, interviewees were aware of privacy issues, and employed stringent privacy measures to protect themselves on Facebook. However, they were happy for Twitter and LinkedIn profiles to be open to promote themselves professionally:

> I use it for career stuff, so I like people being able to find you randomly and think 'oh, that's the person we should employ'.

Privacy was very important on Facebook, and interviewees revealed that they would change their use of, or delete, their profile altogether if privacy settings were no longer available. This decision was conveyed even amongst interviewees who demonstrated heavy dependence on Facebook:

> It would kill me, but I think I would have to really revisit how I use Facebook . . . I would probably have to take a lot of stuff down.

With Facebook, privacy was protected by limiting information disclosure, and restricting access to information. Interviewees generally only allowed Friends to access their information. Some interviewees were careful in accepting Friend requests, with one deleting and reporting strangers who sent her Friend requests. Another regularly reviewed her Friends' list to ensure that only certain Friends could access her online information:

> I look at the person and ask myself 'do I really care about this person' and if no, I unfriend them.

Some interviewees employed additional measures to protect their information. One interviewee prevented strangers from finding her profile by removing it from Facebook's search results. Another employed a privacy feature separating Friends into groups based

on intimacy/familiarity and allowing only close friends to access all information:

> People I don't really know, I've only met them at parties and stuff, I have them as 'acquaintances' so they're on a limited profile.

Although some interviewees believed that properly-used privacy settings should ensure the safety of posted information, others expressed doubt over this, stating:

> I don't think there is anywhere online that you can post information, and it'd be safe.

Even with privacy settings, interviewees highlighted the importance of only sharing information appropriate for wide audiences, as there were no guarantees over who could access profile information:

> If you wouldn't be happy with someone reading your comment in a magazine, don't put it on social networking sites, because it's the same difference at the end of the day. People can get hold of it, and you never know what they may use it for or judge you on.

Many interviewees reported that they were not entirely confident in maintaining privacy, blaming human error and system flaws. Two interviewees were uncertain if they were using appropriate privacy settings, while others reported that Facebook changed too often and did little to inform users as how best to protect themselves:

> It's difficult when the websites change . . . it takes you a while to get around the grasp of it again.
>
> It's too complicated and I think that's on purpose . . . so people get a bit confused and it's better for Facebook because they can control better what they want to do with the information.

Two interviewees were confident in protecting themselves online. For one, it was due to restricting information disclosure instead of relying on privacy settings. For the other, it was due to experience using these sites:

> I've used these sites from the very early days of them existing, so every time they've changed something, I've changed with it.

However, she had witnessed less experienced users struggling with privacy settings. Experience using SNSs appeared important in awareness/understanding of privacy issues and protection. The least experienced interviewee reported that she had difficulty with this and only through experimenting with the site was she beginning to understand Facebook privacy. Another interviewee reported that she had helped other users in setting up their profiles and explain how they could protect themselves:

> They would always come to me and ask me stuff; they were too scared and worried to put anything on there in case it all got out.

Many interviewees reported seeking information from friends and/or media reports regarding privacy issues. Several interviewees reported that SNSs failed to inform users, and that users themselves had to actively seek information and keep updated:

> You do have to keep aware of what's happening. If they have any changes of rules or if you need to update your privacy settings, you just have to keep on top of things really and just change with it.

Although several interviewees reported that they wished SNSs would better inform users, one interviewee noted that the SNSs' role in this is somewhat limited:

> If Facebook was to release information, would you actually pay attention to it? How many people read the terms and conditions?

Employer surveillance. Most interviewees were aware of employers checking SNS profiles, and some interviewees understood why employers used these sites, noting the opportunity for job applicants to take advantage of this trend:

> You can use things like Twitter to show that you're interested in the area you're trying to get a job in, so you're not just going to be someone who turns up at work, that you might have something extra that you can give to the job.

Interviewees were happy with sites such as LinkedIn and Twitter being checked, and some were unconcerned about Facebook checks as they had privacy setting in place and had ensured their information was appropriate. Others showed more reluctance, questioning the relevance/usefulness of Facebook information and arguing that employers should instead focus on information relating to their academic/career achievements. Interviewees were keen to maintain a separation between their work-life and their personal life, and that certain types of social media sites were appropriate in certain contexts:

> I'm one person outside of work, one person in work, and I will be professional and do my job when I'm there, but my downtime is my own.

This separation extended to their online activities, with interviewees creating separate SNS profiles in order to maintain 'several online identities instead of just the one'. This separation went as far as interviewees wishing to block managers and co-workers from their Facebook profiles, unless they were also friends socially. Interviewees argued that Facebook information provided only a limited view of their personality, and, as a result, may cause employers to make negative judgements regarding applicants who are otherwise suitable candidates:

> Seeing the person's social side doesn't really show what they're qualified for.
>
> You can party a lot, but still be a serious person at work, so it's not showing all of your personality.

However, conversely:

> sometimes your personal life can be an indication of what you'll do in your professional life.

Interviewees were concerned that they would be judged unfairly based on their information (particularly as several believed that employers were looking for negative information with which to disqualify candidates) and, as a result, be passed over for the position. Interviewees questioned the accuracy of judgements based on Facebook information, and were concerned about information being taken out of context. Facebook information demonstrated their social lifestyle to the exclusion of professional interests, and so, failed to inform employers about their educational/professional achievements and interests:

> You can still have a very good social life and still be very hardworking.
>
> People take pictures only at certain events; I don't think it captures your entire life.

Several interviewees questioned whether employers looking at SNS information would be objective and **recognise** that information posted on socially-focused SNSs like Facebook would not necessarily conform to professional standards, as it is not employed for this purpose:

> You can't just pretend you're an upstanding citizen hiding behind a really smart profile.

This is a particularly pertinent issue for students who often post content about their university experiences- information which may differ significantly from what employers wish to see.

Evolving use of SNSs. Most interviewees wished to continue using SNSs, post-graduation, as they did currently. However, this depended on changes in SNSs and in their lives. Several reported that they might remove content from their current profiles or create new, professional ones. Those who reported that their profile would remain unchanged were already confident that their information was appropriate or were relying on privacy settings for protection.

While interviewees reported that they would continue to use LinkedIn and Twitter for professional reasons in the future, professional use of Facebook seemed unlikely, with interviewees stating they would be uncomfortable connecting with employers on what they deemed a personal site:

> I would never use Facebook for professional reasons . . . [It] is more a site for friendship-based interactions.
>
> I don't think it's right to have employers mixed with friends.

Others disagreed, stating that although professional use may become more common, using Facebook socially was likely to continue, just perhaps more privately. One interviewee noted that the development of new features aimed at hiding information from unwanted viewers (e.g. different Friend groups) makes it easier and safer for users to continue sharing information freely. Enabling users to target disclosures towards specific audiences is beneficial as '[it will] give you the freedom to say what you want more' and help enhance communication between users while protecting their privacy.

Discussion

Results from the questionnaire and semi-structured interviews were largely consistent with earlier research, yet additional concepts emerged during analysis, particularly about the separation of personal and professional lives (online and offline), the active role played in restricting information disclosures, and the potential impact of employer surveillance.

SNSs may be 'blurring the boundaries between the personal and professional' (Donelan et al., 2009: 94). However, the data outlined in this paper indicates that SNS users take active measures to separate different aspects of their online lives. They strive to maintain boundaries between their social and professional online interactions (McDonald and Thompson,

2016). Smith and Kidder (2010) note that their online image may not be one which applicants wish to show employers. Participants in this research seem to be aware of this and are taking measures in order to ensure that employers only see their professional personas.

It was clear in the interviewee data that while Facebook was used for interacting with friends, Twitter and LinkedIn were deliberately employed for professional purposes. Professional use of SNSs was not as widely established amongst questionnaire respondents, possibly due to the partiality towards Facebook use (98% of respondents reported use), a site highly focused on social interactions. Many questionnaire respondents were against SNS checks simply because they wanted to maintain a separation between their private and professional lives, both online and offline. Questionnaire respondents reported using SNSs to gather/share information related to professional interests; however, very few engaged in active professional networking. In this regard, interviewees cited the availability of personal information and their discomfort with allowing managers/co-workers with whom they had no social relationship to access such information.

Information disclosure and privacy behaviours

Questionnaire respondents demonstrated caution when sharing personal information, with most posted information restricted to friends, or, as in the case of highly personal/sensitive information, hidden from view or omitted altogether. Overall, respondents treated different information in different ways, suggesting that they are utilising more comprehensive privacy settings allowing them to specify the audience for each piece of information. Respondents were also generally aware of who could access different pieces of information, suggesting that most of these users are, or believe they are, protecting their information. Earlier research noted the tendency for SNS users to allow access to information indiscriminately. This was not the case amongst current participants, with most respondents reporting that they allowed only known individuals to access their information, while some interviewees reported placing additional restrictions on accepted Friends. Students are much more active users of social network sites (across almost the whole range of activities such as posting or commenting) than employed or retired people. They are also more active in their use and checking of privacy settings. Young people overall are more likely to have acted to protect their privacy (Blank, 2014; Dutton et al., 2013).

Online privacy was considered important by participants; interviewees, in particular, reported that privacy maintenance was highly important on SNSs which contained personally-orientated information, therefore privacy settings were a necessity. In contrast to earlier research by (Christofides et al., 2009), interviewees reported restricting their information sharing online. However, they also noted that excessive information disclosure and careless privacy behaviours can be promoted by sites such as Facebook. As outlined below, interviews indicated adaption to these contexts by taking an active role in how and to whom information is made available.

Separate audiences and restricted information

As well as separate uses given to different SNS, interviewees also wished to separate the audience of their different profiles, restricting employers to their more professionally-orientated profiles while keeping their Facebook profiles amongst chosen friends. As a result, they kept Facebook profiles private, while leaving other profiles open to the public in order to extend the reach of professional information. LinkedIn, for example was clearly understood as a tool for professional networking that required a professional presence. Despite the opportunity for linking different SNS platforms, participants maintained a separation between SNS profiles, and, perhaps, as noted by interviewees, a separation between their professional and social identity. What was of most concern was the possibility of access/distribution of personal information by unknown/unauthorised parties, and the potential resulting harm to their safety/well-being. The possibility of employer scrutiny of SNSs was not widely reported amongst questionnaire respondents, with only 7.4% reporting this as a general concern, suggesting that, compared to other possible risks, it is not a high level of concern.

Privacy settings were widely used; however, most respondents restricted information sharing, indicating that they did not rely completely on the websites. They were aware that privacy settings were prone to failure, and instead preferred to rely on their own instincts to prevent leaks of personal/sensitive content. It was noted that privacy settings were often overly complicated and subject to frequent change, so it was difficult for users to completely ensure that posted information was secure.

The information made available by SNSs regarding privacy does not appear to be widely used, with only around one-quarter of questionnaire respondents reporting to read privacy policies. Additionally, only two interviewees reported reading the privacy policy.

This does not lead to a disregard for personal privacy, in fact a general awareness of privacy issues makes users more vigilant. Interviewees also prefer turning to friends for advice or seeking information from unrelated sources such as the media and research articles. Seeking advice from friends was particularly apparent amongst less experienced users, with one interviewee reporting that she was frequently approached by friends who were concerned over who could access their information. Although many interviewees complained about the lack of information provided by SNSs, one noted that the role played by these sites in informing users was small, as users choose to overlook the already available information.

All participants were aware of the possibility of SNS checks conducted by employers, with mixed responses regarding impact on future SNS use. For most respondents, this was reported as likely to have an impact, with some indicating that their future use of SNSs would be more cautious as a result of this. Others reported being prepared to make changes to online activities in the event of SNS checks. Interviewees preferred checks of more professionally-focused profiles but were satisfied with general checks of their Facebook profiles, as they believed that employers would be unable to access potentially damaging content. However, interviewees reacted negatively to more invasive checks of Facebook profiles, reporting that this would likely impact their opinion of the company in question. This may be considered an example of a 'chilling effect' in SNS use with a negative attitude towards the relevant company a manifestation of this effect in the external (offline) environment. The idea of a chilling-effect (that is, behaviour modification) can be evidenced in 'real life' behaviours but also is a focus of investigation in the online world and can lead to a resistance to using everyday technology (Sidhu, 2007), for example after the NSA/PRISM surveillance revelations in 2013 (Penney, 2016). However, this may be to some extent ameliorated by users' understanding of how to control social media to their advantage, e.g. in presenting a positive image of themselves to potential employers, as evidenced earlier, as well as a measured acceptance of the behaviour of organisations and SNS providers. The user has the power to control and indeed utilise these effects and current participants were conscious of this.

Participants also reported that employer checks of online profiles would cause them to be more cautious when using SNSs. Sites such as LinkedIn and Twitter are preferred for professional purposes, but users reported that they were prepared to make changes to their Facebook profiles, e.g. altering their current profiles or creating new ones in order to impress employers. Clark and Roberts (2010) identified this as a key problem with employer surveillance of SNS profiles, significantly effecting future use, and weakening SNSs as a medium of communication. However, this need not be the case – participants in this study noted that social communication would remain prominent on SNSs; it may just alter and evolve. Uses for different SNSs have already become established and are not likely to significantly change in the future, with a large proportion of the questionnaire respondents and interviewees reporting that their use of SNSs, though dependent on changes in SNSs and personal circumstances, would remain similar in the future.

Both user behaviour and SNS interface are likely to evolve in the face of employer surveillance, as it is in the interests of both to adapt to this practice. As noted by one interviewee, Facebook is has introduced new features that would prove beneficial for individuals seeking to continue using SNSs for social interaction while facing the possibility of SNS checks; and in the light of very recent negative publicity has rewritten its terms and conditions to make the language clearer (Kleinman, 2018).

Concerns with employer judgements of SNS information

Although research such as Morgan et al. (2010) and Strater and Lipford (2008) assert that SNS users post truthful information, interviewees noted that posted information, although generally accurate, is one-sided, and therefore, is not an accurate portrayal of the individual. Employers engaging in SNS checks may only be making judgements on an incomplete portrayal.

Employers planning to check SNSs as part of their hiring process should focus on job-related information (Madera, 2012). However, this may prove troublesome due to the unavailability of such information on certain profiles. While Twitter and LinkedIn contained information regarding an interviewee's professional experience and interests, Facebook information was related to social interactions, and did not include much reference to professional endeavours. The literature indicates that employers justify checking personal profiles to confirm information provided in applications, particularly education/employment history. However, as low numbers reported to reveal this information to the public, the usefulness of personal profiles for this purpose is questioned. Employers must take care when scanning SNS profiles for confirmatory information, as this information may not be accessible.

Self-presentation in SNS profiles was commented on by interviewees, who noted that 'you can make yourself sound a certain way'. SNSs users can employ personal profiles as a means of representing their public persona, something which may vary considerably depending on their perceived audience (Acquisti and Gross, 2006). Interviewees reported that they took their audience into consideration to avoid negative judgements, consistent with findings from Valkenburg et al. (2006; cited in Pempek et al., 2009) which noted that SNS users posted information aimed at deriving positive feedback from their audience. The possibility of innocent information being misinterpreted by employers was also noted and was a significant concern amongst both questionnaire respondents and interviewees.

Conclusion and recommendations

In response to earlier research predicting significant changes in SNS use because of privacy concerns, and the increasingly common practice of employer surveillance, this study aimed to investigate the potential impact of SNS checks on use of these sites, and to explore possible SNS use in the future.

Several key areas were examined: use of SNSs; information-sharing behaviours; privacy concerns and behaviours; awareness of, and reactions to employer surveillance; and potential impact of employer surveillance on future SNS use. The issues arising provide an insight into individuals' attitudes towards and perceptions of privacy online, and also indicates that users are thinking critically about social media use, if necessary taking action to protect their privacy either through use of relevant privacy settings or indeed how and to whom they disclose information.

Findings are consistent with earlier research demonstrating the importance of information sharing on these sites. However, SNS users face problems in protecting their information due to fallible privacy settings, human error and a lack of clarity regarding a legal right to privacy on SNSs. Participants were aware of issues, with many reporting that they relied on their own judgement when sharing information, as opposed to depending on the SNS to protect their content.

Participants were in general aware of the possibility of employer monitoring and were not dissatisfied if they were able to maintain some control over access to information. Earlier research, highlighted the potential impact of employer checks, proposing that this practice may damage the utility of SNSs as a medium of communication. However, the data described here indicates that, while SNS checks will likely impact communication, it is not to the extent predicted, as users and SNSs themselves are finding ways to adapt to this practice, and indeed increased awareness and the beginnings of change to legalisation and best practice guidelines will all have an impact on understandings and actions in relation to privacy online.

Although over one hundred students took part in the online questionnaire, this is of course a small proportion of the entire student population, and the use of a snowball sampling method resulted in a non-random sample. As Facebook was used as one means of recruiting participants in this way, a bias toward Facebook users may also be considered a limitation. This limits the generalisability of the results; however, they do give indications of possible trends in behaviour. Based on the literature and the findings of the current study, a series of recommendations were developed for SNS users, employers engaging in SNS checks, and the websites themselves.

1. Recommendations for users: What was most apparent was the need for SNS users to be careful with what they post. Current participants advised caution when making information available online and asserted that it was the responsibility of the user to ensure the safety of their content. Additionally, for users on the brink of entering the job market, it is worth taking into consideration the possibility of creating alternative profiles to showcase professional experience and interests, while maintaining old profiles for socialising.
2. Recommendations for employers: Employers should be aware of the fallibility of online information, and refrain from taking SNS content at face value. Information posted online may be incorrect, outdated, posted without knowledge/consent, or may not refer to the correct individual, leading to inaccuracies and possible misinterpretations of information. Available information may not be relevant for employment decisions, while relevant information may be omitted/hidden from view. Employers must avoid allowing personal biases to sway their judgements. Policies and training should be established to ensure standardisation of this practice, and employers should avoid overly invasive SNS checks. Employers should also consider openness regarding hiring procedures – prior knowledge of SNS checks may increase perceptions of fairness, allowing applicants to ensure

professional information is available on their profiles.

3. Recommendations for SNSs: It is important for SNSs to continue developing website features that will help users control the information they post. The sites should continue to educate users regarding available settings and ensure that policies/guidelines are not overly complicated. Sites could ensure that the default settings are higher to protect inexperienced users who may not be aware of the measures they must take to protect themselves.

A response from one international interviewee indicated possible cultural differences in this practice. While SNS checks may be expected in the US and Great Britain, they may be less common, and possibly less acceptable, in other countries. This could make for interesting comparisons internationally.

It has been noted that that attitudes do not always lead to expected changes in behaviour. Carrying out a longitudinal study will provide more information as to how information-sharing and privacy behaviours are changing over time, and to investigate more thoroughly the impact of employer surveillance. Finally, a more wide-scale analysis into how different SNSs are treated by users could be of interest: while responses from interviewees indicated that online behaviour varied from one site to the next, due to constraints in the scope of the current project it was not possible to investigate this among a larger population.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

ACAS (n.d.) Social media - recruitment and performance management. Available at: http://www.acas.org.uk/index.aspx? articleid=3377 (accessed 31 January 2018).

Acquisti A and Gross R (2006) Imagined communities: Awareness, information sharing and privacy on Facebook. In: Danezis G and Golle P (eds) *Privacy Enhancing Technologies*. Berlin/Heidelberg: Springer-Verlag, pp. 35–58.

Amaratunga D, Baldry D, Sarshar M, et al. (2002) Quantitative and qualitative research in the built environment: Application of 'mixed' research approach. *Work Study* 51(1): 17–31.

Arcand M, Nantel J, Arles-Dufour M, et al. (2007) The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review* 31(5): 661–681.

Barnes N (2009) Reaching the wired generation: How social media is changing college admission. National Association for College Admission Counselling. Available at: http://www.nacacnet.org/publicationsresources/marketplace/discussion/pages/socialmediadiscussionpaper.aspx (accessed 31 January 2018).

Barrick MR, Patton GK and Haugland SN (2000) Accuracy of interviewer judgements of job applicant personality traits. *Personnel Psychology* 53: 925–951.

Bateman PJ, Pike JC and Butler BS (2011) To disclose or not: Publicness in social networking sites. *Information Technology & People* 24(1): 78–100.

Blank G (2014) No, digital natives are not clueless about protecting their privacy online. *The Conversation*, 12 September. Available at: https://theconversation.com/no-digital-natives-are-not-clueless-about-protecting-their-privacy-online-31654 (accessed 30 April 2018).

Brandenburg C (2007) The newest way to screen job applicants: A social networker's nightmare. *Federal Communications Law Journal* 60(2): 597–626.

Branine M (2008) Graduate recruitment and selection in the UK: A study of the recent changes in methods and expectations. *Career Development International* 13(6): 497–513.

Byrnside I (2008) Six clicks of separation: The legal ramifications of employers using social networking sites to research applicants. *Vanderbilt Journal of Entertainment and Technology Law* 10(2): 445–477.

Chen X and Michael K (2012) Privacy issues and solutions in social network sites. *IEEE Technology and Society Magazine* 31(4): 43–53.

Cho H, Lee J and Chung S (2010) Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior* 26(5): 987–995.

Christofides E, Muise A and Desmarais S (2009) Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyber Psychology & Behavior* 12(3): 341–345.

Clark LA and Roberts SJ (2010) Employers' use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics* 95(4): 507–525.

Clemmitt M (2006) Cyber socializing. *CQ Researcher* 16(27): 627–648.

De Souza Z and Dick G (2007) What explains the MySpace phenomenon? Extending the Technology Acceptance Model to explain the use of social networking by schoolchildren. In: *Proceedings of the International Academy for Information Management 22nd international conference on informatics education & research*, Montreal, Canada. Available at: http://www.sig-ed.org/ICIER2007/proceedings/what_explains.pdf.

Donelan H, Herman C, Kear K, et al. (2009) Patterns of online networking for women's career development.

Gender in Management: An International Journal 24(2): 92–111.

Dutton W, Blank G and Groselj D (2013) *Cultures of the Internet: The Internet in Britain. Oxford Internet Survey 2013*. Oxford: Oxford Internet Institute, University of Oxford.

Fidel R (2008) Are we there yet? Mixed methods research in Library and Information Science. *Library & Information Science Research* 30(4): 265–272.

Go PH, Klaassen Z and Chamberlain RS (2012) Attitudes and practices of surgery residency program directors toward the use of social networking profiles to select residency candidates: A nationwide survey analysis. *Journal of Surgical Education* 69(3): 292–300.

ICO (2017) Guide to the General Data Protection Regulation. Available at: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (accessed 31 January 2018).

Keenan A and Shiri A (2009) Sociability and social interaction on social networking websites. *Library Review* 58(6): 438–450.

Kim Y, Sohn D and Choi SM (2011) Cultural difference in motivations for using social network sites: A comparative study of American and Korean college students. *Computers in Human Behavior* 27(1): 365–372.

Kleinman Z (2018) Facebook: Cambridge Analytica warning sent to users. *BBC News*, 9 April. Available at: http://www.bbc.co.uk/news/technology-43698733 (accessed 30 April 2018).

Kluemper D and Rosen P (2009) Future employment selection methods: Evaluating social networking web sites. *Journal of Managerial Psychology* 24(6): 567–580.

Landman MP, Shelton J, Kauffmann RM, et al. (2010) Guidelines for maintaining a professional compass in the era of social networking. *Journal of Surgical Education* 67(6): 381–386.

Levashina J (2009) Expected practices in background checking: Review of the human resource management literature. *Employee Responsibilities and Rights Journal* 21: 231–241.

McDonald P and Thompson P (2016) Social media(tion) and the reshaping of public/private boundaries in employment relations. *International Journal of Management Reviews* 18: 69–84.

Madera J (2012) Using social networking websites as a selection tool: The role of selection process fairness and job pursuit intentions. *International Journal of Hospitality Management* 31(4): 1276–1282.

Madhusudhan M (2012) Use of social networking sites by research scholars of the University of Delhi: A study. *International Information & Library Review* 44(2): 100–113.

Morgan EM, Snelson C and Elson-Bowers P (2010) Image and video disclosure of substance use on social media websites. *Computers in Human Behavior* 26(6): 1405–1411.

Nosko A, Wood E and Molema S (2010) All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior* 26(3): 406–418.

Pempek TA, Yermolayeva YA and Calvert SL (2009) College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology* 30(3): 227–238.

Penney JW (2016) Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal* 31(1): 117–182.

Phipps C, Rawlinson K and Mason R (2018) Toby Young resigns from the Office for Students after backlash. *The Guardian*, 9 January. Available at: https://www.theguardian.com/media/2018/jan/09/toby-young-resigns-office-for-students (accessed 21 June 2018).

Pickard AJ (2007) *Research Methods in Information*. London: Facet.

Robles MM (2017) The debate about using social media to screen job applicants. In: *Proceedings of the Appalachian research in business symposium*, pp. 140–145.

Boone NC, USA. Available at: https://encompass.eku.edu/fs_research/108/ (accessed 31 January 2018).

Sánchez Abril P, Levin A and Del Riego A (2012) Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal* 49(1): 63–124.

Sidhu DS (2007) The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans. *University of Maryland Law Journal of Race, Religion and Class* 2: 375–393.

Slovensky R and Ross WH (2012) Should human resource managers use social media to screen job applicants? Managerial and legal issues in the USA. *Info* 14(1): 55–69.

Smith WP and Kidder DL (2010) You've been tagged (then again, maybe not): Employers and Facebook. *Business Horizons* 53(5): 491–499.

Stacey E (2017) Facebook snooping on candidates? GDPR could put a stop to that. *Personnel Today*. Available at: https://www.personneltoday.com/hr/facebook-snooping-candidates-gdpr-put-stop/ (accessed 31 January 2018).

Strater K and Lipford H (2008) Strategies and struggles with privacy in an online social networking community. *Analysis* 1(10): 111–119.

Tashakkori A and Creswell JW (2007) Exploring the nature of research questions in mixed methods research. *Journal of Mixed Methods Research* 1(3): 207–211.

Valkenburg PM, Peter J and Schouten AP (2006) Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *CyberPsychology & Behavior* 9: 584–590.

Author biographies

Deirdre McGuinness is an Assistant Librarian at William Fry Solicitors in Dublin, Ireland. She graduated from Aberystwyth University in Wales in 2013 with a Master's in Information and Library Studies. She then went on to hold

roles in the Oireachtas Library & Research Service (library and research service of the Irish Parliament), the Irish Hospice Foundation and Trinity College Dublin, before joining William Fry as their Library and Information Services Assistant in 2015. She is a member of the British and Irish Association of Law Librarians and won their Dissertation Award for her thesis – *Information disclosure, privacy behaviours, and attitudes regarding employer surveillance of social networking sites*, upon which this paper is based. She is a committee member of the Academic and Special Libraries Section of the Library Association of Ireland.

Anoush Simon is a Senior Lecturer in Information Studies at Aberystwyth University, Wales. Her research and teaching interests include the information society, social impacts of new technologies, digital and social inclusion, public libraries and social justice.

Article

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 223–228

DOI: 10.1177/0340035218785391
journals.sagepub.com/home/ifl

Privacy and libraries in the case of Japan

Yasuyo Inoue
Dokkyo University, Saitama-ken, Japan

Abstract
This essay introduces the concept of privacy from the perspective of the East Asian nation of Japan. Firstly, it provides background context to how privacy is viewed in the country; then it discusses relevant legislative approaches to the protection of privacy in Japan. It goes on to discuss privacy in relation to its relevance to libraries, illustrated with two case studies, before concluding with some suggestions as to the way forward in Japan.

Keywords
Japan, library management, privacy laws

Submitted: 14 January 2018; Accepted: 9 May 2018.

Background and context

When you visit Japan and ride on a train or subway, you may notice that people are reading books covered by paper. You know the size of the book, but you do not know the title of the book. Not all but many Japanese hesitate to show a cover of the book they are reading to strangers in public places. This gives an indication of how Japanese think of privacy as "freedom to read", meaning reading any books freely without being noticed by others. Which book you read or not is "private information". In Japanese libraries one of the most important issues is protection of people's freedom to read, that is, protecting private information.

In 2015 Japan the amended Act on the Protection of Personal Information (Japanese Law, 2017) was promulgated for approval, and in May 2017 the Amended Act (Japanese Law, 2017) came into force. This paper analyzes and discusses privacy issues in libraries, especially in public libraries, related to this Amended Act.

(Amended) Act on the Protection of Personal Information

The main purpose for the (Amended) Act on the Protection of Personal Information (Japanese Law, 2017) is the control of businesses buying and selling various lists of personal information. As the World Economic Forum mentioned in 2011, "personal data is becoming a new economic 'asset class', a valuable resource for the 21st century that will touch all aspects of society" (World Economic Forum, 2011). The amendment of the Act on the Protection of Personal Information resulted in the following changes (Japanese Law, 2017):

- The centralization under one Personal Information Protection Commission's control of the various agents and governmental offices previously responsible for the supervision of data protection;
- The definition of "personal information" was clarified;
- Setting up the rule to change from using anonymous processed personal information to limited particular person;
- Measures against private businesses which are providers of personal information data for sale, and both public and private sectors must provide reports about their business to the Personal Information Protection Commission on duty;

Corresponding author:
Yasuyo Inoue, Dokkyo University, 1-1 Gakuen-machi, Souka-shi, Saitama-ken 3400042, Japan.
Email: yinoue@dokkyo.ac.jp

- Abolishment of the exemption for private companies or organizations with a small quantity of personal information (prior to this amendment, companies and organizations holding personal information for fewer than 5000 individuals did not need to report to the Government agency);
- Agencies which utilize personal information must now notify the Commission, and the Commission must announce that to the public;
- Regulations on the limitation and exemption of providing personal information to third parties outside of Japan.

Personal information and data have become a business resource. To deal with this in 2016, the Basic Act on the Advancement of Utilizing Public and Private Sector Data (Japanese Law, 2016) was approved and enforced. Thus the (Amended) Act on the Protection of Personal Information (Japanese Law, 2017) tries to set up the rules and obligations in the case of utilizing "big data" such that business operators can process personal information anonymously. This raises the question of whether personal information can be processed anonymously and confidentially.

Legal definition

Article 2 of the Act on the Protection of Personal Information (Japanese Law, 2017) amended the definition of "personal information" to mean "that information relating to a living individual" and "containing a name, date of birth, or other descriptions etc.", "that cannot be recognized through the human senses". Article 2 of the Act on the Protection of Personal Information added "meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic, magnetic or other form)". Also this Article 2 explains more in detail about the meaning of "individual identification code": that is, personal information includes formats such as DNA, face composition, iris, voiceprint, physical appearance when walking, vein of hands/fingers, finger print, palm print, and so on. Various public identified numbers are also considered "individual identification code" including the basic pension number or individual number set forth in Article 2 of the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Japanese Law, 2016).

In addition to those, the Act on the Protection of Personal Information (Japanese Law, 2017) defines special care-required concerning personal information, meaning:

> personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.

Among this personal information requiring special care is "the fact that an arrest, search, seizure, detention, institution of prosecution or other procedures related to a criminal case have been carried out against a principal as a suspect or defendant" (Article 2.4 of the Cabinet Order). This could be considered as an example of the "right to be forgotten" (Mantelero, 2013).

Exclusion

Article 76 of the Act on the Protection of Personal Information (Japanese Law, 2017) excludes a number of institutions and individuals from its provisions but not libraries.

Excluded institutions and individuals include:

1. Broadcasting institutions, newspaper publishers, communication agencies and other press organization (including individuals engaged in the press as their business). These are excluded so that those press can function;
2. Professional writers are also excluded so that they can function;
3. Universities and other organizations or groups engaged in academic studies, or a person belonging thereto, so that they may conduct research;
4. Religious bodies for use in a religious activity;
5. Political bodies for use in a political activity.

Therefore, libraries, public libraries in particular, are not excluded from the provisions of the Act on the Protection of Personal Information (Japanese Law, 2017), and need to handle personal information data as specified in the Act. Prior to this legislation, librarians in Japan discussed and implemented measures to protect personal information for users' freedom to read. There has been much discussion in the library sector relating to the management of personal information since the Japan Library Association (JLA) proclaimed the Statement on Intellectual

Freedom (JLA, 1954, rev. 1979) and the Code of Ethics for Librarians (JLA, 1980), and since then libraries have been actively trying to protect personal information.

The Act and libraries

Japanese libraries have largely defined personally identifying information and data as consisting of circulation records, data on overdue/lost library materials, records of reference services, data on reserved materials, inter-library-loan records, and documents on photocopy services. These data have been regarded as users' personal identification information in the same way that name, date of birth, or other descriptions etc. are regarded as personal identification information data by the Act on the Protection of Personal Information (Japanese Law, 2017).

Article 3 of the Japan Library Association's Statement on Intellectual Freedom in Libraries (JLA, 1954, rev. 1979), guarantees the privacy of users. This means "what book a particular person has read or is reading shall be regarded as the privacy of the reader. Libraries shall not reveal a reader's record of reading". But, if the business operators insist that they can handle library users' personal information anonymously under this Act on the Protection of Personal Information (Japanese Law, 2017), and demand that libraries provide access to users' data, what are libraries to do?

As far as any local public libraries are regarded as part of local government authority, full-time positioned librarians come under Article 34 of the Local Public Service Officers' Act (Japanese Law, 1950a), which requires that they keep secret whatever they learn about an individual through their work. Well-trained professional librarians recognize the Statement on Intellectual Freedom in Libraries (JLA, 1954, rev. 1979), and also Article 3 of the Code of Ethics for Librarians, "a librarian should respect the confidentiality of each library user" (JLA, 1980).

Yet when the Committee on Intellectual Freedom of the Japan Library Association undertook a national survey on intellectual freedom in public libraries (JLA, 2013) in 2011, more than 60% answered "yes" when they were demanded by local governmental authority or others to open users' reading records without a warrant issued by a competent judicial officer, as provided in the Constitution (Article 35). Can librarians protect users' personal information to read books freely?

Discussion points

Risk of management by the private sector

There are two trends impacting privacy issues in Japanese libraries: (1) outsourcing the management of public libraries; and (2) the use of part-time staff.

Since the Local Autonomy Law (Japanese Law, 1947) was revised in 2003, and with the Act on Promotion of Private Finance Initiative (Japanese Law, 1999) (approved in 1999), local government authorities have contracted the management of roughly 10% of all public libraries to non-profit organizations (NPO) which are organized by library volunteers, and private sectors including local bookstores and nationwide book and audio-visual material rental chain stores. These private sector management firms are not obliged to protect user privacy.

Public officers are obliged to keep secret whatever they know through their daily work under Article 34 of the Public Service Officers' Act. As mentioned above, library workers are obliged to respect and keep secret users' privacy under the JLA's the Intellectual Freedom Statement (JLA, 1954, rev. 1979) and the Code of Ethics for Librarians (JLA, 1980). As far as library workers are not public officers, what they are obliged to do is provided for by this Statement and the Code of Ethics, now including the IFLA Statement on Libraries and Intellectual Freedom (IFLA, 1999) and the IFLA Code of Ethics for Librarians and other Information Workers (IFLA, 2012). Nevertheless, there have been cases and issues relating to library management and protection of users' personal information. Here, two cases are analyzed and discussed.

Case A: Local public library managed by a private business company (s.n., 2012)

In 2014, the management of the Takeo city local public library was privatized and re-opened by one of the nationwide book and audio-visual material rental chain stores. At the time of the re-opening, the new management company asked residents and others who wanted to use the library to re-register as a library user. The new library card included the company's "point card" which can be added to whenever a user borrows a book or other materials from the library. Librarians from other cities complained, so the company changed the registration system offering users the right to choose a library card with or without the "point card" as there is insufficient explanation of the privacy implications of the card.

Few people understand the implications of using a "point card" as their library registration card. The management company explained that users can get

more points if they borrow more books, and then users can buy any goods with those points at the bookshop attached to the public library. The library does not offer new editions of magazines or newly-published books. If a user wants to read a new one, they must buy these at the shop attached to a coffee shop inside the library. This marketing technique not only sells newly-published books or magazines at the library bookshop but also gathers data from library users. How can this private business undertake this marketing approach?

This is because of the Takeo city mayor's policy at the time of the contract, and also the content of the local government regulation on the protection of personal information. The legal definition of the personal information regulation at this city is too simple, and guidelines on protecting personal information based on the Statement on Intellectual Freedom at Libraries (JLA, 1954, rev. 1979) insisted on by the library staff were not regarded as an important issue. At this library, most of the library staff are contracted part-time workers, and they are in an unstable working situation. They faced difficulties clarifying and persuading the new management authority of the mission of public libraries.

Article 17 of the Library Law (Japanese Law, 1950b) in Japan, states that publicly-funded libraries cannot demand any fee from users. Therefore, the private rental book shop company managing the public library attached a bookshop and café as a means of gaining profit and gathering personal library usage information as a valuable data resource. The company continues expanding its management of public library businesses, and keeps collecting users' personal information, including data on reading. The company does not have any rules or guidelines, or code of ethics on protecting personal information, but under the new amended Act on Protection of Personal Information (Japanese Law, 2017), it is required to have these and make them available to the public.

Case B: Leaking personal information by outsourcing library systems (JLA, 2011)

The second case occurred at a local publicly-funded library and involves two issues: (1) a library director providing users' registered records to the police, and (2) duplicating users' registration and circulation record to other libraries which can be seen by other library staff.

In 2010 the library found their library system was jammed because too many people were searching for books or other information through their OPAC via the Internet at the same time. No library staff members were able to understand the library computer system sufficiently to fix it. The library sought outside assistance from the system vendor, but they were no help. Assuming the system had been hacked, the library director then called the local police. But in fact, the problem was caused by automatic searching by a library user. The library considered that this was done with ill-intention and accused the person of interference with the library functions. The library user was arrested even though the user had no intention to hack. He was kept in custody for a few days and was released on bail.

Because of lack of knowledge of their own system and the failure of the vendor to advise appropriately, the library director released personal information on a user in violation of both the Statement and the Code as a professional librarian. When investigating this case, it was found that the library system vendor had duplicated the library computer system with the library user's registration record including name, address, and other personal information along with circulation records into their library systems, thus failing to protect personal identification information and user privacy.

Conclusion and recommendation

These cases raise several issues and recommendations for dealing with them. Lack of training is a major issue. Librarians need library computer system training. Librarians also need sufficient and consistent training in user privacy issues to recognize and understand users' privacy related to the Intellectual Freedom Statement at Libraries (JLA, 1954, rev. 1979) and the Code of Ethics for Librarians (JLA, 1980). This training should be made available to all library workers including information workers and outsourcing agency staff as well as librarians.

Lack of a clear local user privacy policy and guideline is also an issue. Libraries need to establish rules or guidelines on users' privacy. The trend of library management outsourcing raises a number of issues. If local authorities outsource library management they should build privacy requirements into the contract and further mandate that contracting businesses share information on these measures with the public. Contracting businesses should also be required to train their workers on library users' privacy.

As a result of these cases, the Intellectual Freedom Committee of JLA suggested several actions (JLA, 2011):

- If a library is considering whether personal information should be given to an outside

person or sector, especially to police or other authorities, the potential action must be thoroughly discussed, and, as appropriate, advice sought from the local government's department on public information scrutiny or an attorney belong to the local government;
- Libraries should provide staff with up-to-date training on their library systems;
- Local authorities and any library outsourcing library functions to the private sector must be sure the company has guidelines or a code of ethics protecting personal information in libraries.

In addition, libraries should establish rules or guidelines on protecting personal information, and make these rules open to the public. Although the definition of personal information in the Act on the Protection of Personal Information (Japanese Law, 2017) is different from the definition typically used by libraries, each library should discuss this and make its own rules or guidelines. Finally, local government regulations protecting personal information should include library data, too.

In Japan, we cover books read when we read them in public places. This demonstrates the value placed on reading privacy and corresponds with the library and librarians' protections for readers' freedom to read. Anyone working in libraries should recognize the mission of librarians, that is, for whom the library is working. The library, especially the public library, is the gateway to a democratic society where people gather information, read books and access information in many formats, gain knowledge, and discuss ideas with others without observation or surveillance.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

IFLA (1999) *Statement on Libraries and Intellectual Freedom*. The Hague: IFLA. Available at: https://www.ifla.org/publications/ifla-statement-on-libraries-and-intellectual-freedom (accessed 5 September 2017).

IFLA (2012) *Code of Ethics for Librarians and other Information Workers*. The Hague: IFLA. Available at: https://www.ifla.org/faife/professional-code-of-ethics-for-librarians (accessed 5 September 2017).

Japan Library Association (1954, rev. 1979) *Statement on Intellectual Freedom in Libraries*. Tokyo: Japan Library Association. Available at: https://www.jla.org.jp/portals/0/html/jiyu/english.html (accessed 5 September 2017).

Japan Library Association (1980) *Code of Ethics for Librarians: Approved at the Annual General Conference in June 1980*. Tokyo: Japan Library Association. Available at: https://www.jla.org.jp/portals/0/html/ethics-e.html (accessed 5 September 2017).

Japan Library Association (2011) *Okazaki-shi no toshokan system wo meguru jiken ni tuite*. Tokyo: Japan Library Association. Available at: http://www.jla.org.jp/portal/0/html/jiyu/okazaki2003.html (accessed 5 September 2017).

Japan Library Association (2013) *National Survey on Intellectual Freedom at Public Libraries in Japan, 2011*. Tokyo: Japan Library Association.

Japanese Law (1947) *Local Autonomy Law*. Tokyo: Japan Government. Available at: http://nippon.zaidan.info/seikabutsu/1999/00168/contents/095.htm (accessed 5 September 2017).

Japanese Law (1950a) *Local Public Service Officers' Act*. Tokyo: Japan Government. Available at: http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=325AC0000000261 (accessed 5 September 2017).

Japanese Law (1950b, rev. 1985) *Library Law* (Law No. 118). Tokyo: Japan Government. Available at: http://www.jla.or.jp/portals/0/html/law-e.html (accessed 5 September 2017).

Japanese Law (1999) *Act on Promotion of Private Finance Initiative* (Act No. 117 of July 30, 1999). Tokyo: Japan Government. Available at: http://www.japaneselawtranslation.go.jp/law/detail/?id=103&vm=04&re=01&new=1 (accessed 5 September 2017).

Japanese Law (2013) *Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures* (Act No. 27 of May 31, 2013). Tokyo: Japan Government. Available at: http://www.japaneselawtranslation.go.jp/law/detail/?id=2755&vm=04&re=01&new=1 (accessed 5 September 2017).

Japanese Law (2016) *Basic Act on the Advancement of Utilizing Public and Private Sector Data* [Tentative translation] (Act No. 103 of December 14, 2016). Tokyo: Japan Government. Available at: http://www.japaneselawtranslation.go.jp/law/detail/?id=2871&vm=04&re=01&new=1 (accessed 5 September 2017).

Japanese Law (2017) *Act on the Protection of Personal Information* [Tentative translation] (Act No. 57 of May 30, 2003, amended in 2017). Tokyo: Japan Government. Available at: http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&vm=04&re=01&new=1 (accessed 5 September 2017).

Mantelero A (2013) The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review* 29(3): 229–235.

s.n. (2010) Kojin jouhou ga ryuushutu toshokan system ni huguai cyber kougeki-mondai mo shazai. *Nihon-Keizai-Shinbun*, 1 December.

s.n. (2012) Minkan itaku saarani sinka TSUTAYA toshokan saga ni heikan enchou point huyo. *Nihon-Keizai-Shinbun*, 23 July.

The World Economic Forum (2011) *Personal Data: The Emergence of a New Asset Class*. Geneva: WEF. Available at: http://www.weforum.org/reports/personal-data-emergence-new-asset-class (accessed 5 September 2017).

Author biography

Yasuyo Inoue is Professor of Library Science at Dokkyo University, Japan. She is currently executive advisor for IFLA/FAIFE and a former member of the JLA/Intellectual Freedom Committee. Her recent publications include articles for *Library Management*, *IFLA Journal* and the *Revue de l'Association des Bibliothecaires de France; Bibliotheque*, and a chapter in *The Ethics of Librarianship: An International Survey* (ed. RW Vaagen, 2002) She has also published more than 50 professional articles and books in Japanese. Professor Inoue's main research field is in children's and teens' library services, especially related to intellectual freedom issues.

Article

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 229–239

DOI: 10.1177/0340035218778054
journals.sagepub.com/home/ifl

Privacy, obfuscation, and propertization

Tony Doyle
Hunter College, New York, USA

Abstract

As our digital wake ripples out, big data is standing by to ride it, applying its analytics to make unnerving inferences about our characters, preferences, and future behavior. This paper addresses the challenge that big data presents to privacy. I examine what are perhaps the two most promising attempts to repel big data's attack on privacy: obfuscation and the "propertization" of personal information. Obfuscation attempts to throw data collectors off our digital trail by confusing or misleading them. Propertization calls for treating personal information as intellectual property and would require that data holders compensate data subjects for any secondary use. I try to show that both defenses largely fail. I conclude that privacy is a lost cause and that we should call off the attempts to defend it from the moral point of view. I close with some thoughts about what this all means for libraries.

Keywords

Autonomy, big data, information technology, obfuscation, privacy, propertization

Submitted: 27 December 2017; Accepted: 25 April 2018.

Introduction

Big data, with its massive collection, thorough aggregation, predictive analysis, and lightning dissemination of personal information, has produced previously unfathomable benefits and insights. It is fomenting a Copernican revolution in the social sciences (Mayer-Schönberger and Cukier, 2013; Stephens-Davidowitz, 2017). It has also been a boon for detecting credit card fraud and money laundering, monitoring traffic flows, refining digital translation, matching consumers with useful products and services, improving diagnoses, and tracking public health trends (Acquisti, 2014; Barocas and Nissenbaum, 2014a; Mayer-Schönberger and Cukier, 2013; Schneier, 2015). In libraries, the user experience can be enhanced through "personalization," in which items are recommended based on a user's previous interests, on what other users with similar interests have sought, or on friends' preferences (Pekala, 2017). Analysis is replacing intuition; the gut is yielding to algorithm.

But big data is bearing down on privacy. In what follows, I will use the expression *big data* to cover not just the collection but also the analysis of data. After all, it is the monumental harvesting in combination with ever more sophisticated analysis of it that poses the real threat to privacy.[1] Once upon a time there was too much data to save. No more: Storage costs have long been in free fall. These days, even if a stockpile's utility is not immediately apparent, data holders will warehouse it in the reasonable hope that uses will emerge (Angwin, 2014; Mayer-Schönberger and Cukier, 2013; Schneier, 2015). Gone, too, is the default protection of file cabinets, paper archives, and stand-alone computers. Today, much of that information is available from a single point. Once aggregated, the trove can yield novel and uncanny inferences about our activities, preferences, commitments, aspirations, vulnerabilities, and future behavior. This bounty can then travel widely in a flash. If not quite an open book yet, our lives are anything but a locked diary.

Corresponding author:
Tony Doyle, Hunter College Philosophy Department, Hunter College Library, 695 Park Avenue New York 10065, NY, USA.
Email: tdoyle@hunter.cuny.edu

How should we respond? Notice and consent (or choice), once the great market-based hope for privacy protection, has failed signally. The idea is that optimal privacy is reached when informed individuals agree, or not, to the collection and subsequent use of their data (Schwartz, 2004). However, notices that attempt to cover all contingencies are unreadably long and would gravel even experts. For instance, a 2008 study showed that the average American would need 244 hours to plow through the privacy policies of all the websites he accessed in a year, at an opportunity cost nationwide of $781bn (cited in Landau, 2015). Pared down, accessible statements, on the other hand, strip away crucial detail (Nissenbaum, 2011). Either way, refusing to accept the terms means that we cannot use the service. Third, much of the value of information comes from secondary uses that not even data scientists can anticipate at the time of collection, making nonsense of consent even when people comprehend the statements (Barocas and Nissenbaum, 2014a; Meyer-Schönberger and Cukier, 2013). Fourth, by agreeing to share information, say, about my health, brokers can proceed to make non-trivial inferences about the health of others not in the data set but who are otherwise akin in age and habits (Acquisti et al., 2016; Barocas and Nissenbaum, 2014b). I say more about this below.

Legislation restricting what data holders can do with personal information might offer some hope. However, as Finn Brunton and Helen Nissenbaum point out (2011 and 2015), the law will inevitably lag behind the breakneck innovations of privacy-threatening technology, and data brokers and their clients are likely to have undue influence on how legislation is crafted and how vigorously it is enforced. Inadequate, too, are measures like the US Federal Trade Commission's Fair Information Practices (FIPs) of 1973. These principles forbid secret record-keeping and the unauthorized secondary uses of personal information, both of which are routinely violated. They also give data subjects the right to correct any errors in their dossiers. However, if people do not know what records about them exist, this protection comes to nothing. Anyway, errors are not the main problem; harmful inferences from accurate information are. In addition, the FIPs propose to make data holders responsible for any harm resulting from misuse of data. But the harms in question, which I discuss below, are generally cryptic and amorphous, thwarting detection and frustrating enforcement.

That leaves two far more plausible responses to the assault of big data: obfuscation and propertization. Obfuscation attempts to shield privacy by producing plausible but "misleading, false, or ambiguous data" about a person, "with the intention of confusing an adversary or simply adding to the time or cost of separating good data from bad" (Brunton and Nissenbaum, 2011). Propertization proposes treating personal information as a kind of intellectual property and then compensating data subjects for its use. Ideally, obfuscation and propertization both will allow the rest of us to determine how much privacy we want to retain. I deal with each in turn, concluding that neither will seriously shelter privacy from big data's plunder. First, though, I would like to say a bit more about privacy and about how big data threatens it.

Privacy

I will pass on defining *privacy*, since any definition that I offer is bound to be open to plausible counter-examples. For the sake of discussion, I will follow Helen Nissenbaum's (2010) focus on the context-bound, morally permissible flow of personal information, which she calls "contextual integrity." I will accept her suggestion that sound privacy protection is a function of whether the flow of information follows applicable, context-bound norms or "transmission principles." Each social context comes with its own set of norms. Thus, the norms governing, or constraining, the flow of information differ according to whether the context is, say, doctor-patient, teacher-student, employer-employee, or friend-friend. Transmission principles include *consent*, *confidentiality, reciprocity, notice,* and *desert*. For any bit of personal information that passes hands we need to ask the following questions:

- What is the information about?
- Who is it about?
- Who receives it?
- Under what circumstances?

When the appropriate transmission principles are adhered to, contextual integrity is preserved, otherwise not. Violations of contextual integrity are prima facie wrong; that is, they alert us that the flow of information in question raises serious, though not conclusive, moral reasons for not engaging in the practice. For instance, confidentiality in the context of healthcare means that my doctor is forbidden from sharing information about my health with my employer or *The New York Times* but is free to pass it along to my insurance company or appropriate specialists (Samuelson, 2000). Reciprocity reigns with close friends but not with one's doctor. If I ask a good friend about his health, it can be appropriate for him to ask me about mine in response. By contrast, although my doctor deserves an honest account

in response to her questions about my health, it would obviously be out of place for me to inquire about hers (Nissenbaum, 2010)!

Nissenbaum proposes contextual integrity in response to the radical alterations in the flow of information that digital technology has wrought. Specifically, problems arise when information collected for one purpose—for example, from an app that monitors exercise patterns—is used for other purposes, like determining car insurance rates or making hiring decisions. Contextual integrity implies that it is impossible to say beforehand whether a given piece of information is private or sensitive, on the one hand, or public or non-sensitive, on the other. Context gets the last word. New Year's Eve snapshots of me with lampshade may reasonably be shared among my family and closest friends but not with my boss or my students. Similarly, no information is inherently public. It all depends on who gets it and how they handle it once they do. That is, it is strictly a matter of the context in which the information flows. That I invariably buy black T-shirts and whitening formula toothpaste might seem non-sensitive, but the pattern might slot me with reckless drivers and boost my premiums, despite my own perfect driving record. My stroll down Main Street yesterday might seem public if anything does. After all, it was broad day, hundreds saw me, and I wore no disguise. However, the presence of face-recognizing surveillance cameras there can still violate contextual integrity. First, I might not even be aware of the cameras (*notice*) or, if I am, know nothing about the fact that the information gleaned can be combined with still more information about me and relevant others and then widely disseminated (*notice* again). Second, even if I am wise to all this, I am not given the chance to say yes or no to the capture and subsequent use of the information so gathered (*consent*). Big data menaces privacy because it regularly transgresses time-honored constraints regarding who should get certain information, under which circumstances, and what they can do with this information once they have it. In fact, Nissenbaum's theory might almost be called *beyond privacy,* given her emphasis on morally appropriate information flow. Consider the fact that people who own Harley-Davidson motorcycles tend to have lower than average IQs (Stephens-Davidowitz, 2017). Prospective employers could use that information to exclude qualified candidates from the interview pool. It is not clear that the victims' privacy has been violated. Still, contextual integrity has been breached, since information gathered for one purpose has been used, without notice or consent, for another purpose, to the data subjects' detriment. Anyway, if we look at enough characteristics, we are bound to find some that happen to correlate with traits like IQ (Stephens-Davidowitz, 2017).

The foregoing implies that privacy is a normative concept, which raises the question, Why value it? My answer is that it tends to promote autonomy (see Cohen, 2000). Autonomy means being able to make choices, free of coercion or manipulation, in the light of one's own considered conception of the good life. Autonomy, for its part, promotes well-being by enabling us to increase our opportunities and advance our projects (Tavani and Moor, 2001). Commercial tracking, monitoring, and profiling are bad insofar as they tend to be inimical to privacy and thus to autonomy. People are generally better off when they have more rather than less of both. When information technology threatens them, general well-being is undermined. Privacy matters.

Big data's revelations: Further examples

Big data's phenomenal success comes from taking piles of data collected for one purpose, for example the location information needed to route your calls or texts, and applying them to myriad, apparently unrelated, secondary purposes, like predicting where you will likely be next week at this time. Big data's trick is to merge discrete and apparently trivial details from a person's life into a coherent and potentially privacy-threatening whole that is greater than the sum of its parts (Mayer-Schönberger and Cukier, 2013; Nissenbaum, 2010). This process enables data holders to discriminate ever more finely among people to arrive at the optimal decision, from the former's point of view, about how to treat you and me at a given time (Rule, 2007). For instance, since the early 1990s insurers have used credit scores to figure out who to write policies for and what to charge for the policies they do write, since people with bad credit are significantly more likely to make claims than those with good (Rule, 2007). More recently, data miners have honed their technique to reveal, for instance, that folks who buy cheap motor oil, Chrome-Skull car accessories, and hang out in the local bar, tend to have bad credit and presumably are bad insurance risks as well. This cohort's mirror image are those paragons who buy home carbon monoxide sensors, snow roof rakes, felt feet for their furniture, and premium bird seed (Duhigg, 2009; Mayer-Schönberger and Cukier, 2013).

That's not all. As Cathy O'Neil (2016) amply documents in *Weapons of Math Destruction*, it turns out that just about any data is credit data. In the United States, it is illegal to use credit scores without

subjects' consent. Lacking legal access to the reports themselves, data handlers have helped themselves to . . . you name it: zip codes, purchases, places shopped, Internet surfing patterns, or having friends—real or social media—who meet certain criteria. With this information, data handlers can concoct an e-score, a data-rich stand-in for creditworthiness (Mayer-Schönberger and Cukier, 2013; O'Neil, 2016). E-scores enable data holders to sidestep consent for access to credit scores. Creditworthiness, or its e-score facsimile, in turn substitutes for other virtues like trustworthiness and dependability on the one hand, or for a multitude of sins on the other, whether one is guilty of them or not. One's creditworthiness, real or apparent, can then be used to determine whether one gets a job, a loan, an apartment, or, of course, insurance (and at what rate). In some parts of the United States, creditworthiness counts for considerably more than driving record in determining car insurance rates. O'Neil (2016: 165) adduces Florida, where in 2014 "adults with clean driving records and poor credit scores paid an average of $1,552 more than the same drivers with excellent credit and a *drunk driving conviction*." All of this proceeds, in most of the United States at least, with near impunity, despite the fact that one's credit rating or e-score can slip or tumble for all kinds of reasons that have nothing to do with bad behavior or a weak character, like a devastating accident or serious illness.

The apparently innocuous data that we generate as we go through the motions is more or less up for grabs, and in critical mass it enables data holders to categorize us according to race, ethnicity, political views, and sexual orientation, as well as according to more specific criteria like *gambler*, *smoker in the house*, *adult with elderly parents*, and *adult with wealthy parents* (Singer, 2013). The categorization affects the ads or job offers we see online, the products and prices we are offered there, and the quality of service we receive in a call center (Angwin et al., 2017; O'Neil, 2016).

This is the panoptic sort that Oscar Gandy (1993) warned of long ago. The techniques of big data permit the classification of people based on "their estimated presumed economic or political value" (p. 1). Big data's ability to do so has improved dramatically since Gandy wrote, thanks to those plummeting storage costs, greatly expanded networks, and ever-more sophisticated techniques of re-jiggering data, from which precise, surprising, and profitable inferences can be made about you and me. Gandy (1993) calls the panoptic sort a "difference machine," a "discriminatory technology," that "allocates options and opportunities" based on personal characteristics (pp. 15 and 17). The sort is "an integrated system that is involved in the identification, classification, assessment, and distribution of individuals to their places in the array of life chances" (Gandy, 1993: 35). In other words, it has a great deal to say about the odds that a person has of living a good life. The terms of the exchange are set by data holders and their clients. Nearly all of this happens without data subjects' consent or even awareness of what is collected, who it is being shared with, or what those third parties are doing with the information once they have it (Gandy, 1993). They can see us, but we can't see them. The new panopticon makes Bentham's prototype seem quaint.

Again, big data is all about effective discrimination: Businesses quite reasonably want to know both who to seek out and who to avoid. The reward for effective discrimination is increased profit (Rule, 2007; Schneier, 2015). As we just saw, the canny third party need not have any information about our actual characteristics. Information about those who are otherwise like us suffices to sort us in all kinds of ways. For instance, frequenters of gambling sites might be a bad risk for a bank loan (Steel and Angwin, 2010). More subtly, a detailed picture of one's health can emerge without any third party access to one's medical records, dodging consent. Obesity, a handy proxy for a suite of health risks, can be reliably inferred from the following: regular fast food dining, frequent online shopping for clothes, being a childless minivan owner, and subscribing to premium cable (Walker, 2013). One data broker was able to identify people who were probably arthritic by looking at cat ownership, a preference for jazz, and participation in sweepstakes (Walker, 2013). Creditworthiness, exercise habits, recent websites visited, and TV watching habits might even be interchangeable in some cases with blood and urine samples as a predictor for heart disease, high blood pressure, diabetes, or depression (Mayer-Schönberger and Cukier, 2013; Schneier, 2015). The same goes for race: Zip code coupled with mother's level of education say a lot about it (Ohm, 2014). So much for consent and the control over personal information that it was supposed to provide. In fact, the production of most new information about me can now proceed without my consent and even without information about the relevant trait at all (Mai, 2016).

Obfuscation

Finn Brunton and Helen Nissenbaum (2011, 2013, 2015) offer obfuscation as a rejoinder to big data's outrages. Obfuscation makes the collection of data

about individuals "more difficult to act on, and therefore less valuable . . . adding to the cost, trouble, and difficulty of doing the looking" (Brunton and Nissenbaum, 2015: 46–47).

The case for obfuscation

Online obfuscation promotes anonymity or hides one's actual searches among a gang of plausible fakes. In short, obfuscation makes it harder for receivers of information to tell signal from noise, wheat from chaff (Brunton and Nissenbaum, 2013). It is a "troublemaking strategy" that lets those who use it buy time or wall themselves off from importunate or malign third parties (Brunton and Nissenbaum, 2015: 4). Think of drawing the shades, donning a disguise, or chatting in a language that most others do not understand. It might be our best hope for keeping our information from the clutches of big data.

The technique is actually as old as the hills. Natural selection has gone in for it time and again. Consider the monarch and viceroy butterflies. As a result of feeding on milkweed as larva, monarchs are toxic to many vertebrates (Oberhauser, 2011). The species advertises its venom in flashy black and orange. A bird that has tried to snack on a monarch in the past will presumably remember the shock and shun similarly colored butterflies in the future. It is even possible that natural selection favors predators that are averse to eating monarchs, or anything like them, from the start. At least one mimic has capitalized on the monarch's combination of showiness and bad taste: viceroys (Schnur, 2002). The non-toxic viceroys are all but indistinguishable from their noxious cousins. It is easy to see why natural selection might incline towards obfuscation here. For the predator, information about potential quarry is ambiguous. Is the vibrantly colored bug up ahead a hearty lunch or a possible last meal? The savvy hunter will avoid anything turned out like a monarch.

Online obfuscation works similarly, attempting, for instance, to cloak the surfer's identity or the nature of her queries enough to throw unbidden third parties off the trail. The point is to drown the signal out with ever more noise (Brunton and Nissenbaum, 2011; Howe and Nissenbaum, 2009). Take the web-based obfuscator, Tor. Once I join the Tor network and allow my machine or device to function as a relay, my queries are encrypted and are received not from my IP address but from another "node" in the Tor relay network. The response comes back to me via other nodes, thereby shrouding my identity. Not only can snoops not decrypt the message, but because my computer is acting as a relay, they also will not know whence it came. As Brunton and Nissenbaum (2015: 20) put it, my messages are now "safe in a flock of other messages" that I and others in the network pass along. The result is that adversaries are far less likely to tie my web activity back to me than they would be without the obfuscation. If it is all right to disguise my appearance in public, particularly in the light of proliferating video surveillance, then it looks like I am justified in obfuscating my online activities, or even concealing my identity there altogether, to dodge monitoring and profiling. Until data collectors or regulators can guarantee that personal information flows within the bounds of contextual integrity, those concerned about their privacy apparently have little choice but to obfuscate.

Problems for obfuscation

Nevertheless, obfuscation faces challenges. The first is moral and has to do with the free ride that obfuscators seem to enjoy. The Internet is for the most part ostensibly free because the vast majority of people either innocently share or are coerced into parting with reams of information when they go online. Obfuscators, unlike their credulous or uninformed counterparts, get all or most of the benefits of the Internet without paying for them in the coin of surveillance. Take ad blockers. The software hides ads from the user, while clicking on them all, thereby obfuscating users' true interests and preferences. The result is an ad-free Internet experience. A similar point could be made about Tor: A user cannot be targeted by the personalized ads that underwrite a "free" Internet if she or her true activity is invisible to marketers. It looks like obfuscation offers a haven to its practitioners while abandoning everyone else to the choppy sea. Does this mean that obfuscators are "sneaks more than rebels," as some critics have suggested? (Brunton and Nissenbaum, 2015: 67; see also Brunton and Nissenbaum, 2013). Not necessarily. True, Brunton and Nissenbaum concede, the free Internet is sustained by user information. However, the terms of exchange between data subjects and data gatherers are baffling to most and invariably set by the latter. Normally, when we buy a product, we can form a pretty good idea of its value before paying up. This is not the case when we go online, where hidden costs abound: Most of us do not have the foggiest about how the capture and shuffling of our information will redound to us. Privacy partisans are not asking to get something for nothing. They can acknowledge that Google and Facebook will not provide their services for free and that the substratum of infrastructure involved in GPS services or connecting us to online

friends demand huge investment.[2] What they challenge is the price. As Brunton and Nissenbaum point out, when we trade information for a service or product, we are in effect handing a blank check over to data collectors (Brunton and Nissenbaum, 2015; Mayer-Schönberger and Cukier, 2013). Moreover, the price we are offered for products or services online can be adjusted according to algorithmic hunches about what we are willing to pay. The discrimination is opaque to consumers and perhaps even to merchants. It represents yet another blow for consent, since what I am charged might be a function of what others like me have been willing to pay in the past (Acquisti et al., 2016). Also, as Brunton and Nissenbaum (2011) point out, everyone, not just the cognoscenti, can obfuscate. It is a tool that "aids the weak against the strong" (Brunton and Nissenbaum, 2011), that is, those who know that they will be tracked but lack the skills to take stronger measures to defend their privacy (Brunton and Nissenbaum, 2015). Obfuscation is a way of standing up to the "coercion, exploitation, or threat" of big data (Brunton and Nissenbaum, 2015: 64). It enables us to snatch back that blank check before it is cashed.

Brunton and Nissenbaum attempt to clear obfuscators of the charge of free riding by pointing out that they are "not actively attempting to keep others from enjoying the same benefit . . . [They] cannot be expected to imperil themselves solely because others are in peril; they cannot be morally obligated to starve simply because others are starving" (Brunton and Nissenbaum, 2013: 179). The point is that obfuscators are leaving non-obfuscators no worse off than they would have been without the obfuscation (Brunton and Nissenbaum, 2015).

Will this wash? If the harms of obfuscation fall only to data holders and their clients, no problem, since, as Brunton and Nissenbaum (2015) rightly point out, the information exchange takes place under the dual asymmetries of power and knowledge: The information is often squeezed from us as a condition of countless routine transactions, and we generally do not know what happens to it or how its subsequent use affects us. However, although obfuscation is freely or cheaply available to all, it seems odd to describe the people who will in fact obfuscate as weak. After all, they will likely on average be highly educated and reasonably well-to-do. Brunton and Nissenbaum's slogan seems to be "let the devil take the hindmost" when it comes to evading surveillance. The fact is, they do not know what the costs of obfuscation are to non-obfuscators. They do concede that obfuscation needs to be judged case-by-case (Brunton and Nissenbaum, 2015). Still, the suspicion remains that obfuscators can enjoy a truly free Internet only if others are foolish or naïve enough to surrender their own information.

Also, Brunton and Nissenbaum never satisfactorily face up to the potentially great social costs of obfuscation online, particularly its ability to conceal grave misdeeds on the Web. Consider, for instance, the Silk Road website, which flourished from 2011 until 2013 and provided a massive venue for the sale of arms, human organs, and all manner of recreational drugs (Bilton, 2017). The founder and his associates used Tor to muddy their communications and traded exclusively in all but untraceable bitcoin. I am not claiming that a case like this shows that effective online obfuscation is unconditionally wrong, still less that it should be illegal. However, defenders of the practice need to deal with hard cases like this. Brunton and Nissenbaum have not.

Finally, even if its defenders can plausibly address the moral trials that obfuscation faces, they still have to deal with a serious practical one. As Brunton and Nissenbaum describe it at least, the practice protects at best our online activity. It provides no shield for the myriad other digital records that we routinely deposit through toll passes, credit cards, or our phones. Even if my Internet activities were maximally obfuscated, third parties would still be getting loads of data about me. And the web habits of comparable non-obfuscators will still enable data holders to draw many damaging inferences about me. So it looks like obfuscation is both morally suspect and in practice not terribly effective. In the light of these deficiencies, I would like to consider another option for at least reducing the profitability of big data: propertization, that is, assigning property rights in personal information to data subjects.

Propertization

Propertizers plausibly point out that big data is reaping most of the benefits of collection and analysis while bearing few of the costs, specifically to privacy (Laudon, 1996). These costs are externalized—that is, borne by data subjects—in the same way that polluters externalized theirs in the days before emissions were regulated or taxed. Currently, those who profit from the collection, analysis, and dissemination of personal information have little incentive not to sweep up as much as they can and sell it to the highest bidder. The propertizer need not be opposed to data holders profiting from collection and analysis. After all, the money to finance the ostensibly free Web has to come from somewhere, and those who provide these services naturally need a financial motive to do so. Also, the propertizer will concede that data brokers add considerable

value to the data they amass. The propertizer's objections relate only to *the extent to which* data mongers are profiting at the expense of data subjects.

Actually, propertization is already here to some extent, as when insurers give us discounts for letting them document our driving habits, keep track of how much we exercise, or monitor our cholesterol. Other examples include promo codes and loyalty cards, both of which tie discounts to our identity. Even "free" apps, as well as Google and Facebook, implicitly also involve propertization, since users are in effect swapping information about themselves for services rendered. The current proposal would simply formalize this arrangement and urge that we get our due. The information is fundamentally ours. Let the law acknowledge this.

The case for propertization

I will assume that the best argument for propertizing personal information disclaims moral rights and instead appeals to the good results of granting data subjects legal rights in their information. The same could plausibly be said of any system of property. It is justified to the extent that it contributes to overall well-being, otherwise not. Propertizers in particular argue that data subjects should control the disposition of their personal information, just as they do their house or car (Litman, 2000). Imagine that your barber was profiting from your trimmed hair, say, by making fine wigs from it or selling it to third parties, who were analyzing its DNA or testing it for what it revealed about your lifestyle. You would probably want a say in the matter. Why not with regard to the information you typically surrender in the course of a day? Second, since no two people will value their own information in exactly the same way, a market in personal information would allow them to assign different values to the same type. As Lawrence Lessig (2002: 262) puts it, "I may be a freak about people knowing my birthday, and so would never 'sell' access to that fact for any price, but someone else may be willing to sell access in exchange for 100 frequent flyer miles." I could agree to allow myself to be targeted by data collectors and their clients; you might absolutely refuse to do so. Propertization then would satisfy the full range of privacy preferences, from indifference to obsession (Lessig, 2002; Samuelson, 2000). Like most other market exchanges, propertization seems to offer a positive sum game between buyer and seller. Plus, presumably competition among collectors would drive the price of personal information up, meaning that less of it would make the rounds. It would also allow data subjects to get the best price they can (Rule, 2004). What are we waiting for?

Problems for propertization

A central assumption of propertization is that data subjects can give informed consent to the use of their information for a certain price. Informed consent in turn assumes that subjects are able to form a reasonable idea of what their information is worth at the time of sale, as is generally the case with, say, cars or houses. However, we have good reason to believe that the market will consistently undervalue personal information. At the very least, most sellers will not be in a position to know anything like what its true market value is. As we have seen, the value of personal information generally comes from secondary uses, many of which are impossible to anticipate at the time of collection, even by data scientists. This is inherent in the dynamism of big data. Novel inferences are its stock in trade.

Propertizers might respond that I could be wildly mistaken about the value of my tangible property as well. I might sell a parcel of remote land for next to nothing, not realizing that the Hilton Corporation was planning to acquire it for its latest world class resort and spa. After all, for any commodity or good, neither potential buyer nor seller can have a perfect idea of its current market value, to say nothing of what it will fetch in five years. But almost all of our decisions are made under some degree of uncertainty. How do I know that my morning coffee won't kill me? Or that my next train ride might not be my last? Still, for most other property or commodities the market is a fairly reliable indicator of value in a way that it systematically is not for personal information. And buyers are likely to be in a far stronger position epistemically than sellers. Whither informed consent?

And another thing: property, intellectual or real, is generally thought to be freely alienable. Says Jessica Litman (2000: 1295–1296), "The raison d'etre of property is alienability: the purpose of property laws is to prescribe the conditions of transfer . . . We deem something property in order to facilitate its transfer." If I sell you my 2005 Civic or the rights to the hit song that I dashed off last month, you can go ahead and offer them to others at whatever price the market commands, and I am implicitly agreeing to these terms at the time of sale. So far, so good. But matters are not so straightforward with personal information. If I sell you information about my last six vacations or the music I have been listening to since September, it looks like I will not be able to stop you from passing the goods along to Jones or Brown, who might turn

around and sell them to Smith or Robinson, who in turn combine the stuff with other bits about me, like the magazines I subscribe to or my commute. Or suppose that I sell you that information so that you can ply me with ads about holiday destinations or music streaming services. Would you be free to use the information for other purposes? If my travel or music tastes suggest a susceptibility to payday loans or for-profit colleges, would the data holder be able to sell that inference (O'Neil, 2016; Samuelson, 2000)? Would there be any way to meter these further uses, or would I simply be out of luck? Moreover, with other types of property, I can form a reasonably good idea of how I will be worse off once I sell it. If you buy my car, I know I'll be riding the bus. If I sell off the chunk of real estate, I won't figure on growing as much corn or wheat next year. And in principle I can buy them back. By contrast, as we saw above, no one, not even a data scientist, is generally able to come to an informed opinion about how surrendering my personal information now will redound to me later. Nor can I plausibly buy the information back. Again, what happened to informed consent?

A further question that propertizers need to answer has to do with enforcement, since no property scheme can exist without it. How would violations be enforced or even be detected? On the one hand, in the vast majority of cases data subjects would not even know that their data was being misused or how this misuse was affecting them, since the harms of big data can be hard to pinpoint. Propertizers might respond with the typical solution for hard to detect crimes like blackmail: up the punishment (Schwartz, 2004). However, whether this measure will be effective beyond the margins is an empirical question, and proponents of propertization need to reckon with the increased fiscal and social costs of more severe penalties or punishments. Also, targets of blackmail know full well that they are the victims! On the other hand, suppose data subjects who have agreed to sell their information obfuscate or deliberately falsify it. Should they be criminally liable? Propertizers need to address these problems.

Finally, I have been speaking glibly of personal information as a form of intellectual property, specifically akin to copyrightable material like books, music, or performances. Intellectual property is non-exclusive. That is, it can be in more than one place at a time. You and I can both have a copy of that catchy new song or the latest page turner. It is also non-rivalrous: One person's use does not affect another's. I can copy your novel or music files and proceed to read or listen to them without depriving you of either. By contrast, if a cupcake is mine, all mine, we obviously cannot both have it, and my eating every last crumb deprives you of the pleasure (Hettinger, 1989; Schwartz, 2004). If I can exclude you from free access to my intellectual creations, it must be for some other reason than that you would be depriving me or others of the ability to enjoy or distribute them. What counts is that without proper protection less intellectual property would be produced and distributed in the first place.

Enter the incentive theory, which I will assume for the sake of discussion is the best justification for copyright in particular and intellectual property generally. The incentive theory denies that creators of intellectual goods like books or music have a moral right to the fruits of their labor. Rather, defenders of the view argue that the law should grant creators or distributors near exclusive legal rights to their products for a period, the copyright term. Doing so provides a motive for creating and distributing those things that others find useful, entertaining, informative, or edifying. So the emphasis, morally speaking, is ultimately on the user as opposed to the producer (Hettinger,1989). The term, ideally, enables creators and distributors to recover their investment and to profit reasonably from their efforts, while excluding others for the time being from helping themselves to the product or churning out copies or knock offs (Hettinger, 1989; Samuelson, 2000). Term length should best conduce to the production of and access to creative products. The ideal term would maximize creation and distribution, consistent with maximum long-term access. The notion is to restrict nearly all free access in the short term to maximize production and access in the long run. Compare declaring a fishery off-limits today to increase yield tomorrow. Any term longer, or shorter, than needed to get these outcomes would be morally questionable.

There is surface plausibility to treating personal information as intellectual property. It too is non-exclusive: Your having access to mine does not rob me of it. It is also non-rivalrous, since your use of it does not deplete my stock. Propertizers might even agree that there should be a limit to how long subjects have near exclusive right to their information, analogous to a copyright term. After all, personal information's usefulness tends to decline over time: A recent record of my Web searches says much more about my present condition and preferences than would a record of them from 20 years ago. Additionally, analogous to fair use, propertizers should be willing to commit some information, like birthdates, to the public domain from the start. The trouble is that personal information is unlike familiar forms of intellectual property—or property in general, for that matter—in

two ways not yet discussed. First, property laws are usually established to protect what is relatively scarce. Yet when it comes to personal information, we have an embarrassment of riches. It is *privacy* that is scarce (Samuelson, 2000). Second, unlike conventional forms of intellectual property, people generally do not need an incentive to create information about themselves. Nor, unlike much intellectual property, do they need to recoup any costs (Samuelson, 2000). Most personal information is generated just by living a 21st-century life. Contrast writing a song or a bit of code, where we can plausibly say that copyright leads to more of the sort being created. It looks like the most eligible justification for intellectual property does not apply to personal information at all. Just what kind of property is it then? I defer to propertizers. Until they can give satisfactory answers to the questions I have raised about their proposal, they have failed to make their case that it can save or substantially protect privacy.

Conclusion

I have tried to show that the main candidates for preserving privacy—notice and choice statements, legislation, obfuscation, and propertization—are inadequate. My next suggestion would be my own solution to the problem, but that I do not have (compare Kripke, 1971). Opting out of the digital grid is not a serious option for most people in the rich world nor for increasingly many in the developing world. If we live a 21st-century life, we will leak data wherever we go, like it or not. Soon the leak becomes a spate. Third parties, good, bad, or indifferent, will be standing by with their analytics to make our lives better or worse. We have seen that privacy can be seriously breached even when people do not volunteer the information themselves, as long as others relevantly like them have. Obfuscation, again, suffers from a similar shortcoming. It would protect a mere slice of our data and do little to secure the narrative drawn from credit cards, toll passes, GPS devices, surveillance cameras, phone apps, and even circulation records or research database activity. Yes, we can routinely swap credit cards, sim cards, create dummy social media accounts, and so on, but will we? And how do we resist the breathtaking colonization of the Internet of things, where dishwashers and espresso machines, for instance, have unique "load signatures," which indicate when they are switched on (Mayer-Schönberger and Cukier, 2013)? It is difficult to imagine any strategy capable of facing down these assaults. It is not that technology is an autonomus, inelucable force whose ravages to privacy are inevitable. Rather, it is that technology and the information flood that it produces will not in fact be stopped, in part because those who benefit from current trends are better financed and organized than the far greater number who stand to lose dearly (Rule, 2007), in part because the vast majority of us either do not care or will remain oblivious to big data's unstinting siege.

This brings me to libraries. Librarians, through their professional organizations, have long championed privacy as a bulwark for intellectual freedom (ALA, 2014; Magi, 2011). Assuring patron privacy—or more specifically confidentiality—promotes free inquiry. In other words, it enhances patrons' autonomy as seekers of information (Rubel, 2014). However, the long-standing confidentiality of circulation records has been partially betrayed by library e-books, particularly those that can be uploaded to a Kindle. As Alan Rubel (2014) points out, this both gives Amazon access to a portion of borrowers' records and also permits the company to merge this information with the substantial chronicle it already has about them. Trina Magi (2013) describes a similar problem with database providers. When users create personal accounts in databases, they are potentially revealing their research interests, with approximately no restrictions on how vendors handle this information. A further problem emerges with journals, where "contracts may have provisions requiring libraries to monitor user activity to detect unauthorized use, and notify publishers" about this (Rubel, 2014: 187). Additionally, as Julie Cohen (1995) pointed out long ago, the move from print to e-journals has given publishers unprecedented access to reader activity and thus to their research interests.

Magi (2013) urges that librarians educate their users about these pitfalls so that they can make "informed choices" and that libraries keep circulation and research profile information in house as far as possible (p. 39; see also Fortier and Burkell, 2015). This is all very well, but will it matter? The same can be said about Rubel's worries about Amazon tracking library users through Kindles. Given the heaps that are already out there, the information gleaned from libraries is trivial. It is like worrying about the breaking of the last barn window when the other 99 are already glass-free.

I see an analogy between the threat to privacy and the challenge of climate change. My guess regarding the latter is that we will not get the kind of international cooperation needed to stop the worst havoc, given inertia and the powerful forces that have an interest in sticking with fossil fuel. Likewise with privacy: Over time, our privacy "immune systems,"

to use James Rule's (2007: 165) metaphor, grow weaker; threats to privacy tend to encounter less resistance as the years go by. Imagine telling someone 40 years ago that today every other person on the planet would choose to tote a glorified tracker around with them at all times! Does anyone really think, for instance, that privacy concerns will be foremost in the design and deployment of self-driving cars?

At the turn of the century *The Economist* (1999: 15) shrewdly speculated that:

> All . . . efforts to hold back the rising tide of electronic intrusion into privacy will fail. . . . Twenty years hence most people will find that the privacy they take for granted today will be just as elusive as the privacy of the 1970s seems today. . . . Many might prefer to eschew even the huge benefits that the new information economy promises. But they will not, in practice, be offered the choice.

Evidently. Like it or not, the time has come to give up the ghost of privacy and thus call off the moral debate to save or restore it. Anyway, people evidently enjoy the convenience that big data and its analytics have offered them in terms of movie or vacation recommendations, location services, easy contact with friends and acquaintances, and so on. To some extent, people have acquiesced in the demise of their own privacy. Defenders of privacy need to deal with the fact that it just might be that people *like* being profiled. Also, I mentioned at the outset that big data is transforming the social sciences and our approach to public health. Maybe people will someday view the end of privacy the way we think today about the loss of innocence after Copernicus or Darwin. They could well decide that trading away privacy was worth it in the light of the very considerable benefits that big data has offered for our understanding of ourselves, the control of disease, the efficiency of smart public transportation, and the safety of autonomous cars. Or they might never know what they are missing. Perhaps our real concern should not be with privacy but with the widening gap in wealth and power that big data seems to be driving. *That* is anything but inevitable.[3]

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. I would like to thank an anonymous reviewer for prompting me to make this clarification.
2. I would like to thank Phil Swan for this point.
3. I would like to thank John Buschman, Jane Carter, Don Fallis, Shannon Oltmann, and Philip Swan for their feedback. I would also like to thank attendees of the 2017 Information Ethics Roundtable, held at the School of Information Sciences at the Univerity of Illinios, Urbana-Champaign; and attendees of the 2017 annual meeting of the International Association of Computing and Philosophy, held at Stanford University.

References

Acquisti A (2014) The economics and behavioral economics of privacy. In: Lane J, et al. (eds) *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. New York: Cambridge University Press, pp. 76–95.

Acquisti A, Taylor C and Wagman L (2016) The economics of privacy. *Journal of Economic Literature* 54(2): 442–492.

ALA (American Library Association) (2014) Privacy: An interpretation of the Library Bill of Rights. Available at http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy (accessed 13 December 2017).

Angwin J (2014) *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: Times Books, Henry Holt and Company.

Angwin J, Scheiber N and Tobin A (2017) Facebook job ads raise concerns about age discrimination. *The New York Times*, 20 December, p. 1.

Barocas S and Nissenbaum H (2014a) Big data's end run around anonymity and consent. In: Lane J, et al. (eds) *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. New York: Cambridge University Press, pp. 44–75.

Barocas S and Nissenbaum H (2014b) Big data's end run around procedural privacy protections. *Communications of the ACM* 57(11): 31–33.

Bilton N (2017) *American Kingpin: The Epic Hunt for the Criminal Mastermind behind the Silk Road*. New York: Penguin.

Brunton F and Nissenbaum H (2011) Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday* 16(5).

Brunton F and Nissenbaum H (2013) Political and ethical perspectives on data obfuscation. In: Hildebrandt H and De Vries K (eds) *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. New York: Routledge, pp. 164–188.

Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press.

Cohen J (1995) A right to read anonymously: A closer look at copyright management in cyberspace. *Connecticut Law Review* 28: 981–1040.

Cohen J (2000) Examined lives: Information privacy and the subject as object. *Stanford Law Review* 52(5): 1373–1438.

Duhigg C (2009) What does your credit-card company know about you? *New York Times Magazine*, 17 May, pp. 40–45.

Economist (1999) The end of privacy. *Economist*, 1 May, pp. 15–16.

Fortier A and Burkell J (2015) Hidden online surveillance: What librarians should know to protect their own privacy and that of their patrons. *Information Technology & Libraries* 34(3): 59–72.

Gandy O (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.

Hettinger E (1989) Justifying intellectual property. *Philosophy & Public Affairs* 18(1): 31–52.

Howe D and Nissenbaum H (2009) Trackmenot: Resisting surveillance in web searches. In: Kerr I, Lucock C and Steeves V (eds) *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press, pp. 418–436.

Kripke S (1977) Identity and necessity. In: Munitz M (ed.) *Identity and Individuation*. New York: New York University Press, pp. 135–164.

Landau S (2015) Control use of data to protect privacy. *Science* 347(6221): 504–506.

Laudon K (1996) Markets and privacy. *Communications of the ACM* 39(9): 92–104.

Lessig L (2002) Privacy as property. *Social Research* 69(1): 247–269.

Litman J (2000) Information privacy/information property. *Stanford Law Review* 52(5): 1283–1313.

Magi T (2011) Fourteen reasons privacy matters: A multidisciplinary review of scholarly literature. *Library Quarterly* 81(2): 187–209.

Magi T (2013) A fresh look at privacy: Why does it matter, who cares, and what should librarians do about it. *Indiana Libraries* 32(1): 37–41.

Mai J (2016) Big data privacy: The datafication of personal information. *The Information Society* 32(3): 192–199.

Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution that Will Transform How We Live, Work, and Think*. Boston, MA and New York: Dolan/Houghton Mifflin Harcourt.

Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law.

Nissenbaum H (2011) A contextual approach to privacy online. *Daedalus* 140(4): 32–48.

Oberhauser K (2011) Monarch butterfly. In: *Environmental Encyclopedia. Vol. 2*. 4th edn. Detroit, IL: Gale, pp. 1091–1093.

Ohm P (2014) Changing the rules: General principles for data use and analysis. In: Lane J, et al. (eds) *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. New York: Cambridge University Press, pp. 96–111.

O'Neil C (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

Pekala S (2017) Privacy and user experience in 21st century library discovery. *Information Technology & Libraries* 36(2): 48–58.

Rubel A (2014) Libraries, electronic resources, and privacy: The case for positive intellectual freedom. *Library Quarterly* 84(2): 183–208.

Rule J (2004) Toward strong privacy: Values, markets, mechanisms, and institutions. *University of Toronto Law Journal* 54(2): 183–225.

Rule J (2007) *Privacy in Peril*. New York: Oxford University Press.

Samuelson P (2000) Privacy as intellectual property? *Stanford Law Review* 52(5): 1125–1173.

Schneier B (2015) *Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World*. New York: WW Norton.

Schnur D (2002) Mimicry. In: Cobb A (ed.) *Animal Sciences*. Vol. 3. New York: Macmillan Reference USA, pp. 121–123.

Schwartz P (2004) Property, privacy, and personal data. *Harvard Law Review* 117(7): 2055–2128.

Singer N (2013) A data broker offers a peek behind the curtain. *The New York Times*, 1 September, p. 1.

Steel E and Angwin J (2010) On the web's cutting edge, anonymity in name only. *Wall Street Journal*, 4 August, A1.

Stephens-Davidowitz S (2017) *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us about Who We Really Are*. New York: Dey St.

Tavani H and Moor J (2001) Privacy protection, control of information, and privacy-enhancing technologies. *Computers and Society* 31(1): 6–11.

Walker J (2013) Data mining to recruit sick people. *The Wall Street Journal*, 17 December, B1.

Author biography

Tony Doyle is a Reference/Instruction Librarian and Associate Professor at Hunter College (CUNY) in New York City. He is also an Adjunct Associate Professor in the Philosophy Department at Hunter. He has an MLS from Queens College (CUNY) and a Master's in Philosophy from Northern Illinois University. His research interest is in the ethics of privacy, focusing on how privacy has been affected by digital technology.

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 240–251

DOI: 10.1177/0340035218793572
journals.sagepub.com/home/ifl
SAGE

Abstracts

في العمل على مبدأ "الحق في أن تُنسى" والرفع من القوائم ؛ كي يستعدوا للمشاكل التي ستواجه سير المعلومات في المُستقبل وتغير سياسات وقوانين المعلومات حول العالم، يوضح هذا البحث المسائل القانونية والأخلاقية المُرتبطة بالرفع من القوائم وتؤسس لحوار دولي حول الرفع من القوائم وتُنبه للحاجة إلى بحث أكثر من أجل المُستقبل، ويحتاج مُجتمع المكتبات حول العالم نقاش أوسع حول المسائل المُرتبطة بالحق في أن تُنسى والرفع من القوائم، خاصةً، القوانين والسياسات المُتعلقة بحرية التعبير والخصوصية.

Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries

تشجيع المُستخدمين على استخدام تقنيات حماية الخصوصية: التحديات التي تواجه المكتبة العامة:

Monica G. Maceli

العدد رقم 3،44 من مجلة الإفلا المُتخصصة:

المُلخص: لقد أضحت خصوصية المُستخدمين أمرًا يشغل المكتبات، لقد تغيرت مسؤولياتنا التي كانت فقط داخل المكتبة بعد التطورات التكنولوجية الجديدة واختلاف المشهد المكتبي تمامًا بشكل يُهدد خصوصية المُستخدم، وفي ظل هذا المشهد المُعقد، استمرت المكتبات في التزامها بالحفاظ على الخصوصية، بل وتسعى المكتبات العامة الآن بتوعية المُستخدمين بما يُشكل خطرًا على خصوصيتهم ومعايير الحماية والأدوات المُمكن استخدامها، تعمل هذه المُراجعة النقدية على تحديد التحديات التي تواجه المكتبات الأمريكية في توعية المُستخدمين باستخدام أدوات حماية الخصوصية وتقترح الاستمرار في البحث في هذه المسألة مُستقبلاً، وقد توصل البحث للمشكلات التالية: نقص كبير في معرفة المُستخدمين والمكتبيين والقائمين على المكتبات بالتكنولوجيا، الحاجة إلى دعم عدد كبير من الأدوات والتقنيات التكنولوجية.

Information disclosure and privacy behaviours regarding employer surveillance of SNS

Deirdre McGuinness, Anoush Simon

العدد رقم 3،44 من مجلة الإفلا المُتخصصة:

قتطفات

Privacy awareness issues in user data collection by digital libraries

وعي المكتبات الرقمية بقضية الخصوصية أثناء جمع بيانات المُستخدمين:

Elaine Parra Affonso, Ricardo César Gonçalves Sant'Ana

العدد رقم 3،44 من مجلة الإفلا المُتخصصة:

المُلخص: يهدف هذا العمل إلى بحث جانب الخصوصية في جمع المكتبات الرقمية الوطنية في أمريكا اللاتينية بيانات المُستخدمين، يتبع البحث منهجًا استكشافيًا لتحديد البيانات التي يتم جمعها بعلم المُستخدمين ومدى وجود سياسات واضحة مُتبعة للحفاظ على خصوصيتهم، كما استخدمنا برنامج Wireshark أيضًا للتحقق من كيفية جمع البيانات في البرازيل، وقد اتضح أن مكتبتان رقميتان فقط هما من يتبعا سياسة للخصوصية، وفيما يتعلق بجمع البيانات تفوق البيانات التي يتم جمعها بدون علم المُستخدمين على التي يتم جمعها بعلمهم، وهنا توضح النتيجة أن الخصوصية قد تُنتهك بسبب قلة وعي المُستخدمين بوقت، وكيفية، ومكان الحصول على هذه البيانات،لذا؛ فمن الضروري أنت ترفع المكتبات الرقمية وعي المُستخدمين في هذا الصدد.

Delisting and ethics in the library: Anticipating the future of librarianship in a world that forgets

الرفع من القوائم والأخلاقيات في المكتبة: مُستقبل المكتبات في عالم ينسى:

Katie Chamberlain Kritikos

العدد رقم 3،44 من مجلة الإفلا المُتخصصة:

المُلخص: إن قيم أخصائي المكتبات التقليدي تحمي خصوصية الفرد وتدعم الوصول إلى المعلومات، إن مبدأ "الحق في أن تُنسى" والرفع من القوائم يُمكن أن يخلقا بيئة معلوماتية جديدة في القواعد الأخلاقية وتُعيد تعريف دور المكتبيين إلى جانب مُراقبة الإنترنت وغربلة المحتوى وهي العوامل التي تُنبئ بتغيرات في طريقة تنظيم المحتوى والوصول إلى المعلومات على الإنترنت، يجب أن ينخرط المكتبيون

بالمكتبات من خلال دراستي حالة ويختتم المقال بمُقترحات لصالح الخصوصية في اليابان.

Privacy, obfuscation, and propertization

الخصوصية والتشويش وحقوق الملكية الفكرية:

Tony Doyle

العدد رقم 44،3 من مجلة الإفلا المُتخصصة:

تحظى البيانات الضخمة بأهمية كبيرة في ظل العصر الرقمي وهي ما يُعطي دلالات على سماتنا وما سنفضله في المُستقبل، يُناقش هذا البحث التحديات التي تفرضها البيانات الضخمة على مبدأ الخصوصية، ويبحث أكثر العوامل التي يُمكن أن تتصدى لتلك التحديات وهما "التشويش" و"الملكية" للبيانات الشخصية، حيث يضع التشويش عائقًا أمام مُتعقبي البيانات، أما الملكية فتدعو إلى اندراج البيانات الشخصية تحت حقوق الملكية الفكرية وهو ما يتطلب من مُتعقبي البيانات التفاهم مع مُلاك هذه البيانات قبل استخدامها، ويُختتم البحث أن الخصوصية أصبحت قضية خاسرة ويجب ألا نُدافع عنها من وجهة نظر أخلاقية وأُشير في البحث إلى ما يعنيه ذلك للمكتبات.

المُلخص: يستكشف هذا البحث استخدام وسائل التواصل الاجتماعي بين طلاب جامعة Welshوخاصةً طريقة مُشاركة المعلومات ومدى الحفاظ على الخصوصية وما أثر استخدام هذه المواقع مُستقبلاً، وقد تم اللجوء للمنهج الكمي والكيفي في هذا البحث.

وقد أوضحت النتائج انشغال المُشاركين بالحفاظ على خصوصيتهم على الإنترنت ولكن معايير حماية الخصوصية ليست كافية، كما أن مُعظم المُستخدمين على وعي بمُراقبة هذه الشبكات، ولكن المُستخدمون حريصون على حماية خصوصيتهم من خلال إعدادات الخصوصية المُختلفة.

Privacy and libraries in the case of Japan

الخصوصية والمكتبات في اليابان:

Yasuyo Inoue

العدد رقم 44،3 من مجلة الإفلا المُتخصصة:

**المُلخص: يُقدم هذا المقال مبدأ الخصوصية من وجهة نظر شعوب شرق آسيا واليابان، فأولا يعرض البحث كيف تنظر اليابان إلى مبدأ الخصوصية، ثم يُناقش البحث الأمور التشريعية المتعلقة بحماية الخصوصية في اليابان، ويواصل البحث توضيح علاقة الخصوصية

摘际图联杂志 44-3 英语摘要翻译

Privacy awareness issues in user data collection by digital libraries

数字图书馆采集用户数据中的隐私问题

Elaine Parra Affonso, Ricardo César Gonçalves Sant'Ana

伊莱恩·帕拉·阿方索，里卡多·凯撒·贡萨尔维斯·圣安娜

国际图联杂志，44-3，170-182

摘要： 该研究的目标是探究南美各国的国家数字图书馆在数据收集中与隐私相关的问题，所采用的研究方法是基于数字图书馆的探索性研究，以此来识别所收集的与用户意识和隐私政策的清晰呈现相关的数据。我们也使用了Wireshark软件来研究巴西国家图书馆收集的数据。我们发现，南美只有两个数字图书馆会提供隐私保护指导。关于数据的收集，在用户未知的情况下收集的数据和在用户清楚知道的情况下所收集数据形成对比。最后我们得出结论，隐私问题会受到用户对何时、怎样以及在哪收集数据的意识较低影响，这让隐私政策在数字图书馆中成为必需，以此来提高对数据收集这一过程的意识。

Delisting and ethics in the library: Anticipating the future of librarianship in a world that forgets

图书馆的数据撤销和职业道德：期待在一个遗忘的世界中图书馆事业的未来

Katie Chamberlain Kritikos

凯蒂·夏伯兰·克里蒂科斯

国际图联杂志，44-3，183-194

摘要： 统的图书馆员职业道德保护个人隐私并且促进信息获取。被遗忘权(RTBF)和数据撤销有可能会创造一个新的网络信息生态系统，来打破旧的图书馆员道德标准并且重新定义图书馆员的角色。被遗忘权和数据撤销，还有互联网信息过滤，都是即将转变为内容监控和网络信息获取的先兆。图书馆员现在开始应当接受被遗忘权和数据撤销，为将来可能出现的图书馆信息流动中

断，以及世界范围的与信息相关的政策法规的改变做准备。这篇文章阐述了与数据撤销相关的法律和道德问题，为数据撤销的国际对话奠定了基础，并且指出了未来对相关问题研究的需要。针对被遗忘权和数据撤销的相关问题，国际图书馆界需要进行一次更大规模的讨论，尤其是关于言论自由和隐私的相关法律和政策的讨论。

Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries

鼓励读者使用隐私保护技术：公共图书馆的挑战

Monica G. Maceli

莫妮卡·梅塞丽

国际图联杂志，44-3，195-202

摘要： 读者隐私所受到的威胁一直以来都是图书馆的担忧，而且我们所能尽到的责任也很大程度上被图书馆的物理空间所限。如今，随着新技术的发展，情况也变得完全不同，读者的隐私反而受到更多快速增长的事物的威胁。在这种复杂的情况下，图书馆继续致力于隐私保护，现在公共图书馆也尝试教育读者隐私威胁、隐私保护措施，和他们能使用的一些工具。这篇文献综述力图识别美国公共图书馆在教育和推动读者使用隐私保护技术工具中所面临的挑战，从其它相关学科的研究中吸取借鉴，并启发未来的研究方向。我们发现的问题包括：读者、图书馆管理员和图书馆员工在技术相关方面潜在的知识差距；支持使用大量技术工具和技能的需求；以及加深我们对这些工具潜在创造者视角的理解。

Information disclosure and privacy behaviours regarding employer surveillance of SNS

关于社交网站用户监控的信息泄露和隐私行为

Deirdre McGuinness, Anoush Simon

迪尔德丽·麦吉尼斯，阿诺什·西蒙

国际图联杂志，44-3，203-222

摘要： 这篇文章研究了一所威尔士大学中学生群体使用社交网站(SNSs)的情况，其中特别关注了信息共享和隐私行为，以及社交网站的用户监控对他们未来使用这些网站的潜在影响。该研究采用了定量和定性方法相结合的混合研究方法来对上述议题进行探究。

研究结果显示，参与者对在网络上的隐私保护表示担忧，并且对在社交网络上发帖和保护个人信息都十分注意；但是通常由于人为失误及系统错误，保护措施仍存在缺陷。绝大多数的参与者都知道社交网站的监控，很多人也指出这会对他们未来的使用产生影响，但是社交网站用户会综合使用网站隐私设置和按情况分等级的发布信息等方法来积极保护他们的隐私。

Privacy and libraries in the case of Japan

以日本为例的图书馆与隐私研究

Yasuyo Inoue

井上安代

国际图联杂志，44-3，223-228

摘要： 这篇论文从东亚国家日本的角度来介绍隐私的概念。首先，该文就整个国家是如何看待隐私的，进行了背景信息介绍，然后讨论了日本隐私保护的相关法律途径。接着文章探讨了与图书馆相关的隐私问题，介绍了两个案例研究。最后得出结论，为日本未来发展提出建议。

Privacy, obfuscation, and propertization

隐私、模糊化和财产化

Tony Doyle

托尼·道尔

国际图联杂志，44-3，229-239

摘要： 伴随着数字化时代的余波，大数据已经准备好取而代之，将其数据分析用于对我们个人性格、偏好和未来行为的推断中，这让我们紧张不安。这篇文章阐述了大数据给隐私带来的挑战。我探析了两种可能是最有希望对抗大数据对个人隐私冲击的尝试，即个人信息的模糊化和财产化。模糊化是采用迷惑或者误导的方式，在数字化的过程中摆脱数据收集方。财产化则是将个人信息视为一种知识产权，需要数据持有者在对数

据的任何二次利用中给予数据主体以补偿。我在文中尽力阐明这两种抵抗的尝试都在很大程度上失败了。我从而得出结论，隐私保护注定要失败，我们应该停止从道德的角度进行保护隐私的尝试。文章的最后，我就这些在图书馆领域的影响提出几点想法。

Sommaries

Privacy awareness issues in user data collection by digital libraries

Sensibilisation à la protection de la vie privée dans la collecte de données d'utilisateurs par les bibliothèques numériques

Elaine Parra Affonso, Ricardo César Gonçalves Sant'Ana

IFLA Journal, 44-3, 170-182

Résumé:

Ce travail vise à enquêter sur les aspects de la protection de la vie privée dans la collecte de données par des Bibliothèques Numériques Nationales d'Amérique du Sud. La méthodologie se base sur des recherches exploratoires dans des bibliothèques numériques pour identifier les données collectées dans le cas où l'utilisateur est sensibilisé et la présence explicite de politiques de protection de la vie privée. Nous avons également utilisé l'outil Wireshark pour enquêter sur la collecte de données éventuelle par la Bibliothèque Nationale du Brésil. Nous avons identifié que seulement deux bibliothèques numériques fournissent des notices sur la protection de la vie privée. En lien avec la collecte de données, les informations collectées sans que l'utilisateur s'en aperçoive contraste par rapport à ce qui est fourni consciemment par des utilisateurs. Il a été conclu que la protection de la vie privée peut être influencée par une faible sensibilisation des utilisateurs sur le moment, la façon et l'endroit où la collecte de données s'effectue. La disponibilité de politiques de protection de la vie privée devient essentielle dans des bibliothèques pour créer une sensibilisation de ce procédé.

Delisting and ethics in the library: Anticipating the future of librarianship in a world that forgets

Radiation et éthique dans la bibliothèque: Anticipation de l'avenir de la bibliothéconomie dans un monde qui oublie

Katie Chamberlain Kritikos

IFLA Journal, 44-3, 183-194

Résumé:

L'éthique traditionnelle des bibliothécaires protège la vie privée et favorise l'accès à l'information. Le droit à l'oubli (DALO) et la radiation offrent des possibilités de créer un nouvel écosystème d'information en ligne qui perturbe les normes éthiques et redéfinit le rôle des bibliothécaires. Parallèlement au filtrage d'internet, le DALO et la radiation laissent présager les changements futurs dans la régulation du contenu et d'accès aux informations en ligne. Les bibliothécaires devraient dès à présent accorder de l'attention aux problèmes de DALO et de radiation pour se préparer aux futures perturbations éventuelles dans le flux d'informations dans la bibliothèque et des changements dans la réglementation et la législation sur l'information à travers le monde. Cet article exprime clairement les problèmes légaux et éthiques associés à la radiation, pose les fondations pour un dialogue international sur la radiation et indique les besoins de recherches futures. La communauté internationale de la bibliothéconomie a besoin d'un débat plus ample sur des problèmes liés au DALO et à la radiation, notamment sur la législation et la réglementation relatives à la liberté d'expression et la vie privée.

Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries

L'incitation des usagers à adopter des technologies de protection de la vie privée: les défis pour les bibliothèques publiques

Monica G. Maceli
IFLA Journal, 44-3, 195-202

Résumé:

Les menaces sur la vie privée de nos usagers ont été un souci de longue date dans des bibliothèques, bien que nos responsabilités se limitaient largement à l'espace physique de la bibliothèque. Aujourd'hui, alimenté par de nouvelles technologies, le paysage est extrêmement différent par la menace de la vie privée des usagers par un nombre d'entités en constante augmentation. Dans cette complexité, des bibliothèques poursuivent leur engagement pour la vie privée, des bibliothèques publiques tentent désormais d'éduquer les usagers sur les menaces de la vie privée, des mesures de protection et des outils qu'ils pourraient utiliser. Cette étude documentaire tente d'identifier les défis pour les bibliothèques

publiques aux États-Unis dans l'éducation et la préconisation d'utilisation d'outils de protection de la vie privée par les usagers, en s'inspirant d'études dans une variété de domaines associés, tout en suggérant des orientations pour des recherches futures. Les sujets identifiés comprennent: des vides substantiels dans les connaissances sur les technologies parmi nos usagers, nos bibliothécaires et notre personnel de bibliothèque; le besoin de soutenir un large nombre d'outils et de techniques technologiques; ainsi que la formation de notre compréhension de la perspective des créateurs à la base de ces outils.

Information disclosure and privacy behaviours regarding employer surveillance of SRS

Le comportement de divulgation d'information et la protection de la vie privée par rapport à la surveillance de SRS par des employeurs

Deirdre McGuinness, Anoush Simon
IFLA Journal, 44-3, 203-222

Résumé:

Cet article étudie l'utilisation de sites de réseaux sociaux (SRS) parmi la population étudiante d'une Université galloise, particulièrement en ce qui concerne le comportement de partage d'informations et de protection de la vie privée, et l'impact potentiel de vérification des SRS par des employeurs sur l'utilisation future de ces sites. Un concept d'études aux méthodes mixtes comprenant aussi bien des approches quantitatives que qualitatives a été utilisé pour enquêter sur la problématique de la recherche.

Les résultats ont démontré que les participants se souciaient de sauvegarder leur vie privée en ligne et qu'ils étaient prudents pour poster et protéger des informations sur les SRS; néanmoins des mesures de protection n'étaient pas parfaites en raison d'erreurs humaines et du système. La plupart des répondants étaient conscients de la surveillance des SRS, beaucoup d'entre eux notaient que cela pouvait avoir un impact sur leur utilisation future, néanmoins des utilisateurs étaient actifs dans la protection de leur vie privée par une combinaison d'utilisation de réglages de protection de la vie privée et différents niveaux de divulgation d'informations en fonction du contexte.

Privacy and libraries in the case of Japan

La vie privée et les bibliothèques: le cas du Japon

Yasuyo Inoue

IFLA Journal, 44-3, 223-228

Résumé:

Cet essai introduit l'idée de la protection de la vie privée du point de vue d'un pays en Asie de l'Est qu'est le Japon. D'abord, il fournit un contexte de fond sur la considération de la vie privée dans le pays; ensuite, il traite les approches législatives pertinentes de protection de la vie privée au Japon. Il continue de parler de la vie privée en lien avec sa pertinence pour les bibliothèques, illustrée par deux études de cas, avant de conclure avec quelques suggestions sur la marche à suivre au Japon.

Privacy, obfuscation, and propertization

La vie privée, le brouillage et l'appropriation

Tony Doyle

IFLA Journal, 44-3, 229-239

Résumé:

Comme notre sillage numérique s'étend, les big data ou mégadonnées sont là pour les parcourir, en appliquant leurs analyses pour faire des interférences énervantes sur nos caractères, nos préférences et notre comportement futur. Cet article aborde le défi que les big data présentent pour la vie privée. J'étudie ce que sont peut-être les deux tentatives les plus prometteuses pour repousser l'attaque des big data sur la vie privée: le brouillage et l'appropriation d'informations personnelles. Le brouillage tente de semer des collecteurs de données de notre trace numérique en les déroutant ou en les induisant en erreur. L'appropriation prévoit de traiter les informations personnelles comme de la propriété intellectuelle et exigerait que les détenteurs de données indemnisent les personnes concernées pour toute utilisation secondaire. Je tente de démontrer que les deux défenses échouent amplement. Je conclus que la protection de la vie privée est une cause perdue et que nous devrions annuler les tentatives de la défendre d'un point de vue moral. Je termine par quelques réflexions sur ce que cela signifie pour les bibliothèques.

Zusammenfassungen

Privacy awareness issues in user data collection by digital libraries

Bewusstsein zum Datenschutz bei der Datenerhebung über Benutzer von digitalen Bibliotheken

Elaine Parra Affonso, Ricardo César Gonçalves Sant'Ana

IFLA Journal, 44-3, 170-182

Abstrakt:

Diese Studie beschäftigt sich mit Aspekten des Datenschutzes bei der Datenerhebung seitens der nationalen digitalen Bibliotheken in Südamerika. Die Vorgehensweise beruht auf der Explorationsforschung in digitalen Bibliotheken zur Feststellung, ob Daten mit dem Wissen des Benutzers erhoben wurden und ob ausdrückliche Datenschutzbestimmungen vorlagen. Für die Bestimmung der möglichen Datenerhebung in der brasilianischen Nationalbibliothek benutzten wir ebenfalls das Wireshark-System. Von uns wurde festgestellt, dass nur zwei digitale Bibliotheken Datenschutzrichtlinien bieten. In Bezug auf die Erhebung von Daten fällt der Umfang der ohne das Wissen der Benutzer erhobenen Daten im Vergleich zu dem auf, was von den Benutzern bewusst bereitgestellt wurde. Als Fazit lässt sich feststellen, dass Datenschutzprobleme durch das geringe Bewusstsein von Benutzern, wann, wie und wo die Datenerhebung erfolgt, beeinflusst werden können. Die Verfügbarkeit von Datenschutzbestimmungen werden somit ein wesentlicher Aspekt in digitalen Bibliotheken, um das Bewusstsein über diesen Prozess zu fördern.

Delisting and ethics in the library: Anticipating the future of librarianship in a world that forgets

Lösung und Ethik in der Bibliothek: die mögliche Zukunft des Bibliothekswesens in einer Welt, die mehr und mehr vergisst

Katie Chamberlain Kritikos

IFLA Journal, 44-3, 183-194

Abstrakt:

Die traditionelle Ethik von Bibliotheken dient dem Datenschutz und fördert den Zugriff auf Daten. Das Recht auf Vergessenwerden (RTBF) und das Entfernen von Angaben bieten die Möglichkeit zur Schaffung eines neuen Online-Ökosystems für Informationen, das die ethischen Normen sprengt und die Rolle der Bibliothekare neu definiert. Zusammen mit dem Filter Internet sind das Recht auf Vergessenwerden und das Entfernen von Angaben die Vorboten künftiger Veränderungen in Bezug auf den Umgang mit Daten und deren Online-Zugriff. Bibliothekare sollten sich mit Aspekten wie dem Vergessenwerden und Entfernen jetzt auseinandersetzen, damit sie auf mögliche künftige Unterbrechungen des Informationsflusses in der Bibliothek und auf Veränderungen bei Datenschutzbestimmungen und -gesetzen in aller Welt vorbereitet sind. Dieses Papier beschreibt die rechtlichen und ethischen Fragen, die mit dem Entfernen von Listen verbunden sind, es legt den Grundstein für einen internationalen Dialog zu dem Entfernen von Listen und zeigt den Bedarf an Forschungsarbeiten in der Zukunft auf. Die internationale Gemeinschaft der Bibliotheken braucht eine umfassendere Diskussion über die Aspekte des Rechts auf Vergessenwerden und das Entfernen von Angaben, ganz besonders wenn es um Gesetze und Bestimmungen zur Meingungsfreiheit und zum Datenschutz geht.

Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries

Förderung von Kunden bei der Umsetzung von Datenschutztechnologien: Herausforderung für öffentliche Bibliotheken

Monica G. Maceli

IFLA Journal, 44-3, 195-202

Abstrakt:

Bedrohungen bezüglich des Datenschutzes unserer Kunden sind seit langer Zeit ein Aspekt in Bibliotheken, obwohl unsere Verantwortung zumeist auf den tatsächlichen Raum der Bibliothek beschränkt war. Durch das Aufkommen neuer Technologien hat sich diese Umgebung jedoch deutlich verändert, sodass der Datenschutz von Kunden durch eine stetige Zunahme von Einflussfaktoren bedroht wird. Vor dem Hintergrund dieser Komplexität setzen sich Bibliotheken weiterhin für den Datenschutz ein: Öffentliche Bibliotheken bemühen sich darum, das Bewusstsein der Kunden über den Datenschutz, mögliche Schutzvorkehrungen und über Hilfsmittel, die sie nutzen könnten, zu verstärken. Anhand dieser Literaturrecherche sollen Herausforderungen in US-amerikanischen Bibliotheken aufgezeigt werden, wenn es um Aufklärung und Förderung der Kunden in Bezug auf die Verwendung von technischen Hilfsmitteln zum Datenschutz geht. Die Studie beschäftigt sich mit einer Vielzahl angrenzender Bereiche und zeigt zudem Richtungen für künftige Studien auf. Die erfassten Punkte umfassen erhebliche technologiebezogene Wissenslücken bei unseren Kunden, Bibliothekaren und Bibliotheksbeschäftigten, das Bedürfnis, eine

große Zahl technologischer Hilfsmittel und Techniken zu unterstützen sowie zudem die Entwicklung eines größeren Verständnisses, wenn es um die Perspektive der Hersteller solcher Tools geht.

Information disclosure and privacy behaviours regarding employer surveillance of SNS

Enthüllung von Angaben und Umgang mit dem Datenschutz in Bezug auf die Überwachung von Arbeiternehmern über soziale Netzwerke

Deirdre McGuinness, Anoush Simon
IFLA Journal, 44-3, 203-222

Abstrakt:

Die Studie beschäftigt sich mit der Nutzung von Websites zur sozialen Vernetzung von Studierenden einer walisischen Universität, vor allem in Bezug auf den Austausch von Daten und den Umgang mit dem Datenschutz sowie auf den möglichen Einfluss von Prüfungen solcher Websites durch Arbeitgeber, und zwar in Hinsicht auf die künftige Verwendung dieser Websites. Für die Untersuchung dieser Fragen wurde eine Kombination mehrerer Forschungskonzepte mit sowohl quantitativen als auch qualitativen Ansätzen gewählt.

Die Ergebnisse zeigten, dass die Teilnehmenden sich Sorgen um den Datenschutz online machen, sie darauf achteten, was sie auf solchen Websites einstellen und wie sie es schützen, aber Schutzmaßnahmen erweisen sich durch menschliche und technische Fehler als nicht perfekt. Die meisten der Befragten waren sich der Überwachung von Websites für soziale Netzwerke bewusst; viele führten auch an, dass dies einen Einfluss auf deren Verwendung in der Zukunft hätte. Benutzer schützen ihre Privatsphäre jedoch anhand einer Kombination aus Datenschutzeinstellungen und – je nach Kontext – unterschiedlichen Ebenen der Angabe von Informationen.

Privacy and libraries in the case of Japan

Datenschutz und Bibliotheken in Japan

Yasuyo Inoue

IFLA Journal, 44-3, 223-228

Abstrakt:

Dieser Essay beschreibt das Konzept des Datenschutzes aus der Perspektive von Japan. Zunächst werden Hintergrundinformationen darüber geboten, wie das Land mit dem Datenschutz umgeht, bevor relevante rechtliche Ansätze zum Datenschutz in Japan dargelegt werden. Im Anschluss wird der Aspekt Datenschutz im Verhältnis zu Bibliotheken erörtert; das geschieht anhand von zwei Fallbeispielen und abschließend werden einige Vorschläge für den weiteren Weg in die Zukunft in Japan vorgetragen.

Privacy, obfuscation, and propertization

Datenschutz, Verschleierung und Besitzübernahme

Tony Doyle

IFLA Journal, 44-3, 229-239

Abstrakt:

Während unsere digitale Wache immer umfassender wird, stehen die Big Data schon zum Einsatz bereit und analysieren die Daten, um erstaunliche Schlussfolgerungen über unseren Charakter, unsere persönlichen Vorlieben und unser künftiges Verhalten zu ziehen. Diese Studie beschäftigt sich mit der Frage, welche Herausforderung Big Data für den Datenschutz darstellt. In diesem Kontext prüfe ich die beiden vielversprechendsten Versuche zum Schutz des Datenschutzes vor den Angriffen von Big Data: Verschleierung und die Besitzübernahme persönlicher Angaben. Anhand der Verschleierung werden diejenigen, die versuchen, unsere Daten zu bekommen durch Irreführung oder Verwirrung von unserer digitalen Fährte gebracht. Die Besitzübernahme zielt darauf ab, persönliche Angaben als geistiges Eigentum zu betrachten, was den Dateninhaber verpflichten würde, die Datensubjekte für jedwede weitere Verwendung zu entschädigen. Ich versuche aufzuzeigen, dass beide Schutzmaßnahmen weitestgehend unwirksam sind. Ich komme zu dem Schluss, dass der Datenschutz doch nicht zu gewährleisten ist und wir alle Versuche zum Datenschutz aufgeben und ihn stattdessen aus moralischer Sicht verteidigen sollten. Ich schließe den Text mit einigen Gedanken über die Bedeutung von all dem für Bibliotheken ab.

Рефераты статеи

Privacy awareness issues in user data collection by digital libraries

Осведомленность о конфиденциальном характере сведений в процессе сбора цифровыми библиотеками информации о пользователях

Элейн Парра Аффонсо, Рикардо Сезар Гонсалвес Сант'Ана

IFLA Journal, 44-3, 170-182

Аннотация:

Целью настоящей работы является изучение отношения к конфиденциальным сведениям, затрагиваемым в процессе сбора информации Национальными цифровыми библиотеками Южной Америки. В основу работы было положено зондирующее исследование в цифровых библиотеках с целью определения данных, собранных при осведомленности пользователя и при явном присутствии политики конфиденциальности. Кроме того, нами использовались инструменты "Wireshark" для изучения возможного сбора данных Национальной библиотекой Бразилии. Мы определили, что только две цифровые библиотеки предоставляют руководство относительно конфиденциальной информации. Что же касается сбора данных, то информация, собранная без соответствующего осознания пользователем, выделяется при сравнении с теми данными, которые пользователь представляет сознательно. В результате был сделан вывод о том, что на вопросы, связанные с конфиденциальностью, оказывает влияние слабая осведомленность пользователя о времени, способах и местах, где осуществляется сбор информации. Для повышения уровня осведомленности о данном процессе существенным условием является наличие доступа к политике конфиденциальности.

Delisting and ethics in the library: Anticipating the future of librarianship in a world that forgets

Исключение из списков и библиотечные этические принципы: предвидение будущего библиотечного дела в забывающем мире

Кейти Чемберлен Критикос

IFLA Journal, 44-3, 183-194

Аннотация:

Общепринятая библиотечная этика стоит на страже конфиденциальных сведений и содействует доступу к информации. Право на забвение, а также исключение из списков обладают потенциалом для создания новой информационной экосистемы в режиме онлайн, которая разрушает этические нормы и переосмысливает роль библиотекарей. Наряду с фильтрованием сети Интернет, право на забвение и исключение из списков являются предвестниками грядущих перемен в сфере регулирования содержания и доступа к информации в режиме онлайн. Библиотекарям стоит сейчас уделить внимание вопросам, связанным с правом на забвение и с исключением из списков, для того чтобы подготовиться к возможным будущим нестроениям в информационных потоках библиотеки, а также к сдвигам в информационной политике и соответствующих законах по всему миру. В настоящей работе сформулированы правовые и этические вопросы, связанные с исключением из списков, заложено основание для международного диалога по вопросу исключения из списков, а также содержится указание на необходимость будущих исследований. Международное библиотечное сообщество нуждается в широком обсуждении вопросов, связанных с правом на забвение, а также с исключением из списков, в особенности в отношении законов и положений, касающихся свободы слова и конфиденциальности.

Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries

Стимулирование использования клиентами технологий, направленных на защиту конфиденциальных сведений: вызов для общественных библиотек

Моника Мачели

IFLA Journal, 44-3, 195-202

Аннотация:

Наличие угроз для конфиденциальных сведений посетителей библиотек уже в течение длительного времени вызывает у нас озабоченность, притом что наши обязанности были преимущественно ограничены физическим пространством библиотеки. Сегодня под влиянием передовых технологий картина сильно изменилась, и конфиденциальная информация наших посетителей

подвергается угрозам со стороны постоянно растущего количества объектов. В гуще этих хитросплетений библиотеки по-прежнему привержены идее сохранения конфиденциальной информации, и сейчас общественные библиотеки стараются просвещать своих посетителей в таких вопросах, как угрозы для личной информации, защитные меры и методы, которыми те могут воспользоваться. В данном обзоре литературы предпринимается попытка обозначить задачи общественных библиотек Соединенных Штатов в деле просвещения и пропаганды использования клиентами методов из области технологий защиты конфиденциальной информации; обзор основан на исследованиях в различных смежных областях, при этом в нем предлагаются направления для дальнейших исследований. Задачи, определенные в рамках настоящей работы, включают в себя: существенные пробелы в знаниях в области технологий у наших клиентов, библиотекарей и работников библиотек; необходимость поддержки большого количества технологических средств и методов, а также формирование нашего понимания перспективных решений, заложенных создателями в основу соответствующих технологических средств.

Information disclosure and privacy behaviours regarding employer surveillance of SNS

азглашение информации и обращение с конфиденциальными данными в свете изучения социальных сетей работодателями

Деирдри МакГиннесс, Ануш Саймон
IFLA Journal, 44-3, 203-222

Аннотация:

В рамках настоящей работы рассматривается использование сайтов социальных сетей (SNS) студентами университета в Уэльсе, при этом особое внимание уделяется действиям в области обмена информацией и обращения с конфиденциальными данными, а также изучается потенциальное влияние проверок SNS работодателями на будущее использование данных сайтов. Для изучения предмета настоящей работы использовался смешанный метод исследования, включающий как количественный, так и качественный подходы.

Результаты показали, что участники стремились к сохранению конфиденциальности в сети и были осторожны в части размещения и защиты информации в SNS, однако защитные меры были несовершенны в связи с ошибками как человека, так и системы. Большинство респондентов было осведомлено о наблюдении за SNS, и многие заметили, что это окажет влияние на использование этих сайтов в будущем, при этом пользователи предпринимают действия, направленные на защиту своих конфиденциальных данных, включающие сочетание используемых настроек конфиденциальности и различных уровней разглашения информации в зависимости от контекста.

Privacy and libraries in the case of Japan

Конфиденциальность и библиотеки в Японии

Ясуё Иноуэ

IFLA Journal, 44-3, 223-228

Аннотация:

В данном эссе представлена концепция конфиденциальности с точки зрения Японии, государства из Восточной Азии. В работе сначала изложена базовая информация о понятии конфиденциальности в стране, после чего обсуждаются соответствующие законодательные подходы к защите конфиденциальных сведений в Японии. Далее рассматривается понятие конфиденциальности в контексте ее применимости в библиотеках, и в качестве иллюстрации приводится анализ двух примеров из практики, после чего следует заключение, в котором содержатся некоторые предложения относительно дальнейшего пути развития в Японии.

Privacy, obfuscation, and propertization

Конфиденциальность, искажение и собственничество

Тони Дойл

IFLA Journal, 44-3, 229-239

Аннотация:

По мере распространения нашей цифровой волны огромные массивы данных приготовились к тому, чтобы оседлать ее, используя свои аналитические методы, для получения неутешительных заключений о наших характерах, предпочтениях и будущем поведении. Данная работа посвящена массивам данных, представляющим серьезную проблему для конфиденциальной информации. Я рассматриваю явления, которые, возможно, являются двумя наиболее перспективными

попытками отразить нападение массивов данных на конфиденциальную информацию: умышленное искажение персональных данных и "собственничество" в отношении их. Цель умышленного искажения данных заключается в том, чтобы сбить сборщиков информации с нашего цифрового следа путем дезориентации или введения в заблуждение. Собственничеством называется отношение к персональной информации как к интеллектуальной собственности, что требовало бы предоставления держателем информации компенсации в пользу субъекта информации за каждое повторное ее использование. Я пытаюсь показать, что обе защитные стратегии преимущественно неэффективны. Я делаю вывод о том, что битва за конфиденциальные данные проиграна, и что нам следует прекратить попытки защитить их с моральной точки зрения. В заключение я привожу некоторые рассуждения о значении всего вышеупомянутого для библиотек.

Resúmenes

Privacy awareness issues in user data collection by digital libraries

Cuestiones de sensibilización en materia de privacidad en la recopilación de datos de usuarios realizada por las bibliotecas digitales

Elaine Parra Affonso, Ricardo César Gonçalves Sant'Ana

IFLA Journal, 44-3, 170-182

Resumen:

este trabajo tiene como objetivo investigar los aspectos de privacidad en la recopilación de datos realizada por las Bibliotecas digitales nacionales de América del Sur. La metodología se basó en la investigación exploratoria en bibliotecas digitales para identificar los datos compilados con la sensibilización del usuario y la presencia explícita de políticas de privacidad. Asimismo, utilizamos la herramienta Wireshark para examinar la posible recopilación de datos realizada por la Biblioteca Nacional de Brasil. Determinamos que solo dos bibliotecas digitales ofrecen unas directrices de privacidad. Con respecto a la recopilación de datos, la información compilada sin percepción del usuario destaca, en comparación con lo que los usuarios ponen a disponibilidad de manera consciente. Se llega a la conclusión de que las cuestiones relacionadas con la privacidad pueden verse afectadas por la escasa sensibilización del usuario sobre cuándo, cómo y dónde se recopilan los datos. La disponibilidad de políticas de privacidad resulta esencial en las bibliotecas digitales para aumentar la sensibilización sobre este proceso.

Delisting and ethics in the library: Anticipating the future of librarianship in a world that forgets
Eliminación de las listas y ética en la biblioteca: cómo anticipar el futuro de la bibliotecología en un mundo que olvida

Katie Chamberlain Kritikos

IFLA Journal, 44-3, 183-194

Resumen:

la ética del bibliotecario tradicional protege la privacidad y fomenta el acceso a la información. El derecho a ser olvidado (RTBF, por sus siglas en inglés) y la eliminación de las listas poseen el potencial para crear un nuevo ecosistema de información en línea que perturba las normas éticas y permite una nueva definición del papel de los bibliotecarios. Junto con el filtrado de Internet, el RTBF y la eliminación de las listas anuncian los cambios venideros en la regulación de los contenidos y del acceso a la información en línea. Los bibliotecarios deberían ahora comprometerse con las cuestiones relativas al RTBF y a la eliminación de las listas a fin de prepararse ante posibles perturbaciones en el flujo de la información en la biblioteca y cambios en las políticas y leyes sobre información por todo el mundo. Este artículo formula las cuestiones legales y éticas asociadas con la eliminación de las listas, sienta las bases para un diálogo internacional sobre dicha eliminación de las listas y señala la necesidad de seguir investigando sobre el tema. La comunidad internacional de bibliotecarios necesita un debate más amplio sobre las cuestiones relacionadas con el RTBF y la eliminación de las listas, especialmente en lo que a leyes y políticas sobre libertad de expresión y privacidad se refiere.

Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries

Cómo fomentar la adopción de tecnologías de protección de la privacidad en los clientes: retos para las bibliotecas públicas

Monica G. Maceli

IFLA Journal, 44-3, 195-202

Resumen:

a las bibliotecas siempre nos han preocupado las amenazas a la privacidad de nuestros clientes, aunque nuestras responsabilidades se han visto en gran medida limitadas por el espacio físico de las bibliotecas. En la actualidad, impulsado por las nuevas tecnologías, el panorama es muy diferente, y vemos que la privacidad de nuestros clientes está amenazada por un número creciente de entidades. En esta complejidad, las bibliotecas siguen comprometidas con la privacidad; en la actualidad las bibliotecas públicas intentan educar a los clientes sobre los peligros que amenazan a la privacidad, las medidas de protección y las herramientas que pueden emplear. Este examen de documentos pretende identificar los retos a los que se enfrentan las bibliotecas de Estados Unidos a la hora de educar y defender el uso por parte de los clientes de herramientas de tecnología para la protección de la privacidad. Se basa en la investigación en una serie de campos afines, al tiempo que sugiere nuevos horizontes de investigación. Entre los asuntos identificados se encuentran los siguientes: deficiencias importantes en el conocimiento relacionado con la tecnología de nuestros clientes, bibliotecarios y personal de las bibliotecas; la necesidad de ser compatibles con un gran número de herramientas de tecnología y técnicas; así como el aumento de nuestra comprensión de la perspectiva de los creadores de base de las herramientas.

Information disclosure and privacy behaviours regarding employer surveillance of SNS

Divulgación de la información y conductas de privacidad con respecto a la vigilancia de los SNS realizada por los empleados

Deirdre McGuinness, Anoush Simon

IFLA Journal, 44-3, 203-222

Resumen:

este ensayo explora el uso de los sitios de redes sociales (SNS, por sus siglas en inglés) entre la población estudiantil de una universidad galesa, centrándose en la conductas relacionadas con el intercambio de información y la privacidad, así como en el impacto potencial de las verificaciones de los SNS realizadas por los empleadores en el uso futuro de estos sitios. Se utilizó un diseño de investigación que combina diferentes métodos, incorporando tanto enfoques cuantitativos como cualitativos, para examinar la cuestión de la investigación.

Los resultados demostraron que a los participantes les preocupaba el mantenimiento de la privacidad en línea y tenían cuidado en lo referente a la publicación y a la protección de la información en los SNS; sin embargo, las medidas de protección eran imperfectas debido a errores humanos y del sistema. La mayoría de las personas eran conscientes de la vigilancia de los SNS, y muchas señalaban que esto tendría un impacto en su uso futuro. No obstante, los usuarios participan de forma activa en la protección de su privacidad mediante una combinación del uso de ajustes de privacidad y diversos niveles de divulgación de la información, según el contexto.

Privacy and libraries in the case of Japan

Privacidad y bibliotecas en el caso de Japón

Yasuyo Inoue

IFLA Journal, 44-3, 223-228

Resumen:

este ensayo introduce el concepto de privacidad desde la perspectiva del país del sol naciente. En primer lugar, proporciona el contexto de fondo sobre cómo se entiende la privacidad en Japón; a continuación, explica los enfoques legislativos relevantes en lo tocante a la protección de la privacidad en el país. Después trata la privacidad con relación a su relevancia para las bibliotecas, ilustrada con dos estudios de caso, y concluye con algunas sugerencias sobre el camino a seguir en Japón.

Privacy, obfuscation, and propertization

Privacidad, confusión y tenencia en propiedad

Tony Doyle

IFLA Journal, 44-3, 229-239

Resumen:

a medida que nuestro despertar digital se expande, el Big Data está ahí para aprovecharlo, aplicando su analítica para hacer deducciones inquietantes sobre nuestras personalidades, preferencias y conductas futuras. Este artículo aborda el reto que el Big Data representa para la privacidad. Examino lo que quizás son los dos intentos más prometedores de repeler el ataque a la privacidad del Big Data: la confusión y la tenencia en propiedad de la información personal. La confusión intenta que los encargados del acopio de datos pierdan nuestro rastro digital, ofuscándolos

o engañándolos. La tenencia en propiedad exige que la información personal se trate como propiedad intelectual y requeriría que los propietarios de la información compensasen a los personas a las que se refieren dichos datos por cualquier uso secundario que se hiciese de los mismos. Intento mostrar que ambas defensas fracasan en gran medida. Concluyo que la privacidad es una causa perdida y que deberíamos dejar a un lado todos los intentos por defenderla desde el punto de vista moral. Acabo con algunas ideas sobre las implicaciones que esto tiene para las bibliotecas.