10-2015

Enhancing Key Digital Literacy Skills: Information Privacy, Information Security, and Copyright/ Intellectual Property

Jacquelyn A. Burkell
Faculty of Information and Media Studies, University of Western Ontario, jburkell@uwo.ca

Alexandre Fortier
Faculty of Information and Media Studies, University of Western Ontario, afortie@uwo.ca

Lisa Di Valentino
Faculty of Information and Media Studies, University of Western Ontario, ldivalen@uwo.ca

Sarah T. Roberts
Faculty of Information and Media Studies, University of Western Ontario, sarah.roberts@ucla.edu

Western
FIMS
Faculty of Information & Media Studies

Enhancing Key Information Literacy Skills

Information Security, Information Privacy, and Information Ownership

Jacquelyn Burkell, Ph.D.
Associate Professor and Assistant Dean, Research

Alexandre Fortier, M.S.I.
Doctoral Candidate

Lisa Di Valentino, M.A, M.L.I.S., J.D.
Doctoral Candidate

Sarah Roberts, Ph.D.
Assistant Professor

Faculty of Information and Media Studies
The University of Western Ontario

Knowledge synthesis report submitted to the
Social Sciences and Humanities Research Council of Canada

London, Ontario
30 October 2015

Contents

Key Messages

Background

- Knowledge and skills in the areas of information security, information privacy, and copyright/intellectual property rights and protection are of key importance for organizational and individual success in an evolving society and labour market in which information is a core resource.
- Organizations require skilled and knowledgeable professionals who understand risks and responsibilities related to the management of information privacy, information security, and copyright/intellectual property.
- Professionals with this expertise can assist organizations to ensure that they and their employees meet requirements for the privacy and security of information in their care and control, and in order to ensure that neither the organization nor its employees contravene copyright provisions in their use of information.
- Failure to meet any of these responsibilities can expose the organization to reputational harm, legal action and/or financial loss.

Context

- Inadequate or inappropriate information management practices of individual employees are at the root of organizational vulnerabilities with respect to information privacy, information security, and information ownership issues. Users demonstrate inadequate skills and knowledge coupled with inappropriate practices in these areas, and similar gaps at the organizational level are also widely documented.
- National and international regulatory frameworks governing information privacy, information security, and copyright/intellectual property are complex and in constant flux, placing additional burden on organizations to keep abreast of relevant regulatory and legal responsibilities.
- Governance and risk management related to information privacy, security, and ownership are critical to many job categories, including the emerging areas of information and knowledge management. There is an increasing need for skilled and knowledgeable individuals to fill organizational roles related to information management, with particular growth in these areas within the past 10 years. Our analysis of current job postings in Ontario supports the demand for skills and knowledge in these areas.

Key Competencies

- We have developed a set of key competencies across a range of areas that responds to these needs by providing a blueprint for the training of information managers prepared for leadership and strategic positions. These competencies are identified in the full report.
- Competency areas include:
  - conceptual foundations
  - risk assessment
  - tools and techniques for threat responses
  - communications
  - contract negotiation and compliance
  - evaluation and assessment
  - human resources management
  - organizational knowledge management
  - planning; policy awareness and compliance
  - policy development
  - project management.

Executive Summary

Background

This report provides the results of a knowledge synthesis examining three key areas of digital literacy: information privacy, information security, and information ownership (copyright/intellectual property). These represent three information management issues that are of key importance for organizational and individual success in an evolving society and labour market in which information is a core resource. The report examines the general state of public knowledge and skills in these areas, discusses workplace and employer requirements for expertise in these domains, and provides an integrated overview of required competencies and training appropriate for professionals responsible for the management of information privacy, security, and copyright/intellectual property in the workplace.

To fulfil the objectives of this Knowledge Synthesis, we identified relevant resources using a wide variety of search techniques (e.g. pearl growing, successive fractions, and forward and backward citation searching) along with a judicious used of controlled vocabularies to ensure exhaustiveness. Our search encompassed: scholarly journals and monographic works within relevant disciplines (e.g. computer science, education, law, library and information science, management, media studies and sociology); grey literature, including reports, press releases, curricula, and policy documents from education government, business, and not-for-profit organizations; newspapers and other popular media sources in Canada and worldwide; court records (to identify legal actions related to privacy, security, or copyright/intellectual property breaches); and position descriptions and job advertisements to identify workplace requirements for these digital literacy skills.

Organizations require significant expertise with respect to these aspects of digital literacy in order to ensure that they and their employees meet requirements for the privacy and security of information in their care and control, and in order to ensure that neither the organization nor its employees contravene copyright provisions in their use of information. Failure to meet any of these responsibilities can expose the organization to reputational harm, legal action and/or financial loss.

Knowledge, Skills, and Expertise in Information Management

Inadequate or inappropriate information management practices of individual employees are at the root of organizational vulnerabilities with respect to information privacy, information security, and information ownership issues. Our review of the literature indicates that, at an individual level, users demonstrate inadequate skills and knowledge coupled with inappropriate practices in these areas, and similar gaps at the organizational level are also widely documented.

User surveys demonstrate a low level of understanding of information security risks and practices, and many users, including those with significant relevant educational backgrounds, show inadequate compliance with basic security practices such as verifying the source of an email before opening an attachment, using anti-virus software, and installing software patches in a timely manner. Training in information and cybersecurity is associated with better security practice, and those who demonstrate basic security awareness are more likely to enact security practices. Discrepancies between attitudes and behaviour related to privacy have are also commonly observed, and individuals typically do not act according to their privacy opinions, preferences or concerns, no matter how strong these are. Internet users demonstrate misunderstanding and lack of knowledge regarding aspects of online privacy including data flows, behavioural tracking, and they have difficulty understanding the content of privacy policies that ostensibly disclose data collection and sharing practices. With respect to creator rights, users sometimes assume that anything on the Internet is free to use, or that it is

permissible to use any copyrighted material if they are not profiting from it; this is consistent with the widespread notion that authors or creators are giving permission for use simply by posting material online. Although there is widespread support for encouraging discovery and innovation along with associated intellectual property rights, many also hold the inconsistent perspective that piracy is not a serious crime. The confusion about creator rights has implications not only for copyright infringement: it also affects user understanding of their *own* intellectual property rights with respect to creative content.

When we shift our attention to organizational security, privacy, and intellectual property knowledge and practices, similar inadequacies emerge. In many cases, organizations fail to meet basic regulatory requirements, such as the requirement for notice given the collection of personal information. Moreover, these same institutions are ill-prepared to address the privacy challenges raised by new technologies, and many fail to address or even consider the privacy challenges raised by transactions across national boundaries. Although organizations recognize the need for information security policies, many operate without such a policy, and among those organizations that *do* have policies, dissemination and enforcement are inconsistent, and the coverage of the policies is far from comprehensive. In some cases, limitations in policies and practices appear to be the result of inadequate understanding at an organizational level. A survey of senior decision makers in small- to medium-sized enterprises in Canada, for example, found that many were unfamiliar with basic issues in intellectual property.

Regulatory Environment

Even at a national level, the regulatory framework for information management is complex and changing. Canada has national and provincial regulations regarding the privacy of personal information that govern both commercial and governmental activities, while copyright is regulated by the *Copyright Act.* Online activities often involve multiple jurisdictions, and organizations must therefore also be cognizant of international regulatory frameworks that apply to their information-related activities and practices. This issue is particularly relevant with respect to transborder data flows and cloud computing. Moreover, regulatory frameworks are in constant flux in response to changing technological and social contexts, and organizations must keep abreast of these changes.

Workplace Demands for Information Management Skills

Governance and risk management related to information privacy, security, and ownership are critical to many job categories, including the emerging areas of information and knowledge management. Responsibility for these aspects of information management falls within the mandate of Chief Information Officers, Privacy Officers, Privacy Managers, Security Officers, and Copyright Officers, and there is a building recognition of the importance of an integrated management approach to these issues. There is an increasing need for skilled and knowledgeable individuals to fill organizational roles related to information management, with particular growth in these areas within the past 10 years. We are also witnessing the rise of associated certification programs, including 'Certified Information Security Manager' (offered by ISACA); 'Certified Information Privacy Professional' (offered by the International Association of Privacy Professionals), and the 'Certificate in Copyright Management' (offered by the Special Libraries Association). Our analysis of current job postings in Ontario reveals significant demand for management expertise in the areas of information privacy, information security, and copyright/intellectual property. This demand crosses sectors including finance, health, technology, and law enforcement, and encompasses positions that include *Director of Compliance, Privacy Officer, Information Security Manager, Corporate Communications Specialist,* and *Information Manager.*

Key Competencies for Information Management

Information management in the areas of privacy, security, and copyright/intellectual property requires a multifaceted training approach. Effective training must augment a focus on technical skills with a situated understanding of the cultural, social, and legal implications of information privacy, security, and ownership; thus, both technological and human issues must be taken into). It is also critical to focus on the international perspective, particularly since regulatory frameworks differ across jurisdictions. We have developed a set of key competencies that responds to these needs by providing a blueprint for the training of information managers prepared for leadership and strategic positions. The report presents specific key competencies in each of these areas for each of information privacy, information security, and copyright/intellectual property.

Competency areas include:

- *Conceptual foundations*: introduction to key concepts (e.g., types of privacy) in each of the three areas.
- *Risk assessment:* skills to assess risks, report, and take action, with a focus on technical, organizational, and external risks.
- *Tools and techniques for threat responses:* responses to key information management threats, including technical, social, and organizational approaches.
- *Communications:* business communication skills, with a focus on policy development and communication, interpretation of regulatory changes, etc.
- *Contract negotiation and compliance:* ability to read and implement complex contractual with a focus on information management implications, including advocacy for organization with respect to informational needs and interests.
- *Evaluation and assessment:* developing, setting, and assessing performance metrics related to key aspects of information management.
- *Human resources management:* development of organizational culture and position development related to information management.
- *Organizational knowledge management:* ability to make strategic recommendations and plan for knowledge management infrastructure, policy, and operations.
- *Planning:* organizational planning for effective information management including strategic, budgetary, technological, and infrastructure planning needs.
- *Policy awareness and compliance:* exposure to pertinent local, provincial, federal, and international information policy and regulation, with a focus on needs specific to Canadian organizations.
- *Policy development:* developing, setting, and implementing organizational information management policies, including ensuring compliance, identification of best practices, and development of appropriate organizational culture.
- *Project management:* project management, including budgets, timelines, staffing, and infrastructure requirements; analysis of implications for information management.

Key Findings

Context

Digital literacy is essential for "creating the right conditions for a world-class digital economy" (Industry Canada, 2010; see also Webber & Johnston, 2000), a "survival skill for the Information Age" (American Library Association, 1989), and a critical expertise "that young people will need to be fully engaged workers and citizens in the knowledge society of the 21st century" (Council of Ministers of Education, Canada, 2011). Digital literacy education is, therefore, one of "the most pressing education and learning issues facing Canadians today" (Council of Ministers of Education, Canada, 2008).

Information privacy, information security, and information ownership (which we will refer to, collectively, as 'information management' throughout this report) are key aspects of digital literacy (Hoffman & Blake, 2003; Joint, 2006; Manguson, 2011; Media Awareness Network, 2010; MediaSmarts, 2012; Hamel, 2011; Warren and Duckett, 2010; Weatherley, 2014). These same principles are reflected in many digital literacy frameworks (see, e.g., British Columbia Ministry of Education, n.d.), and literacy competency standards (see, e.g., Association of College and Research Libraries, 2000). Expertise in these areas of digital literacy (or the lack thereof) has significant economic and workplace implications. Information security or privacy-related breaches, for example, typically result from the actions of employees who did not observe simple workplace data security procedures (Computer Security Institute, 2004). An understanding of copyright and intellectual property issues is also highly valued by employers: a group of key informants representing various sectors of the Canadian economy recently ranked "complying with legal copyright provision" as one of the most important digital skills (Chinien & Boutin, 2011), and employees who lack this knowledge expose organizations to legal actions on the basis of copyright infringement. Good information security and privacy practices (e.g., securing personal information against identity threat, encrypting sensitive information, and installing local firewalls) are also critical digital skills (Chinien & Boutin, 2011), and failing to engage in basic security practices can result in significant information leaks that place organizations at risk: witness, for example, the loss of the personal data of thousands of Canadians by a Human Resources and Skills Development Canada employee (Canadian Press, 2012). For workers, understanding the boundaries between work and private life, which digital technologies have blurred, is also crucial to ensuring a healthy and productive workplace environment (Herbert, 2011; Ibata, 2011). There can be no doubt, therefore, that digital literacy in these areas has significant value in the workplace (Cheuk, 2008; Cooney & Hiris, 2003).

The current technological and social context has increased the demand for information management skills on the part of individuals; this context has also increased the responsibility of organizations vis-à-vis these issues. Organizations require significant expertise with respect to information management In order to ensure that they meet requirements for the privacy and security of information in their care and control, and in order to ensure that neither the organization nor its employees contravene copyright provisions in their use of information. In particular, organizations must have a heightened and up-to-date awareness of: changing technological and social contexts (e.g., increasingly sophisticated security threats using social engineering techniques; Ohaya, 2006); privacy, security, and copyright risks in the online environment; tools and best practices required to ensure privacy, security, and appropriate acknowledgement of information ownership (e.g., knowledge of the tools available to encrypt digital information); and relevant regulatory frameworks that govern privacy, security, and information ownership (e.g., the *Copyright Act*, 1985).

There is, therefore, a complex body of knowledge necessary to manage organizational risk with respect to information management. Moreover, the relevant digital literacy skills have proven to be difficult to teach: among the five information literacy competency standards identified by the

Association of College and Research Libraries (2000), the fifth, which addresses economic, legal, and social issues, has proven the most challenging to address in information literacy training (Lampert, 2004; Prillman, 2012). Although these skills are addressed in digital literacy curricula at elementary and high school levels in Canada (see, e.g., www.digitalliteracy.gov, www.mediasmarts.ca), at universities in Canada and the U.S., and in continuing education opportunities offered (e.g., Certificate in Copyright Management offered by copyrightlaws.com), there continue to exist demonstrable gaps in privacy, security, and copyright literacy (Furnell & Moore, 2014; Trepte et al., 2015; Yankova, Vasileva, Stancheva, & Miltenoff., 2013). This Knowledge Synthesis will help to address these gaps by identifying a comprehensive set of key information management competencies that will assist in the development of Canadian educational initiatives that effectively addresses training needs in the areas of information security, information privacy, and information ownership.

Implications

This Knowledge Synthesis contributes to education and policy related to information security, privacy, and ownership. The project documents the requirement for training in these three key areas of digital literacy, identifies the coverage of existing educational curricula in these areas, and establishes a comprehensive list of key competencies for information management that will prepare Canadians to be competitive in an economic and employment environment that requires sophisticated knowledge of policy, regulation, and best practices in these areas of digital literacy. The project results also assist in the development of continuing education and certification initiatives for Canadian professionals in these key areas of digital literacy. The key competencies identify a training agenda that focuses on contemporary information management in modern organizations and will support the development of employees and managers who are fluent and literate across the three core competencies of intellectual property, information privacy, and information security.

Approach

To fulfil the objectives of this Knowledge Synthesis, we employed a wide variety of search techniques (e.g. pearl growing, successive fractions, and forward and backward citation searching) and a judicious used of controlled vocabularies to ensure exhaustiveness. The search encompassed:

1. Scholarly journals and monographic works within relevant disciplines (e.g. computer science, education, law, library and information science, management, media studies and sociology) along with interdisciplinary work of scholars drawing from multiple disciplines to identify gaps in knowledge and identify evaluations of existing training in the areas of information security, privacy, and ownership;
2. Grey literature, including reports, press releases, curricula, and policy documents from education government, business, and not-for-profit organizations;
3. Newspapers and other popular media sources in Canada and worldwide;
4. Court records (to identify legal actions related to privacy, security, or copyright/intellectual property breaches); and
5. Position descriptions and job advertisements to identify workplace requirements for these digital literacy skills.

A full bibliography of references consulted is presented in Appendix I. Additional details about the methodology, including the databases that were consulted and the search strings that were used, can be found in Appendix II.

Background

We live in an information economy, and the management of information privacy, security, and ownership is critical in almost every organization and business context (Allen, 2006; Chan, 2003; Davison, Clark, Smith, Langford, & Kuo 2003; Fine & Castagnera, 2003; Greenaway & Chan, 2005; Herman, 2002; Solms & Solms, 2004). Organizations collect, store, and analyse information about customers, patients, and patrons; they record and analyse information about their own practices; they develop their own information products; they use information products developed by others. These activities raise requirements and responsibilities with respect to privacy (ensuring that the privacy of individuals is respected in the collection, storage, use, and sharing of personal information), security (ensuring that information assets are protected from unwanted or unauthorized access), and ownership (ensuring that information ownership rights – both those of the organization and those of others whose information is accessed by the organization – are respected). Organizations faced with data breaches, especially those that involve the release of personal information of clients, must carefully manage communications regarding the incident (Veltsos, 2012). In the context of privacy and security, organizations must balance management objectives with legal and ethical obligations (Greenaway, Chan, & Crossler, 2015) and take client perspectives into account in policy development (Greenaway & Chan, 2013). Organizations need to work to optimize employee compliance with information management policies and recommended practices. Evidence suggests that compliance is enhanced when employees feel it will have a positive impact on the organization, when they feel they can be effective in their security practices, and (potentially) when they are rewarded for security practices (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009a; 2009b). Organizations must develop corporate cultures that promote best practices with respect to information management (Dourish & Anderson, 2006; Johnson & Goetz, 2007; Kraemer & Carayon, 2007), and they need to assess the 'fit' between response (e.g., security countermeasures) and employee breach (e.g., information system misuse; D'Arcy & Hovav, 2007). There is virtually no business, non-profit, or government sector immune to these considerations, and concerns about these aspects of information management are raised in areas as diverse as education (Fine & Castagnera, 2003), health (Kelly & McKenzie, 2002), and even farming (Gronau, 2015).

Changes in the technological and social context (e.g., cloud computing, the internet of things, ubiquitous computing, social media, mobile technologies, behavioural tracking, big data, user-generated content tools; see, e.g., Becher et al., 2011; EY, 2014; Henderson, De Zwart, Lindsay, & Phillips, 2010; Palfrey, Gasser, Simun, & Barnes, 2009; Svantesson & Clarke, 2010) are introducing new information management risks and considerations for organizations and individuals. Organizations must ensure that at an individual and corporate level information privacy, security, and copyright/intellectual property practices and policies meet relevant regulatory guidelines – a task that is complicated by the fact that operating online, and especially in a cloud computing environment, raises uncertainty about 'where' an activity is carried out and thus what regulatory frameworks apply. Organizations that collect and hold personal information, for example, incur responsibilities with respect to that information and their handling of it: they are required to provide legally valid notice of collection and use, and they must ensure that their collection, use, and storage of information meets not only regulatory requirements but also client expectations. Security of that personal information is a primary responsibility of organizations; in addition, organizations must protect other valuable information resources that they develop and own. Computer viruses, malware, and social engineering attacks compromise the security of information and systems, and users and organizations must deploy technological responses coupled with policies and training in order to minimize the associated risks. Similarly, organizations must ensure that their intellectual property is protected against unwarranted use; they must also ensure that they and their employees use information and inventions produced by others in ways that respect copyright

and intellectual property regulations. Thus, organizations face a wide variety of information management issues and responsibilities.

Organizations have direct responsibilities *vis-à-vis* information management (e.g., ensuring that they have policies in place that meet regulatory requirements); they also have a corporate interest in ensuring that their information assets are protected both at an organizational level and at the level of individual employee actions (e.g. ensuring that employees comply with provisions designed to protect the security of information assets). At the same time, employers can be held vicariously liable for actions of their employees, including those that breach personal privacy rights (e.g., *Evans v. Bank of Nova Scotia*, 2014; *Hynes v. Western Regional Integrated Health Authority,* 2014; see also Gratton, 2015a), intellectual property rights (*The Canadian Copyright Licensing Agency ("Access Copyright") v. York University*, 2013), and information security (*Condon v. Canada,* 2014). It is incumbent upon the employer to ensure there are corporate or institutional policies relating to data privacy, security, and copyright compliance, and to educate and train employees in the content of the policies. The consequences for an organization of failure or inadequacies in any aspect of information management can be significant, including financial loss and reputational harm (Acquisti, Friedman, & Telang 2006; Ayyagari, 2012; Cavusoglu, Mishra, & Raghunathan, 2004; Garg & Curtis, 2003; Gatzlaff & McCullough, 2010; Ponemon Institute, 2011; Ponemon Institute, 2012), and even the potential for intra-industry transfer of impacts of some breaches (Zafar, Ko, & Osei-Bryson, 2012).

Information security is widely recognized as a critical issue for organizations (ISACA, 2008; Solms & Solms, 2004), and there is increasing focus on the management, as opposed to purely technical, side of security (Dutta & McCrohnan, 2002). In its *Global State of Information Security Survey 2015*, however, PricewaterhouseCoopers (2014) reported that the compound annual growth rate of detected information security incidents had increased 66 per cent year-on-year since 2009, and in 2016 PricewaterhouseCoopers (2015) indicated a further 38 per cent increase, highlighting that existing prevention and detection methods are largely ineffective against increasingly sophisticated security attacks. Security attacks can compromise private information about employees (Roose, 2014); they can also expose organizational to risk of unwanted access to internal information (Hill, 2014), and some security attacks can even paralyze an organization (e.g., malware and/or computer viruses; McCord, 2014). Employees remain the most important source of information security incidents (Boss et al., 2009; DiDio, 2014; PricewaterhouseCoopers, 2015; Richardson, 2007; Siponen & Vance, 2010; Universities UK, 2013; Whitman, 2003). In fact, the incidence of security breaches attributed to the 'human element' (e.g., social engineering attacks such as 'phishing' emails) is increasing, while those attributable to external 'hacking' attacks are on the decline (Ayyagari, 2012).

Security breaches have implications for organizational information assets; they also have implications for the privacy of patrons, consumers, or patients whose personal information is collected by the organization, and security breaches that compromise personal information are among the most serious for an organization. In fact, as Lacey (2009) suggests, "a breach of customer confidentiality has always been one of the most damaging security risks to organisations" (p. 30). Thus, for example, a security breach at Target Corporation exposed credit card and personal data from more than 110 million consumers in December 2013 (Vijayan, 2014; see also Stedman, 2014); this is only one of many such reports in the media. Security breaches of personal information can negatively influence customer confidence (Humphries, 2014), and also have direct financial implications for organizations, in the form of lawsuits and/or decreasing stock values (Acquisti et al., 2006). As a result of hackers accessing and then releasing the personal information of Ashley Madison subscribers (an internet 'dating' service for people wanting to have an affair), for example, the company faces a $578 million class action lawsuit

(Myr, 2015). The same breach resulted in the company CEO stepping down (Garcia, 2015), and hurt a planned IPO (Farrell, 2015; see also Brinded, 2015).

When organizations, or their employees, infringe copyright or intellectual property provisions, the consequences can include negative publicity; the time, inconvenience, and expense of a trial; and financial damages. Many claims are settled out of court, and thus details of the claims and resolution are not available; nonetheless, these out of court settlements represent a significant burden for corporations. In the U.S., courts have upheld criminal copyright infringement charges against individuals accused of sharing software, music and movies (*Capitol Records, Inc. v. Thomas-Rasset*, 2012) with awards as high as US$675,000 (*Sony BMG Music Entertainment v. Tenenbaum*, 2011). In one U.S. case, a student used the university website as a platform to provide access to copyrighted material (McCollum, 1999); he was turned in by the university itself, and eventually convicted under the *No Electronic Theft Act (1997)* against Internet piracy (part of the U.S. *Copyright Act*, 1976). Organizations and web sites have had to defend themselves against copyright infringement claims. In *MGM Studios, Inc. v. Grokster, Ltd.* (2005) the Supreme Court of the United States held that companies behind file sharing programs such as Grokster and Morpheus could be sued for contributing to copyright infringement. Grokster shut down and settled with the plaintiffs rather than face a further suit for actual damages (Borland, 2006), while the creators of Morpheus were found liable for encouraging copyright infringement by users (Duhigg, Gaither, & Chmielewski, 2006). A more routine example, and one that could easily result from a lack of information about copyright, emerges in a Canadian lawsuit. Connon Nurseries, an Ontario firm, was sued by the Software Alliance (also known as the Business Software Alliance, or BSA) for installing software beyond the number of computers allowed by the license ("Software piracy costs Connon Nurseries," 2014). Access Copyright, a collective of copyright owners, brought suit against York University in 2013, claiming that faculty members have used their materials outside the scope of the fair dealing exception, thus infringing copyright (Access Copyright, 2013). In Canada, copyright infringement for commercial purposes can subject a business to statutory damages of up to $20,000 per work infringed (*Copyright Act*, 1985, § 38.1(1)).

Knowledge or Expertise Gaps

Inadequate or inappropriate individual practices—practices of employees—are at the root of organizational vulnerabilities with respect to information privacy, information security, and information ownership issues. Within organizations, individuals are often identified as the 'weakest link' in information security and privacy (Boss et al., 2009; Bulgurcu et al., 2010). If employees demonstrate a low level of understanding of privacy, security or copyright, if they fail to protect their individual rights in these domains, or if they fail to act to protect the rights of others, the organization itself will be at risk. Our review of the literature indicates that, at an individual level, users demonstrate inadequate skills and knowledge coupled with inappropriate practices in these areas. Similar gaps are also documented at the organizational level.

User surveys demonstrate a low level of understanding of information security risks and practices (Al-Hamdani, 2006), and many users, including those with significant relevant educational backgrounds, show inadequate compliance with basic security practices such as verifying the source of an email before opening an attachment, using anti-virus software, and installing software patches in a timely manner (Furnell, Jusoh, & Katsabas, 2006; Teer, Kruck, & Kruck., 2007). Users are lax with their protection of even that most personal and important of devices: the cell phone (Clarke & Furnell, 2005; Jones & Heinrichs, 2012; Jones, Chin, & Aiken, 2014; Tan & Sagala, 2012). In general, too little attention is paid to usability in the development of security tools, with the result that users find them difficult to implement effectively (Furnell, 2007). Users are also vulnerable to 'security complacency' (Mylonas, Kastania, & Gritzalis 2013), for example trusting the security of application repositories to ensure that

'apps' are safe to install rather than carefully attending to security messages, notices, and terms of service. Users are more likely to deploy security features and comply with security policies if they feel they have the knowledge required to use the tools (Workman & Gathegi, 2007; Zhang, Reithel, & Li, 2009). Training in information and cybersecurity is associated with better security practice (Tan & Sagala, 2012), and in particular, those who demonstrate basic security awareness are more likely to enact security practices (Dinev & Hu, 2007). There are demographic differences in security awareness and practices: older adults, for example, are less security-aware and less likely to practice effective information security compared to their younger counterparts (Grimes, Hough, Mazur, & Signorella, 2010) and compared to women, men demonstrate higher levels of risky behaviour (e.g., clicking on a link from an unknown source) coupled with increased use of technical security measures (e.g., encryption, password protection; Jones & Heinrichs, 2012; Mensch & Wilkie, 2011).There is, therefore, widespread evidence that at least some users demonstrate inadequate security practices in their personal lives, and the attitude, knowledge, and skill gaps that lead to these inadequate practices are likely also to influence their behaviour within an organization.

Discrepancies between attitudes and behaviour related to privacy have are also commonly observed (Acquisti & Grossklags, 2004; Berendt, Günther, & Spiekermann, 2005; Metzger, 2006; Joinson, Reips, Buchanan, & Schofield, 2010). In electronic commercial transactions, for instance, individuals do not act according to their privacy opinions, preferences or concerns, no matter how strong these are: people often do not monitor and control the release of their personal information (Berendt et al., 2005; Metzger, 2006). This privacy paradox is also observed in social media, where usage gratification tends to outweigh people's perceived threats to privacy (Barnes, 2006; Debatin, Lovejoy, Horn, & Hughes, 2009). Research on the economics of privacy indeed indicates that the trade-off between information release and information protection is influenced by bounded rationality (i.e. the inability to calculate probabilities for risks) and psychological distortions such as undervaluing long-term risks (Acquisti & Grossklags, 2004). Contrary to the belief that younger people would be more inclined to share information, research suggests that there is no difference between younger and older generations (Hoofnagle, King, Li, & Turow, 2010). Internet users demonstrate misunderstanding and lack of knowledge regarding aspects of online privacy including data flows and behavioural tracking (Lenhart & Madden, 2007; Turow, 2003; Turow, Feldman, & Meltzer, 2005; Ur, Leon, Cranor, Shay, & Wang, 2012), and they have difficulty understanding the content of privacy policies that ostensibly disclose data collection and sharing practices (Leon et al., 2012). These and other results present a consistent picture with respect to information privacy, documenting user confusion about the degree and impact of release of personal information. Again, the lack of knowledge and skill will translate into the organizational context, influencing employee practices with respect to information privacy.

Information ownership—especially the understanding of creator and user rights and responsibilities—is a third critical aspect of information literacy. Electronic materials are easily copied, altered, and distributed with a few clicks of a button. As download speeds increase, it could take only a few minutes to download an entire movie, or to upload it for use by others. Technology makes decentralized peer-to-peer file sharing easy, and (at least on the surface) anonymous. As with file sharing of movies and music, software can easily be downloaded from "torrent" sites. Various factors influence willingness to pirate software, such as the price of the software and its availability (Lau, 2003). Users sometimes assume that anything on the Internet is free to use, or that it is permissible to use any copyrighted material if they are not profiting from that use (MacKay, 2015). An Angus Reid survey in 2009 showed that 45 percent of adult Canadian Internet users believe that they are allowed to download music from the Internet, and 23 percent believe it is against the law but is "not a big deal" (Geist, 2009). Many have the view that author or owner is giving implicit permission to use by posting on the Internet, particularly social media sites (Vilneff, 2015). In some cases, users believe that the use of

copyrighted material is permitted as long as the source is acknowledged; for example Wikipedia editors might contribute non-free images to an article only to be informed that it is copyright infringement and exposes the Wikimedia Foundation to legal liability ("Wikipedia:Copyright violations," 2015). Many users demonstrate inconsistent attitudes toward intellectual property protections (including copyright protection). The large majority of Canadians believe that encouraging discoveries and innovations is important to the future prosperity of Canada and an equally large proportion support or strongly support intellectual property rights. Nonetheless, one quarter of respondents to a poll by Environics Research Group support strong IP laws but at the same time do not consider piracy to be a serious crime; instead of looking to the law, they take cues from peers, government, employers, and parents to determine what is acceptable (Environics Research Group, 2008). Similarly, a large majority of E.U. citizens display strong support for IP and yet at an individual level believe that breaking IP rules can be justified at an individual level because products are too expensive and corporations make too much money (Office for Harmonization in the Internal Market (Trade Marks and Designs), 2013). The confusion about creator rights has implications not only for copyright infringement: it also affects user understanding of their *own* intellectual property rights with respect to creative content. On an individual level, knowledge with respect to rights is often limited: high school and undergraduate students doing research based on government grants, for example, usually do not know who owns the intellectual property in the results of the research and whether they would be listed as an author or creator (Mabrouk, 2013). If employees don't know about intellectual property concepts such as trade secrets, confidential organizational information could be put at risk (Villasenor, 2012).

As with attitudes and practices toward information security and privacy, demographic variables predict differences in copyright attitudes and practices: copyright infringement appears to be more common among men and those in scientific fields as opposed to business and economics (Chiang & Assane, 2002). 'Moral obligation' and perceived risk of prosecution are among the factors that predict decreased intention to engage in at least some forms of copyright violation (music and software piracy; Alleyn, Soleyn, & Harris, 2015). Young people, deeply involved in creating user-generated content and uploading, downloading, streaming and remixing of creative content, demonstrate confusion and misunderstanding related to copyright and intellectual property (Palfrey et al., 2009), and even communication scholars demonstrate confusion about user and creator rights under copyright law (Ad Hoc Committee on Fair Use and Academic Freedom, 2010).

When we shift our attention to organizational security and privacy practices, similar inadequacies emerge. In many cases, organizations fail to meet basic regulatory requirements, such as the requirement for notice given the collection of personal information. Recent data examining large U.S. companies demonstrate that while the large majority of those companies post privacy policies online, the coverage of the policies is, in many cases, insufficient to meet basic Fair Information Practice Principles (Case, King, & Gage, 2015; Li, Stweart, Zhu, & Ni, 2014). Library privacy policies, for example, are frequently insufficient to meet regulatory requirements or effectively protect patron privacy (Burkell & Carey, 2011; Magi 2007; Wang & Zhou, 2012) despite deep organizational and professional commitments to privacy. Moreover, these same institutions are ill-prepared to address the privacy challenges raised by new technologies (Sturges et al., 2003), and many fail to address or even consider the privacy challenges raised by the policies and practices of the outside vendors with whom they transact business (e.g., companies that host online catalogues; Magi 2010). Although organizations recognize the need for information security policies, research suggests that a sizeable proportion of even large organizations operate without such a policy, and among those organizations that *do* have policies, dissemination is inconsistent (Fulford & Doherty, 2003), and the coverage of the policies is far from comprehensive (Doherty, Anastasakis, & Fulford, 2009). A study of U.S. hospitals, for example, indicated that fewer than two-thirds comply with the privacy provisions in the *Health Insurance*

Portability and Accountability Act (1996), and less than one-fifth comply with security provisions in that act (Appari, Anthony, & Johnson, 2009). A 2003 study revealed that many American universities lacked intellectual property policies to protect rights of academics participating in corporate research partnerships (Fine & Castagnera, 2003). Despite the fact that copyright policies are a necessary tool to assist employees (e.g., university faculty members) in ensuring compliance with complex copyright regulation (see, e.g., DiCola & Sag, 2012; Gasaway, 2002; Gould, Lipinski, & Buchanan, 2005), many universities do not make policies available to faculty on their websites (Di Valentino, 2014).

We can document other significant breaches or limitations, beyond compliance with applicable regulatory and legal frameworks, in these areas of information management. Baker and Wallace (2007) demonstrate that information security management strategies are deployed unequally across organizations, and many aspects of information security management are inadequate. One recent study suggests that the majority of data breaches are related to inadequate implementation and enforcement of security policies and processes, suggesting the need for employee training and stricter enforcement of organizational policies (Albrechtsen & Hovden, 2010; Ayyagari, 2012). In some cases, limitations in policies appear to be the result of inadequate understanding at an organizational level. Gratton (2015b), for example, indicates that in Canada, organizational definitions of "personal information" are less inclusive than the definitions used in Canadian legislation; alternatively, organizations fail to define the scope of information protected by policies and instead simply give examples that make personal information look more narrow than "information about an identifiable individual", which is the definition used within the Canadian legal framework. In some cases, knowledge gaps at the management level are evident, with obvious potential consequences. A survey of senior decision makers in small- to medium-sized enterprises in Canada, for example, found that 42% of respondents thought themselves "not familiar" with the term "intellectual property", 62% could not name a type of intellectual property, and 81% could not name an organization in Canada that was responsible for registering intellectual property (Industry Canada, 2007). While larger organizations demonstrate good understanding and awareness of intellectual property rights, the same cannot necessarily be said of smaller organizations: one UK study indicated that small to medium sized businesses are often effectively unaware of the intellectual property system (Pitkethly, 2012).

Regulatory Environment

With respect to legal and policy regulation, the online environment presents significant challenges. Among these is the issue of jurisdiction (Reidenberg, 2005), since online information flows cross-geographic (and thus regulatory) boundaries. As a result organizations must be aware of and conform to the regulatory frameworks in effect in multiple jurisdictions. Negotiating the complex interactions between different regulatory frameworks creates organizational challenges (Baumer, Earp, & Poindexter, 2004), which are exacerbated when we consider transborder data flows (Ruraswamy & Vance, 2001) and the 'cloud' environment (Ruiter & Warneir, 2011). Moreover, regulatory frameworks are constantly in flux, responding to technological advances, changes in public perception, and increasingly sophisticated attacks (see, e.g., Breaux & Baumer, 2011). Effective organizational response to information privacy, security, and copyright/intellectual property issues requires detailed and up-to-date knowledge of the relevant regulatory frameworks. In this section, we address some of the regulatory issues relating to information privacy, security, and copyright.[1]

[1] This is not intended as a comprehensive overview of regulatory frameworks—such an overview is outside the scope of this project. Instead, we intend to flag critical and emerging issues in regulation of privacy, security, and copyright/intellectual property.

Various privacy guidelines have been proposed for the collection, retention and use of personal information in the online environment. Arguably foremost among these is the set of Fair Information Practice Principles (FIPPs) proposed by the United States Secretary's Advisory Committee on Automated Personal Data Systems (1973), which are: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. FIPPs and other guidelines are not themselves enforceable, but their underlying principles form the basis of regulatory frameworks, including Canada's *Privacy Act* (1985), which regulates federal departments and agencies, and *Personal Information Protection and Electronic Documents Act* (2000; PIPEDA) which regulates private sector organizations and federal works undertakings and businesses in respect of employee personal information. PIPEDA applies to commercial activities in all provinces, except for organizations that collect, use or disclose personal information entirely within provinces that have their own privacy laws, which have been deemed substantially similar to PIPEDA (Office of the Privacy Commissioner of Canada, 2013). Organizations must also review their internal privacy practices with respect to employee surveillance to ensure that they conform to relevant legislation. Email monitoring, for example, is an increasingly common organizational practice, and organizations engaging in this activity should understand both their rights and those of their employees (Smith & Tabak, 2009); this is another area where there are significant jurisdictional differences in regulatory frameworks (Determann & Sprague, 2011). Employers accessing the social network profiles of their employees or prospective employees must similarly understand the appropriate and legally valid use of this information source (Sánchez Abril, Levin, & Del Riego, 2012; Slovensky & Ross, 2012; Smith & Kidder, 2010).

Privacy concerns, historically, have focused on the collection, use and retention of personally identifiable information (PII), that is to say, information that explicitly identifies individuals (names, addresses, identifying numbers, etc.). Increasingly, however, organizations are collecting an analyzing non-personally identifiable information (NPII; e.g., Internet Protocol address, browser configuration information and details of browsing behaviour: Soltani, Canty, Mayo, Thomas, & Hoofnagle, 2009; McDonald & Cranor, 2010; Ayenson, Wambach, Soltani, Good, & Hoofnagle, 2011; Chester, 2012). Regulatory bodies (e.g., the Office of the Privacy Commissioner of Canada, the U.S. Federal Trade Commission, and the European Commission) are becoming increasingly sensitized to the privacy issues associated with NPII, with the result that NPII has come to attract the privacy protections that were historically associated with personally identifiable information. At the same time, specific policies and regulations are being developed with respect to this form of data collection: the Federal Trade Commission in the U.S., for example, has developed self-regulatory principles for online behavioural advertising and the 'do not track' legislation, and the Office of the Privacy Commissioner of Canada has put forth a position on privacy and online behavioural advertising.

Canada has recently sanctioned the *Digital Privacy Act* (2015) requiring organizations that experience a breach of the security of personal information under their control, if that breach creates risk of harm to an individual, to provide notice to the Office of the Privacy Commissioner of Canada, to the individuals in question, and to other organizations if that organization could reduce the risk of harm from the data breach. This brings Canadian law into registration with the regulatory framework in almost every state in the United States, and makes Canadian regulations consistent with the *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* developed by the Organization for Economic Co-operation and Development's (2013). Aside from these notice requirements, there are few regulations governing information security programs. One exception is at the federal government level in the United States, where the *Federal Information Security Management Act* (2002*)* requires federal agencies to implement information security programs. The situation is similar in the European context, where current regulations do not require organizations, other than telecommunication companies, to adopt information security measures and to report incidents

(European Commission, 2013). Organizations must thus rely on self-regulated cyber-security frameworks guidelines. Two major sets of guidelines exists: the International Organization for Standardization and International Electrotechnical Commission's (2013) *Information technology—Security techniques—Information security management systems—Requirements* and the U.S. National Institute of Standards and Technology's (2013) *Framework for Improving Critical Infrastructure Cybersecurity*. These guidelines mirror the elements highlighted by the U.S. National Institute of Standards and Technology (2002).

Different jurisdictions have substantially different approaches to privacy and privacy legislation. The European Union (E.U.), for example, has recently enacted the 'right to be forgotten,' which affords E.U. citizens the right to request the deletion of personal information once the data are no longer 'necessary'. Although privacy protection is in general less regulated in the U.S., in that jurisdiction there is a specific act that pertains to the privacy of children in the online context: The *Children's Online Privacy Protection Act* (1998). Because information, including personal data, is often stored digitally on servers in places other than the physical location of the institution, or because a Canadian web site might outsource its database services to a foreign company, it may be that the laws of another jurisdiction, such as the United States, apply. Transborder data flows are a specific concern where the level or type of protection differs in the jurisdictions between which data are flowing. The United States does not have an omnibus information privacy scheme for the private sector comparable to Canada's PIPEDA or the E.U.'s *Data Protection Directive* (1995; Techvibes NewsDesk, 2014). Instead, various federal laws exist to protect different types of information, such as financial or health data. California's state laws include mention of personal information privacy; however, these laws only apply to residents of the state (*Online Privacy Protection Act* (2003). Moreover, all information stored in the U.S. (even information about Canadian residents) is subject to the *USA Patriot Act* (2011) which permits the FBI to access personal information with a court order, and without the individual's consent or knowledge, if that information is believed to be connected to terrorism (Stoddart, 2004; Treasury Board of Canada, 2006). Thus, personal information does not attract the same protections in the U.S. as it does in Canada, and organizations involved in transborder data transfers must be aware of these differences.

The same issues arise with data transfers between the E.U. and other jurisdictions. The E.U.'s *Data Protection Directive* (1995) deals with cross-border flow of personal information by requiring that any non-E.U. jurisdiction to which the data of E.U. member citizens flow must have laws providing an "adequate" level of protection for this data (EC, 1995, Art. 25). The E.U. and the U.S. had entered into a safe harbour agreement in 2000 for this purpose. However, in 2015, a European Court of Justice decision invalidated the pact because "national security, public interest, or law enforcement requirements" in the U.S. have been given primacy over the principles of the safe harbour agreement and the fundamental rights of persons to information privacy (*Schrems v. Data Protection Commissioner*, 2015, para. 86–87). The case was first brought in Ireland after Edward Snowden's revelations about PRISM, a surveillance program of the U.S. National Security Agency (NSA) that collects Internet information and activities of users of online services such as Google and Facebook (O'Brien, 2015). PRISM is not limited to American users; because the infrastructure of the Internet is mostly located in the U.S., Canadian communications (even those between servers physically located in Canada) are often routed through that country ("Canadian network sovereignty ('boomerang routes')," n.d.; McGuire, 2013).

The goal copyright law is to protect the rights of copyright owners while at the same time not discouraging the creative use of materials. This task is complicated by new and emerging technologies that allow uses that were not anticipated in original copyright legislation, developed to address the use of hard copy materials. Copyright law is regularly amended to address these changes. Thus, for example, the Canadian Parliament introduced in 2012 the Non-Commercial User-Generated Content Exception

(also known as the "YouTube" or "mash up" exception), which allows for the creative combination of copyrighted materials by individuals, so long as there is no expectation of commercial exploitation (§ 29.21). Educational exceptions to the Canadian *Copyright Act* (1985) have been added to address issues that arise in distance education (§ 30.01 [telecommunication of lessons]; 30.04 [materials available on the Internet]). These and other exceptions complicate the issue of copyright for those who wish to use copyrighted materials.

Technologies also introduce new mechanisms for copyright protection – and thus new possibilities for breaches of copyright and new questions about user and creator rights. Technological protection measures and digital rights management include a variety of techniques to restrict access to, copying of, or use of digital materials: for example, a web site could be password protected; right-clicking could disabled to prevent copying of content; software use could require a registration key; e-books may be limited in terms of number the ability to save or print content; the geographical reach of a web service can be limited. Both Canadian and U.S. copyright law have provisions protecting DRMs and prohibiting their circumvention in many circumstances. Legitimate users can be inconvenienced by these measures, and for these and other reasons users will often seek ways to 'get around' the restrictions. These include sharing of registration keys or passwords (Rawlinson & Lupton, 2007), the use of 'virtual private networks' to circumvent geographical restrictions on access, or the use of tools to remove digital rights management software. It remains to be seen whether these types of work-arounds would be considered a violation of copyright law. In Canada there has not yet been a court case having directly to do with DRM circumvention, so some details are unclear as to what types of acts would contravene the provision. Even if such acts are not deemed to be infringements of copyright, they might violate the web site or software's terms of use. A web site's terms of use, or a database's subscription licence, might restrict what can be done with the materials, even if the use is otherwise permitted under copyright law.

For the most part, web pages available on the Internet are accessible from any country—and many jurisdictions have their own copyright laws. A Canadian user, for example, might post a mash up video on YouTube, which is located in the U.S. There are important differences between Canadian and American copyright laws that are relevant in this situation: whereas Canada has introduced the user-generated content exception to encourage these creative uses of materials, U.S. copyright law does not have an equivalent provision. American law allows copyright owners to send a "notice and takedown" alert to content providers, who are then obliged to remove the allegedly infringing content. In Canada, the poster is not required to remove the content: instead, they are notified that of a copyright infringement claim against them. The length of copyright protection is shorter in Canada than in the U.S., so some works are in the public domain in Canada (and thus free to use) but still under copyright protection in the U.S. In situations such as these, organizations must be sensitive to issues of jurisdiction (which country's copyright law apply?) and sensitive to the different copyright protections offered in different jurisdictions.

Organizations must also protect their *own* intellectual property within a complex legal environment. In some contexts, questions about intellectual property ownership remain unsettled. Universities have been focusing on partnerships with the private sector (Bradshaw, 2012), face unresolved questions regarding ownership in the output of the project and thus a claim to revenues (Board of Trade of Metropolitan Montreal, 2011; Silvernagel, Schultz, Moser, & Aune, 2009).

Workplace/Employer demand

In the modern economy that is driven in large part by the creation and exchange of information, there is an increased demand in the workplace for skills and expertise related to information privacy, information security, and copyright/intellectual property. These skills are critical to many job categories,

including the emerging area of knowledge management (Van der Veer Martens & Hawamdeh, 2010). Governance and risk management related to information privacy, security, and ownership fall within the mandate of Chief Information Officers, Privacy Officers, Privacy Managers, Security Officers, and Copyright Officers. There is building recognition of the importance of an integrated management approach to many of these issues (e.g. Fahy, 2014; Oliver 2011; Souza, & Prafullchandra, 2015), especially to address emerging technological and social issues that raise organizational challenges in multiple areas of information management (e.g., social media use, see Bertot, Jaeger, & Hansen, 2012). Within the past 10 years we have witnessed a 'remarkable growth' in demand for Chief Privacy Officers (Foege, 2013; International Association of Privacy Professionals, 2010), and in 2013 Cranor and Sadeh (2013) identified 'privacy engineer', which combines technical expertise in privacy and security with legal and policy knowledge, as a 'hot new career'. Similarly, there is an increasing demand for Copyright Officers, most evident in the contexts of libraries (Albitz, 2013) and universities (Crews, 2014; Ferullo, 2014). With respect to copyright/intellectual property, many organizations have historically focused on the protection of their own rights; increasingly, however, they are required to broaden their focus to include organizational and individual practices with respect to the risk of copyright infringement in the use of materials produced outside the organization.

Demand for information management skills is reflected in workplace requirements, and in the development of certification programs related to information management. Park, Jun, and Kim (2015), for example, documented the skill requirements for Information Security Consultants in U.S. and Korean job advertisements, noting that many of these positions required expertise in 'information security management' (security policies, security compliance, security awareness). Their results also identified the 'Certified Information Security Manager' (ISACA, n.d.) accreditation as a key certification for these positions. The International Association of Privacy Professionals (IAPP) offers two certifications related to privacy management: Certified Information Privacy Professional (CIPP), focused on privacy laws and regulations, and Certified Information Privacy Manager (CIPM), launched in 2013, for those who manage day-to-day privacy issues within an organization. In the U.S., the Special Libraries Association offers a Certificate in Copyright Management, and the Copyright Clearance Centre offers the OnCopyright Education Certificate Program.

Even outside the ranks of management, copyright skills are increasingly important. Information professionals (including librarians) and publishers have always required familiarity with copyright in their professional roles (Charbonneau & Priehs, 2014; Cheng & Winter, 2014; Datig & Russell, 2014; Johnson & Simpson, 2005). It is becoming more and more important for many job seekers to have at least some basic intellectual property background. Employers are finding that a lack of intellectual property and information ethics knowledge on the part of employees result in financial costs to a business (Black, 2007). Businesses require policies relating to intellectual property, and they must know how potential employees perceive intellectual property and what they know about it, so that they can communicate these policies (Rawlinson & Lupton, 2007). Others who are self-employed, such as musicians, artists, writers, and entrepreneurs, would also benefit from basic knowledge about intellectual property use and ownership.

In order to understand they key competencies required to prepare employees for IP, information privacy and security-related employment, we must understand what employers are seeking in terms of skills and competencies in these areas. An ideal source for such information is current job postings placed by employers in Canada. Looking at time periods in September and October of 2015, using the employment aggregator Indeed[2], we conducted searches on recent positions posted within the most recent 15 days of the search and seeking employees with skills and competencies through the

[2] http://ca.indeed.com

three key areas of (1) intellectual property skills, (2) information privacy skills and (3) information security skills. We discovered that the need for these competencies spread across 268 jobs in numerous sectors – many of them high-growth and strategic – and at many different skill levels.

Of the 268 jobs found, fully 115 sought employees with competencies in the area of privacy skills and knowledge. One-third (33%) of the collected job listings belonged to the industries of health and elder care, while about one-fifth (21%) was in the financial services industry. This is not surprising, as each of those industries depends on the collection, management and use of very personal information, with particular focus on the regulatory demands and adherence to laws that such practices necessitate. Half of the postings were for private sector companies, and half were for public sector employers. Only 11% were looking for candidates with a high level of knowledge about privacy law, while over half (56%) required some familiarity. Positions were varied, ranging from privacy officer or consultant (10%) to office administrators (11%) to medical practitioners and information technology workers (9% each). One public sector employer included adherence to MFIPPA as a job requirement, no matter the position (including cook). A number of positions mentioned a requirement or preference for CIPP or CIPM certification, including positions related to regulatory compliance in the insurance industry, software development, and the health sector (*Director of Compliance, Privacy Officer, Privacy Analyst, Privacy Manager).*

In the Information Security area, of the 101 jobs returned, the vast majority of solicitations (83%) were for information technology, database, and/or software development, yet those positions crossed over a number of different industrial sectors. Financial services accounted for 41% of the job postings, and 24% were in the area of technology (including engineering). Over 90% of the employers were in the private sector. In this case, many employers were looking for a high level of knowledge in information security (29%), rather than simply mid- or low-level competency, such as in the case of IP or privacy skills. Specific job titles included *Manager of Security Services, Manager of Cyber Security, Information Security Advisor.* In some cases, there was explicit requirement for management or governance of information security, as in the job posting for an *Information Security Governance Specialist* in the banking sector. Some job postings (e.g. for an *Information Security Manager* in the technology sector) also required expertise in legal and regulatory requirements, specifically those related to privacy (e.g. the *Personal Information Protection and Electronic Documents Act*).

Within the parameters described above, 52 job postings were returned that solicited employees with competencies in the intellectual property arena. Almost one-quarter (24%) percent of job listings collected requiring some kind of IP knowledge belonged to the technology industry, and the majority (81%) were in the private sector. Thirty one percent of job listings specified patent knowledge; however, copyright and trademark were each specified in 25% of job listings, and 19% did not specify any particular type of IP. While patent knowledge is obviously valuable to employers, it has not completely overshadowed the other types. Some of the employers (about 20%) were searching for IP experts (high level of IP knowledge), many more only required a medium (43%) or low (30%) level of expertise. This indicates that awareness of these issues is a key competency that employers feel they now need. They do not require experts but, rather, employees who understand the need to seek out information in this area and how it will impact organizational practices, planning and activities. Specific positions that required expertise in copyright issues included a *Corporate Communications Specialist* in police services, and an *Association Medical Information* Manager.

Key Competencies for Information Management

Information privacy, information security, and IP/copyright are complex organizational issues, requiring a multifaceted training approach. These issues are addressed, jointly and singly, in many

disciplines, and training in these areas must take account of these multiple perspectives (Theoharidou & Gritzalis, 2007). Effective training must augment a focus on technical skills with a situated understanding of the cultural, social, and legal implications of information privacy, security, and ownership (Hentea, Dhillon, & Dhillon, 2006); thus, both technological and human issues must be taken into account (Cegielski, 2008; Gritzalis, Theoharidou, & Kalimeri, 2005; Wood, 2004). It is also critical to focus on the international perspective, particularly since regulatory frameworks differ across jurisdictions (Long and White, 2010; White and Long, 2007). To be effective, training should also engage students in 'real-life' scenarios or problems (Humphries-Smith & Adrian, 2012; Karjalainen & Siponen, 2011).

Our examination of the pool of sample recent job postings for skills and competencies solicited in intellectual property, information privacy and information security, makes it clear that competencies in some, if not all, of these areas, are being sought by employers throughout numerous industries and worksites in both the public and private sector. Employers are not necessarily seeking high-level competency or a set of extremely specialized skills in one or two defined areas; instead, the vast majority of postings sought competency at a low or medium level. Importantly, these competencies overlap and are frequently in dialogue with or reliant on knowledge in one of the other key areas. Based on these postings, we anticipate the need for professionals who can respond—beyond an operational level—to a complex and information-rich working environment that requires the balancing and keeping abreast of technology, policy and human factors within organizations and in the larger environmental context. Information managers also need traditional management skills, and the knowledge of how informational management integrates in a larger sense within an organization's strategic direction and operational functions, alongside their information management focus.

We understand the need for employees who can demonstrate broad-based competencies across several intersecting areas, rather than expert, specialization in few, yet no Canadian program we assessed currently delivers these comprehensive competencies across the three key areas or in toto. We also recognize the key need to provide trained professionals who can respond to the specificities and requirements of the Canadian context, at a local, regional/provincial and federal level, yet with an international perspective. We have therefore developed an integrated list of key competencies at the nexus of the need for these broad-based competencies that provide a big-picture lens, while being firmly grounded in the informational perspectives, and needs, of Canadian employees and organizations. This list of key competencies responds to these needs by producing a blueprint for the training of information managers prepared for leadership and strategic positions, rather than more operational specialists. Importantly, it is not sector specific, but, rather, anticipates the need for information management across all industrial sectors.

In the rubric below, we offer examples of the key competencies within the areas of IP, information privacy and information security that our proposed integrated curriculum would provide. We provide a brief description of how each one might be manifested in the context of an integrated information management curriculum and give examples of aspects of the competencies specific to the three key areas. While the key competencies are split into ten distinct competencies or skill areas across the three key areas of IP, information privacy and information security, we note the interrelatedness of the skills—a key to the comprehensive nature of this curriculum. With the ultimate goal of producing information professionals prepared to take on leadership and management roles with an eye toward the informational needs of Canadian organizations and firms, we have proposed a robust training program that can respond to the complex, dynamic information environment of today, and tomorrow.

Examples of Competencies and Skills Development within Key Areas

Competency or Skill Type	Description	Intellectual Property	Information Privacy	Information Security
Conceptual foundations	Introduction to fundamental concepts and components in each of the three key areas.	Develop an understanding of the components of information ownership: the principles of copyright, fair dealing and fair use.	Develop an understanding of the components of privacy: types of personal information; principles of fair information practices; information life cycle.	Develop an understanding of the requirements for effective information security governance: threats; information security strategy; organisational alignment
Risk Assessment	Program participants will gain skills to assess risk across the three areas, with focus on technical, organizational, internal and external risks, and will develop skills needed to report and take actions on risks that are discovered.	Assess business-to-business (b2b) threats to organization's IP, onsite and off. Secure IP through R&D and production, and in storage.	Assess organization for threats to compliance with relevant privacy standards and legislation, both from within and without organization, and take steps to mitigate those threats.	Create a culture of prioritizing information security among organization's employees. Monitor for new and emerging security threats and security gaps in human and technological resources. Work with technical operational teams to remediate threats.
Tool and techniques for threat responses	Introduction to the tools and techniques for responding to threats in the three key areas	Develop an understanding of the tools and techniques used to license information ownership, such as Creative Commons; knowledge regarding appropriate citation practices	Develop an understanding of the tools and techniques used to mitigate information security threats: social engineering awareness, encryption techniques, creation of strong passwords, digital rights management.	Develop an understanding of the of tools and techniques used to mitigate privacy threats: monitoring of behavioural tracking,

Communications	Curriculum will provide appropriate exposure to and development of business communications skills, with emphasis on in the three key areas. This could include training and skills development in policy and contract writing, interpreting regulatory changes, and so on.	Develop written materials describing firm's policies regarding its IP holdings and communicate on this topic with internal and external stakeholders.	Serve as a communications intermediary between the pertinent legal and regulatory frameworks and the local organizational context (internal and external stakeholders) using a variety of communications media (e.g., written documents; web sites; intranets).	Develop ability to translate complex technology issues into implementable, comprehensible information to be put into use by organization's staff members; effective public communication regarding privacy/security breaches
Contract Negotiation and Compliance	Curriculum provides for participants to gain competencies and confidence in their ability to negotiate, read and implement complex contractual agreements (b2b, b2c), and to properly advocate for the organization and its informational needs and interests.	Manage electronic resources, participate in and/or manage vendor/partner negotiation, end-user compliance, and licensing related to organization's IP.	Ensure that any contractual obligations the organization enters into comply with and protect organization's information privacy, and that of staff and customers, and comply with pertinent legal obligations.	Ensure that any contractual obligations the organization enters into comply with and protect organization's information security, and that of staff and customers.
Evaluation and Assessment	Curriculum will develop participant's competencies in the area of programmatic, technological and organizational assessment and evaluation, including developing, setting and assessing performance metrics related to key competency areas.	Ability to asses and evaluate organization's IP program and its management; make recommendations in areas deemed to not meet performance standards.	Ability to asses and evaluate organization's information privacy program and policies; make recommendations in areas deemed to not meet performance standards.	Ability to asses and evaluate organization's information security program and policies; make recommendations in areas deemed to not meet performance standards.
Human Resource Management	Program participants will gain skills in the area of human resource management, with specific focus on the key competency areas. Curriculum will cover the recruitment, retention, evaluation and career- path growth for employees who help organization meet its informational management needs. Skills developed will include cultural competencies, organizational culture, and position development.	Ability to assess and meet organization's needs in the area of IP staffing.	Ability to assess and meet organization's needs in the area of information privacy staffing. Deliver information privacy training to ensure staff compliance and comprehension of information privacy regulations.	Ability to assess and meet organization's needs in the area of information security staffing. Develop and deliver information security training to staff.
Organizational Knowledge Management	Program participants will attain the ability to make strategic recommendations and to plan for the organization's knowledge management	Work with operational employees and technologists to devise best practices for organization's IP management,	Ensure that information privacy considerations are taken into account in the building, deployment and ongoing	Ensure that information security considerations are taken into account in the building, deployment and ongoing

	infrastructure, policy and operations.	and to develop and maintain systems that ensure it over the long term.	management of the organization's information infrastructure and knowledge repositories. Consult with operational and technological teams to make decisions about systems and best practices that will ensure continued compliance will all local and external privacy policy.	management of the organization's information infrastructure and knowledge repositories. Consult with operational and technological teams to make decisions about systems and best practices that will support organization's security policies, practices and infrastructure.
Planning	Participants will gain exposure to the skills required for adequate organizational planning in the three key areas, with a focus on strategic, budgetary, technological and infrastructure planning needs.	Plan for long-term curation of IP (analogue and digital) that focuses on infrastructure and technological requirements, and their budgetary implications, to ensure both security of and access to IP data. Relate plans to the strategic goals of the organization.	Develop strategic plans for organization that focus on information privacy concerns, including data protection of employees and customers. Integrate planning with organizational strategic goals. Plan for appropriate infrastructure and technological spending and forecast informational privacy needs.	Develop strategic plans for organization that focus on information security concerns. Integrate planning with organizational strategic goals. Plan for appropriate infrastructure and technological spending and forecast informational security needs.
Policy Awareness and Compliance	Curriculum will provide exposure to pertinent local, provincial, federal, international informational policy, with a focus on needs specific to Canadian organizations. Information for both public- and private sector organizations will be covered.	Consult with appropriate parties (e.g., legal counsel) to maintain awareness of and compliance with any Canadian and international regulations affecting organization's IP holdings. Stay abreast of changes by maintaining familiarity with pertinent governance and oversight agencies.	Maintain an on-going awareness of the regulatory landscape affecting information privacy of organization's employees, partners and customers, and implement changes as needed to ensure compliance.	Maintain an on-going awareness of the dynamic information security landscape and environment affecting organization’s employees, partners and customers, and implement changes as needed to ensure compliance.
Policy Development	Program participants will develop skills in the arena of developing, setting and implementing policy, intra- and inter-organizationally, with a focus on ensuring compliance with regulatory frameworks, best practices and organizational culture, as they intersect	Develop and implement policy framework around firm's IP and business data utilization, access and storage (analogue and	Create and implement local policies that comply with regulatory frameworks pertinent to the organization at provincial,	Create, monitor and implement ethical guidelines and information-related codes of conduct for organization's

	with the three key areas.	digital).	federal and international levels.	employees.
Project Management	Curriculum will develop participants' competencies in the area of project management, including project budgets, timelines, staffing, and infrastructure requirements and developing appropriate documentation of project activities.	Develop project management skills to support the IP needs of the organization. Projects to include the implementation of new IP management systems, metadata schemata, storage facilities, and similar.	Develop project management skills to support the information privacy needs of the organization. Projects to include the implementation of new privacy regulations or frameworks that could alter the business processes of the organization.	Develop project management skills to support the information security needs of the organization. Projects to include any information security-related undertakings that require specialized, concentrated attention during a finite period of time.

Additional Resources

We include as appendices to this report a full bibliography of resources consulted (Appendix 1), details of our methodology (Appendix 2).

Further Research and Research Gaps

This knowledge synthesis documents the need for training and skills in information privacy, security, and ownership, examines existing training initiatives, and proposes an integrated curriculum for the training of professionals. Our focus is on training for information management roles: Information Officer, Privacy Officer, Security Officer, or Copyright Officer (or management roles that integrate these functions). Future research should explore best practices in the teaching and development of corporate cultures that effectively support appropriate privacy, security, and copyright behaviour on the part of individual employees.

One issue that rose to prominence in our literature review, but which is not within the scope of the current project, is the importance of organizational culture in ensuring good privacy, security, and copyright/intellectual property practices (Berson, Oreg, & Dvir, 2008; Chang and Lin, 2007; Knapp, Marshall, Rainer, & Ford, 2006; Svärd, 2014). The literature suggests that managers have a critical role to play in setting organizational culture and norms (Chang & Ho, 2006; Hu, Dinev, Hart, & Cooke, 2012; Knapp et al., 2006). An organizational culture that focuses on the value (including moral value) of compliance with privacy, security, and copyright/intellectual property policies and best practices is an important determinant of employee compliance, along with judicious use of reward (for compliance) or punishment (for non-compliance) (Bulgurcu et al., 2010; Herath & Rao, 2009a; Herath & Rao, 2009b; Sipponen & Vance, 2010; Workman & Gathegi, 2007). Future research should explore best practices in the development of corporate cultures that effectively support appropriate privacy, security, and copyright behaviour on the part of individual employees (see, e.g., Albrechtsen & Hovden, 2010; Rader, Wash, & Brooks, 2012; Martinez-Moyano, 2011).

Our knowledge synthesis highlights the importance and complexity of the national, international, and transnational regulatory frameworks that govern organizational and individual practices with respect to information privacy, information security and copyright/intellectual property. We have touched on some of the relevant issues (e.g., changing regulatory frameworks, emerging transnational issues, jurisdictional questions), and identified key legislation and policy within the Canadian context. A full treatment of this issue, critically important for success on the international stage, is beyond the scope of this review. This represents another key area for future research.

Knowledge mobilization

Our knowledge mobilization activities focus on two professional audiences: information professionals and educators; we also extend our outreach to policy makers and the general public. Our professional audiences are chosen for different and specific reasons: information professionals because we have identified them as a group whose professional role is likely to include management of information privacy, security, and ownership concerns within corporate, government, and not-for-profit organizations, and educators because the responsibility for providing training in these areas of digital literacy at elementary, secondary, and post-secondary levels falls within their mandate. Our goal in our knowledge mobilization activities is twofold: to heighten the awareness of information privacy, security, and ownership issues as aspects of digital literacy, and to provide some of needed to address these issues. Thus, the goal of our knowledge mobilization activities is to raise awareness of these critical

digital literacy issues, rather than providing comprehensive training to our target audiences: our research has revealed that these are challenging digital literacy issues that require an extensive curriculum in order to provide required expertise.

Our outreach to information professionals began with a presentation to the Canadian Library Association in June 2015. In that presentation, we raised awareness among our professional audience of the need for enhanced skills in these areas of digital literacy. We will be presenting the results of the knowledge synthesis to another information science audience at the Association of Library and Information Science Educators meeting in January 2016, and we intend to return to the Canadian Library Association meeting this spring in order to present our results as followup to our earlier presentation to that group. In October, we developed a workshop on information privacy, security, and ownership and delivered this workshop to teachers in training as part of their required curriculum; this same material will be integrated into other presentations, including workshops for the general public on these issues of information management.

This final report will be posted to an open access research repository at the University of Western Ontario, and copies will be shared directly with the Office of the Privacy Commissioner of Canada and the Ministry of Education. We will over the next year publish this material in the form of peer-reviewed journal articles in business, information studies and/or education journals. Ultimately, the results of this knowledge synthesis will translate directly into educational initiatives. At the University of Western Ontario, information security, privacy, and copyright issues are relevant to our programs in Library and Information Science, Media in Journalism and Communication, and Media Studies, and the curricular issues identified in this report will inform the development of courses in these programs. In addition, we plan develop a graduate program specifically to train competent professionals well versed in the areas of intellectual property (IP), privacy and security. The full range of training/education issues identified in this report will form the basis for the curriculum in that program.

References

Access Copyright. (2013, April 8). Canada's writers and publishers take a stand against damaging interpretations of fair dealing by the education sector [Press release]. Retrieved from http://www.accesscopyright.ca/media/35670/2013-04-08_ac_statement.pdf

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior: Losses, gains, and hyperbolic discounting. In J. Camp & S. Lewis (Eds.), Economics of information security (Vol. 12, pp. 165–178). New York: Springer.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In D. Straub & S. Klein (Eds.), Proceedings of 27th Annual International Conference on Information Systems, paper 94.

Ad Hoc Committee on Fair Use and Academic Freedom. (2010). Clipping our own wings: Copyright and creativity in communication research. Retrieved from http://cmsimpact.org/sites/default/files/documents/pages/ICA_-_Clipping.pdf

Al-Hamdani, W. A. 2006. Assessment of need and method of delivery for information security awareness program. In Proceedings of the 3rd annual conference on Information security curriculum development (pp. 102–108). ACM, New York.

Albitz, R. S. (2013). Copyright information management and the university library: Staffing, organizational placement and authority. The Journal of Academic Librarianship, 39(5), 429–435.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432–445.

Allen, M. (2006). Social engineering: A means to violate a computer system. Bethesda, MD: SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

Alleyn, P., Soleyn, S., & Harris, T. (2015). Predicting accounting students' intentions to engage in software and music piracy. Journal of Academic Ethics, 1-19.

American Library Association. (1989). Presidential Committee on Information Literacy: Final report. Retrieved from http://www.ala.org/acrl/publications/whitepapers/presidential

Appari, A., Anthony, D. L., & Johnson, M. E. (2009). HIPAA compliance: An examination of institutional and market forces. In Proceedings of the 8th Workshop on Economics of Information Systems. London, UK. Retrieved from http://apps.himss.org/foundation/docs/appari_etal2009_hipaacompliance_20091023.pdf

Association of College and Research Libraries. (2000). Information literacy competency standards for higher education. Retrieved from http://www.ala.org/acrl/sites/ala.org.acrl/files/content/standards/standards.pdf

Ayenson, M. D., Wambach, D. J., Soltani, A., Good, N., & Hoofnagle, C. J. (2011). Flash cookies and privacy II: Now with HTML5 and ETag respawning (SSRN Scholarly Paper No. ID 1898390). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1898390

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. Journal of Information Privacy and Security, 8(2), 33–56.

Baker, W. H., & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. IEEE Security & Privacy, 5(1), 36–44.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/1394

Baumer, D. L., Earp, J. B., & Poindexter, J. C. (2004). Internet privacy law: A comparison between the United States and the European Union. Computers & Security, 23(5), 400–412.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. In Proceedings of the 2011 IEEE Symposium on Security and Privacy (pp. 96–111). Washington, DC, USA: IEEE Computer Society.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. Communications of the ACM, 48(4), 101–106.

Berson, Y., Oreg, S., & Dvir, T. (2008). CEO values, organizational culture and firm outcomes. Journal of Organizational Behavior, 29(5), 615–633.

Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. Government Information Quarterly, 29(1), 30–40.

Black, D. (2007). Copyright training in the corporate world. Information Outlook, 11(6), 12–18.

Board of Trade of Metropolitan Montreal. (2011). A look at Canadian university-industry collaboration. Montreal, QC. Retrieved from http://www.ccmm.qc.ca/documents/activities_pdf/autres/2010_2011/ccmm_rdvs-savoir_2011_en.pdf

Borland, J. (2006, May 30). Last waltz for Grokster. CNET. Retrieved September 29, 2015, from http://www.cnet.com/news/last-waltz-for-grokster/

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151–164.

Bradshaw, J. (2012, October 17). The tricky business of funding a university. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/news/national/time-to-lead/the-tricky-business-of-funding-a-university/article4619883/

Breaux, T. D., & Baumer, D. L. (2011). Legally “reasonable” security requirements: A 10-year FTC retrospective. Computers & Security, 30(4), 178–193.

Brinded, L. (2015, April 15). Ashley Madison is staging its IPO in London because Britain has lower moral standards. Business Insider UK. Retrieved from http://uk.businessinsider.com/ashley-madison-aims-to-raise-200-million-in-london-ipo-2015-4

British Columbia Ministry of Education. (n.d.). Profile for digitally literate students. Retrieved from http://www.bced.gov.bc.ca/dist_learning/69profile.htm

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548.

Burkell, J., & Carey, R. (2011). Personal information and the public library: Compliance with Fair Information Practice Principles. Canadian Journal of Information and Library Science, 35(1), 1–16.

California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).

Canadian network sovereignty (“boomerang routes”). (n.d.). Retrieved October 27, 2015, from https://ixmaps.ca/sovereignty

Canadian Press. (2012, December 28). Personal info for thousands lost by federal government: Privacy commissioner notified about loss affecting about 5,000 Canadians. Retrieved from. http://www.cbc.ca/news/canada/story/2012/12/28/privacy-commissioner-hrdsc-lost-info-personal.html

Capitol Records, Inc. v. Thomas-Rasset, 692 F (3d) 899 (8th Cir. 2012). Retrieved from https://scholar.google.ca/scholar_case?case=8202023323419999031

Case C. J., King, D. L., & Gage, L. M. (2015). Online privacy and security at the Fortune 500: An empirical examination of practices. ASBBS E-Journal, 11(1).

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce, 9(1), 69–104. Retrieved from https://www.utdallas.edu/~huseyin/paper/market.pdf

Cegielski, C. G. (2008). Toward the development of an interdisciplinary information assurance curriculum: knowledge domains and skill sets required of information assurance professionals. Decision Sciences Journal of Innovative Education, 6(1), 29–49.

Chan, Y. (2003). Competing through information privacy. In J.N. Luftman (Ed.), Competing in the Information Age: Align in the sand (2nd ed.). New York: Oxford University Press.

Chang, E. S., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438–458.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345–361.

Charbonneau, D. H., & Mcglone, J. (2013). Faculty experiences with the National Institutes of Health (NIH) public access policy, compliance issues, and copyright practices. Journal of the Medical Library Association, 101(1), 21–25.

Cheng, S., & Winter, C. (2014). Copyright skills in academic libraries. Feliciter, 60(2), 8–12.

Chester, J. (2012). Cookie wars: How new data profiling and targeting techniques threaten citizens and consumers in the "big data" era. In S. Gutwirth, R. Leenes, P. D. Hert, & Y. Poullet (Eds.), European data protection: In good health? (pp. 53–77). Dordrecht: Springer Netherlands.

Cheuk, B. (2008). Delivering business value through information literacy in the workplace. Libri, 58: 137-143.

Chiang, E., & Assane, D. (2002). Software copyright infringement among college students. Applied Economics, 34(2), 157–166.

Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (1998).

Chinien, C. & Boutin, F. (2011). Defining essential digital skills in the Canadian workplace: Final report. Retrieved from http://www.nald.ca/library/research/digi_es_can_workplace/digi_es_can_workplace.pdf

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. Computers & Security, 24(7), 519–527.

Computer Security Institute. (2004). Issues, trends 2004: CSI/FBI Computer abuse and security survey. Retrieved from http://www.infragardphl.org/resources/FBI2004.pdf

Condon v. Canada, 2014 FC 250. Retrieved from http://canlii.ca/t/g69g7

Cooney, M., & Hiris, L. (2003). Integrating information literacy and its assessment into a graduate business course: A collaborative framework. Research Strategies, 19(3-4), 213–232.

Copyright Act of 1976, 90 Stat. 2541 (1976).

Copyright Act, R.S.C. 1985, c. C-42. (1985).

Council of Ministers of Education, Canada. (2008). Learn Canada 2020. Retrieved from http://www.cmec.ca/Publications/Lists/Publications/Attachments/187/CMEC-2020-DECLARATION.en.pdf

Council of Ministers of Education, Canada. (2011). Canada's ministers of education move ahead on pan-Canadian priorities. Retrieved from http://www.scics.gc.ca/english/conferences.asp?a=viewdocument&id=170

Cranor, L., & Sadeh, N. (2013). Privacy engineering emerges as a hot new career. IEEE Potentials, 32(6), 7–9.

Crews, K. D. (2014). Copyright and universities: Legal compliance or advancement of scholarship? (The growth of copyright). IPR Info, 2014(2). Retrieved from http://ssrn.com/abstract=2457292

D'Arcy, J., & Hovav, A. (2007). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. Journal of Information Systems Security, 3(2), 1–30.

Data Protection Directive, Official Journal L 281, p. 0031–0050 (1995).

Datig, I., & Russell, B. (2014). Instructing college students on the ethics of information use at the reference desk: a guide and literature review. Reference Librarian, 55(3), 234–246.

Davison, R. M., Clark, R., Smith, H. J., Langford, D., & Kuo, F.-Y. (2003). Information privacy in a globally networked society: Implications for information systems research. Communications of the Association for Information Systems, 12, 341–365.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83–108.

Determann, L., & Sprague, R. (2011). Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States. Berkeley Technology Law Journal, 26(2): 979–1036.

Di Valentino, L. (2014, February 7). Canadian university fair dealing policies, part two [Blog post]. Retrieved from http://fairdealingineducation.com/2014/02/07/canadian-university-fair-dealing-policies-part-two/

DiCola, P., & Sag, M. (2012). An information-gathering approach to copyright policy. Cardozo Law Review, 34(1), 173–247.

DiDio, L. (2014, February 7). Careless, reckless staff are corporate security's biggest threat. E-Commerce Times. Retrieved from http://www.ecommercetimes.com/story/79930.html

Digital Privacy Act, S.C. 2015, c. 32 (2015).

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386–408.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management, 29(6), 449–457.

Dourish, P., & Anderson, K. (2006). Collective information practice: Emploring privacy and security as social and cultural phenomena. Human-Computer Interaction, 21(3), 319–342.

Duhigg, C., Gaither, C., & Chmielewski, D. C. (2006, September 28). Creator of Morpheus is found liable. Los Angeles Times. Retrieved from http://articles.latimes.com/2006/sep/28/business/fi-morpheus28

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67–87.

Environics Research Group. (2008). Looking for leadership: Canadian attitudes toward intellectual property. Retrieved from http://www.wipo.int/ip-outreach/en/tools/research/details.jsp?id=160

European Commission. (2013, February 7). EU Cybersecurity plan to protect open internet and online freedom and opportunity – Cyber security strategy and proposal for a directive. Retrieved October 20, 2015, from http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Evans v. The Bank of Nova Scotia, 2014 ONSC 2135. Retrieved from http://canlii.ca/t/g79cg

EY (2014). Privacy trends 2014: Privacy Protection in the age of technology. London: EY. Retrieved from: http://www.ey.com/Publication/vwLUAssets/EY_-_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf

Fahy, B. (Ed.). (2014). Security leader insights for information protection: Lessons and strategies from leading security professionals. Amsterdam: Elsevier.

Farrell, M. (2015, July 20). How hackers may have hurt a possible Ashley Madison IPO. The Wall Street Journal. Retrieved from http://blogs.wsj.com/moneybeat/2015/07/20/can-ashley-madison-still-go-public-post-hacking/

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 et seq. (2002).

Ferullo, D. L. (2014). Managing copyright in higher education: A guidebook. Lanham, MD: Rowman & Littlefield.

Fine, C. R., & Ottavio Castagnera, J. (2003). Should there be corporate concern? Examining American university intellectual property policies. Journal of Intellectual Capital, 4(1), 49–60.

Foege, A. (2013, February 5). Chief privacy officer profession grows with big data field. Retrieved from http://data-informed.com/chief-privacy-officer-profession-grows-with-big-data-field/

Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: An exploratory investigation. Information Management & Computer Security, 11(3), 106–114.

Furnell, S. (2007). Making security usable: Are things improving? Computers & Security, 26(6), 434–443.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. Computers & Security, 25(1), 27–35.

Furnell, S., & Moore, L. (2014). Security literacy: the missing link in today's online society? Computer Fraud & Security, 2014(5), 12–18.

Garcia, A. (2015, August 28). CEO of Ashley Madison parent company steps down after hack. CNN Money. Retrieved from http://money.cnn.com/2015/08/28/news/ashley-madison-ceo-hack/

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. Information Management & Computer Security, 11(2), 74–83.

Gasaway, L. N. (2002). Drafting a faculty copyright ownership policy. The Technology Source, (March/April 2002). Retrieved from http://technologysource.org/article/drafting_a_faculty_copyright_ownership_policy/

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. Risk Management and Insurance Review, 13(1), 61–83.

Geist, M. (2009, March 12). Angus Reid surveys find public against new media and file sharing ISP levies [Blog post]. Retrieved from http://www.michaelgeist.ca/2009/03/angus-reid-survey/

Gould, T. H., Lipinski, T. A., & Buchanan, E. A. (2005). Copyright policies and the deciphering of fair use in the creation of reserves at university libraries. The Journal of Academic Librarianship, 31(3), 182–197.

Gratton, E. (2015a). 2015 privacy class actions in Canada. Retrieved from http://www.eloisegratton.com/blog/2015/06/23/2015-privacy-class-actions-in-canada/

Gratton, E. (2015b). Top five mistakes when drafting website privacy policies. Retrieved from http://www.eloisegratton.com/blog/2015/07/06/top-five-mistakes-when-drafting-website-privacy-policies/

Greenaway, K. E., Chan, Y. E. (2005). Theoretical explanations for firms' information privacy behaviors. Journal of the Association for Information Systems, 6(6), article 7.

Greenaway, K. E., Chan, Y. E. (2013). Designing a customer information privacy program aligned with organizational priorities. MIS Quarterly Executive, 12(3), 137–150.

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: A conceptual framework. Information Systems Journal, 25(6), 579–606.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of Internet hazards. Educational Gerontology, 36(3), 173–192.

Gritzalis, D., Theoharidou, M., & Kalimeri, E. (2005). Towards an interdisciplinary information security education model. In 4th IFIP World Conference on Information Security Education (pp. 22–35). Moscow: Moscow Engineering Physics Institute. Retrieved from http://scholar.google.com/scholar?cluster=15410215740882931598&hl=en&oi=scholarr

Gronau, I. (2015, June 29). Implementing precision privacy, security, and ownership policies [Blog post]. Retrieved from: http://www.precisionfarmingdealer.com/articles/1516-implementing-precision-data-privacy-security-and-ownership-policies

Hamel, A. v. (2011). The Privacy Piece: Report on privacy competencies in digital literacy programs in Canada, Britain, Australia, America, and Brazil. Ottawa, ON: Office of the Privacy Commissioner of Canada. Retrieved from https://www.priv.gc.ca/information/research-recherche/2011/hamel_201111_e.asp

Health Insurance Portability and Accountability Act of 1996, 10 Stat. 1936 (1996).

Henderson, M., De Zwart, M., Lindsay, D., & Phillips, M. (2010). Legal risks for students using social networking sites. Australian Educational Computing, 25(1), 3–7 Retrieved from http://acce.edu.au/journal/25/1/legal-risks-students-using-social-networking-sites

Hentea, M., Dhillon, H., & Dhillon, M. (2006). Towards changes in information security education. Journal of Information Technology Education: Research, 5(1), 221–233.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154–165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125.

Herbert, W. A. (2011). Workplace consequences of electronic exhibitionism and voyeurism. IEEE Technology and Society Magazine, 30, 25–33. Retrieved from http://works.bepress.com/william_herbert/16/

Herman, M. L. (2002). Managing technology risks: Staying on course and out of trouble. Retrieved from http://www.betterimpact.com/wp-content/uploads/2015/05/Managing-Technology-Risks-Staying-On-Course-and-Out-of-Trouble.pdf

Hill, K. (2014, December 4). Sony Pictures hack was a long time coming, say former employees. Retrieved from http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/

Hoffman, M. & Blake, J. (2003). Computer literacy: Today and tomorrow. Journal of Computer Sciences in Colleges, 18(5), 221-233.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? (SSRN Scholarly Paper). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1589864

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615–660.

Humphries-Smith, T., & Adrian, A. (2012). Intellectual property education–thinking outside the box meets colouring within the lines. International Journal of Learning and Intellectual Capital, 9(3), 337–350.

Humphries, D. (2014, June 11). Survey: Consumer confidence in the security-breach era [Blog post]. Retrieved from http://intelligent-defense.softwareadvice.com/consumer-confidence-security-breach-era-0614/

Hynes v. Western Regional Integrated Health Authority, 2014 NLTD(G) 137. Retrieved from http://canlii.ca/t/gf8z9

Ibata, D. (2011, October 11). Ruling goes against Barrow teacher who lost job over Facebook posting. Atlanta Journal-Constitution. Retrieved from http://www.ajc.com/news/news/local/ruling-goes-against-barrow-teacher-who-lost-job-ov/nQMb8/

Industry Canada. (2007). Canadian small and medium sized enterprises: Baseline awareness of intellectual property. Retrieved from https://www.ic.gc.ca/eic/site/icgc.nsf/eng/04362.html

Industry Canada. (2010). Improving Canada's digital advantage: Strategies for sustainable prosperity. Retrieved from http://publications.gc.ca/collections/collection_2010/ic/Iu4-144-2010-eng.pdf

International Association of Privacy Professionals. (2010). A call for agility: The next-generation privacy professional. York, ME: International Association of Privacy Professionals. Retrieved from http://www.huntonprivacyblog.com/uploads/file/IAPP_Future_of_Privacy.pdf

International Organization for Standardization and International Electrotechnical Commission. (2013) ISO/IEC 27002:2013: Information technology—Security techniques—Code of practice for information security controls. Geneva: ISO.

ISACA. (2008). Top business/technology issues survey results. Rolling Meadows, IL: ISACA. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Top-Business-Technology-Issues-Survey-Results-2008_res_Eng_0808.pdf

ISACA. (n.d.) Certified information security manager. Retrieved from: http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

Johnson, D., & Simpson, C. (2005). Are you the copy cop? Learning & Leading with Technology, 32(7), 14–20.Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. IEEE Security & Privacy, 5(3), 16–24.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure Online. Human–Computer Interaction, 25(1), 1–24.

Joint, N. (2006). Teaching intellectual property rights as part of the information literacy syllabus. Library Review, 55(6), 330–336.

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? Journal of Computer Information Systems, 53(2), 22–30.

Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky business: Students and smartphones. TechTrends, 58(6), 73–83.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. Journal of the Association for Information Systems, 12(8), 518–555.

Kelly, G., & McKenzie, B. (2002). Security, privacy, and confidentiality issues on the internet. Journal of Medical Internet Research, 4(2), e12. Retrieved from http://www.jmir.org/2002/2/e12/

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. Information Management & Computer Security, 14(1), 24–36.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), 509-520.

Lacey, D. (2009). Managing the human factor in information security: How to win over staff and influence business managers. Hoboken, NJ: Wiley.

Lampert, L. D. (2004). Integrating discipline-based anti-plagiarism instruction into the information literacy curriculum. Reference Services Review, 32(4), 347–355.

Lau, E. K. W. (2003). An empirical study of software piracy. Business Ethics: A European Review, 12(3), 233–245.

Lenhart, A., & Madden, M. (2007). Teens, privacy and online social networks: How teens manage their online identities and personal information in the age of MySpace. Retrieved from http://www.pewinternet.org/2007/04/18/teens-privacy-and-online-social-networks/

Leon, P. G., Cranshaw, J., Cranor, L. F., Graves, J., Hastak, M., Ur, B., & Xu, G. (2012). What do online behavioral advertising privacy disclosures communicate to users?. In Proceedings of the 2012 ACM workshop on Privacy in the electronic society (pp. 19-30).

Li, Y., Stweart, W., Zhu, J., & Ni, A. (2014). Online privacy policy of the thirty Dow Jones corporations: Compliance with FTC Fair Information Practice Principles and readability assessment. Communications of the IIMA, 12(3), article 5. Retrieved from http://scholarworks.lib.csusb.edu/ciima/vol12/iss3/5/

Long, J., & White, G. (2010). On the global knowledge components in an information security curriculum – A multidisciplinary perspective. Education and Information Technologies, 15(4), 317–331.

Mabrouk, P. A. (2013). An investigation of the evolution of high school and undergraduate student researchers' understanding of key science ethics concepts. Journal of College Science Teaching, 43(2), 93–99.

MacKay, G. (2015, September 22). The latest Social Media Donkey award unveiled… [Blog post]. Retrieved from http://mackaycartoons.net/2015/09/22/the-latest-social-media-donkey-award-unveiled/

Magi, T. J. (2007). The gap between theory and practice: A study of the prevalence and strength of patron confidentiality policies in public and academic libraries. Library & Information Science Research, 29(4), 455–470.

Magi, T. J. (2010). A content analysis of library vendor privacy policies: do they meet our standards? College & Research Libraries, 71(3), 254–272.

Magnuson, L. (2011). Promoting privacy: Online and reputation management as an information literacy skill. College & Research Libraries News, 72(3), 137–140.

Martinez-Moyano, I. J., Conrad, S. H., & Andersen, D. F. (2011). Modeling behavioral considerations related to information security. Computers & Security, 30(6), 397-409.

McCollum, K. (1999, September 3). Oregon student is convicted of providing pirated music on university web site. The Chronicle of Higher Education, A48.

McCord, M. (2014, February 21). Risks continue to grow for small organizations' IT infrastructure. New Hampshire Business Review. Retrieved from http://www.nhbr.com/February-21-2014/Risks-continue-to-grow-for-small-organizations-IT-infrastructure/

McDonald, A., & Cranor, L. F. (2010). Beliefs and behaviors: Internet users' understanding of behavioral advertising (SSRN Scholarly Paper No. ID 1989092). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1989092

McGuire, P. (2013, June 10). Canadians should be concerned about the NSA and PRISM. VICE. Retrieved October 28, 2015, from http://www.vice.com/en_ca/read/canadians-should-be-concerned-about-the-nsa-and-prism

Media Awareness Network. (2010). Digital literacy in Canada: From inclusion to transformation. Retrieved from http://www.ic.gc.ca/eic/site/028.nsf/eng/00537.html?Open&pv=1

MediaSmarts (2012). Privacy matters for Media Literacy Week 2012! Available online at http://mediasmarts.ca/blog/privacy-matters-media-literacy-week-2012.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. Academy of Information and Management Sciences Journal, 14(2), 91–116.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. Communication Research, 33(3), 155–179. http://doi.org/10.1177/0093650206287076

MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). Retrieved from https://scholar.google.ca/scholar_case?case=864795647667642615 5

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security, 34, 47–66.

Myr, P. (2015, August 20). Class-action lawsuit filed in Canada against Ashley Madison. Global News. Retrieved from http://globalnews.ca/news/2176979/class-action-lawsuit-filed-in-canada-against-ashley-madison/

No Electronic Theft Act,111 Stat. 2678 (1997).

O'Brien, D. (2015, October 5). No safe harbor: how NSA spying undermined U.S. tech and Europeans' privacy. Retrieved October 28, 2015, from https://www.eff.org/deeplinks/2015/10/europes-court-justice-nsa-surveilance

Office for Harmonization in the Internal Market (Trade Marks and Designs). (2013). European citizens and intellectual property: Perception, awareness and behaviour. Alicante, Spain: European Union. Retrieved from https://oami.europa.eu/ohimportal/en/web/observatory/ip_perception

Office of the Privacy Commissioner of Canada. (2013). Interpretation bulletin: Personal information. Retrieved from https://www.priv.gc.ca/leg_c/interpretations_02_e.asp

Ohaya, C. (2006). Managing phishing threats in an organization. In Proceedings of the 3rd Annual Conference on Information Security Curriculum Development (pp. 159–161). New York: ACM.

Oliver, G. (2011). Organisational culture for information managers. Oxford: Chandos Publishing.

Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22575 et seq. (2003). Retrieved from http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579.

Organisation for Economic Co-operation and Development. (2013). Guidelines on the protection of privacy and transborder flows of personal data. Paris: OECD. Retrieved from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Palfrey, J., Gasser, U., Simun, M., & Barnes, R. F. (2009). Youth, creativity, and copyright in the digital age. International Journal of Learning and Media, 1(2), 79–97. Retrieved from https://dash.harvard.edu/handle/1/3128762

Park, S. K., Jun, H. J., & Kim, T. S. (2015). Using online job postings to analyze differences in skill requirements of information security consultants: South Korea versus United States. PACIS 2015 Proceedings, paper 111. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1145&context=pacis2015

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (2000).

Pitkethly, R. H. (2012). Intellectual property awareness. International Journal of Technology Management, 59(3/4), 163–179.

Ponemon Institute. (2011). Reputation impact of a data breach: Executive summary. Retrieved from http://f6ce14d4647f05e937f4-4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/ponemon-institute-study-reputation-impact-data-breach-pdf-w-540.pdf

Ponemon Institute. (2012). 2011 cost of data breach study: United States. Retrieved from http://www.ponemon.org/blog/2011-cost-of-data-breach-united-states

PricewaterhouseCoopers. (2014). The Global State of Information Security survey 2015: Managing cyber risks in an interconnected world. London: PwC. Retrieved from http://www.pwchk.com/home/eng/rcs_info_security_2015.html

PricewaterhouseCoopers. (2015). The Global State of Information Security survey 2016: Turnaround and transformation in cybersecurity. London: PwC. Retrieved from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Prillman, J. S. (2012). Incorporating the fifth standard of ACRL's information literacy competency standards for higher education into information literacy curriculum. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2030958

Privacy Act, R.S.C., 1985, c. P-21 (1985).

Rader, E., Wash, R., & Brooks, B. (2012). Stories as informal lessons about security. In SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security (Article no. 6). Retrieved from https://cups.cs.cmu.edu/soups/2012/proceedings/a6_Rader

Rawlinson, D. R., & Lupton, R. A. (2007). Cross-national attitudes and perceptions concerning software piracy: A comparative study of students from the United States and China. Journal of Education for Business, 83(2), 87–93.

Reidenberg, J. R. (2005). Technology and Internet jurisdiction. University of Pennsylvania Law Review, 153(6), 1951–1974.

Richardson, R. (2007). 2007 CSI computer crime and security survey. Orlando, FL: Computer Security Institute. Retrieved from http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

Roose, K. (2014, December 2). More from the Sony Pictures hack: Budgets, layoffs, HR scripts, and 3,800 social security numbers. Retrieved from http://fusion.net/story/30850/more-from-the-sony-pictures-hack-budgets-layoffs-hr-scripts-and-3800-social-security-numbers/

Rudraswamy, V., & Vance, D. A. (2001). Transborder data flows: Adoption and diffusion of protective legislation in the global electronic commerce environment. Logistics Information Management, 14(1/2), 127–137.

Ruiter, J., & Warnier, M. (2011). Privacy regulations for cloud computing: Compliance and implementation in theory and practice. In S. Gutwirth, Y. Poullet, P. de Hert, & R. Leenes (Eds.), Computers, privacy and data protection: An element of choice (pp. 361-376). Dordrecht: Springer.

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

Schrems v. Data Protection Commissioner, C‑362/14, [2015] ECR I–1. Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en

Silvernagel, C., Schultz, R. R., Moser, S. B., & Aune, M. (2009). Student-generated intellectual property: Perceptions of ownership by faculty and students. Journal of Entrepreneurship Education, 12, 13–33.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.

Slovensky, R., & Ross, W. H. (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, W. P., & Kidder, D. L. (2010). You've been tagged! (Then again, maybe not): Employers and Facebook. Business Horizons, 53(5), 491–499.

Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy? The Academy of Management Perspectives, 23(4), 33–48.

Software piracy costs Connon Nurseries. (2014, December 11). The Belleville Intelligencer. Retrieved from http://www.intelligencer.ca/2014/12/11/software-piracy-costs-connon-nurseries

Solms, B. v., & Solms, R. v. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371–376.

Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2009). Flash cookies and privacy (SSRN Scholarly Paper No. ID 1446862). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1446862

Sony BMG Music Entertainment v. Tenenbaum, 660 F (3d) 487 (1st Cir. 2011). Retrieved from https://scholar.google.ca/scholar_case?case=6349690935852737851

Souza, E. d., & Prafullchandra, H. (2015, July 15). Should this be the era of the Chief Security Privacy Officer? Retrieved from: https://iapp.org/news/a/should-this-be-the-era-of-the-chief-security-privacy-officer

Stedman, A. (2014, December 9). Leaked Sony emails reveal nasty exchanges and insults. Variety. Retrieved from http://variety.com/2014/film/news/leaked-sony-emails-reveal-nasty-exchanges-and-insults-1201375511/

Stoddart, J. (2004). Privacy implications of the USA Patriot Act. Canadian Parliamentary Review, 27(4), 17–24.

Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Iliffe, U., Oppenheim, C., & Hardy, R. (2003). User privacy in the digital library environment: An investigation of policies and preparedness. Library Management, 24(1/2), 44–50.

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review, 26(4), 391–397.

Svärd, P. (2014). Information culture in three municipalities and its impact on information management amidst e-government development. IFLA journal, 40(1), 48–59.

Tan, M., & Sagala Aguilar, K. (2012). An investigation of students' perception of Bluetooth security. Information Management & Computer Security, 20(5), 364–381.

Techvibes NewsDesk. (2014, October 9). How Canada's privacy laws differ from those in US, Europe. Retrieved from http://www.techvibes.com/blog/how-canadas-privacy-laws-differ-from-those-in-us-europe-2014-10-09

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empirical study of students' computer security practices/perceptions. Journal of Computer Information Systems, 47(3), 105–110.

The Canadian Copyright Licensing Agency ("Access Copyright") v. York University, 2013

Theoharidou, M., & Gritzalis, D. (2007). Common body of knowledge for information security. IEEE Security & Privacy, 5(2), 64–67.

Treasury Board of Canada. (2006, March 28). Frequently asked questions: USA PATRIOT ACT comprehensive assessment results. Retrieved October 28, 2015, from http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/usapa/faq-eng.asp

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), Reforming European data protection law (pp. 333–365). Dordrecht: Springer Netherlands.

Turow, J. (2003). Americans & online privacy: The system is broken. Philadelphia, PA: Annenberg Public Policy Center of the University of Pennsylvania. Retrieved from http://repository.upenn.edu/asc_papers/401/

Turow, J., Feldman, L., & Meltzer, K. (2005). Open to exploitation: American shoppers online and offline. Philadelphia, PA: Annenberg Public Policy Center of the University of Pennsylvania. Retrieved from http://repository.upenn.edu/asc_papers/35/

U.S. Department of Justice. (1999, August 20). First criminal copyright conviction under the "No Electronic Theft" (NET) Act for unlawful distribution of software on the Internet [Press release]. Retrieved from http://www.justice.gov/archive/opa/pr/1999/August/371crm.htm

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. Gaithersburg, Md. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology. (2002). Federal Information Security Management Act: Detailed overview. Gaithersburg, Md. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/overview.html

Universities UK. (2013). Cyber security and universities: Managing the risk. Retrieved from http://www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: perceptions of online behavioral advertising. In SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security (Article no. 4). Retrieved from https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12007.pdf

USA Patriot Act, 115 Stat. 272 (2001).

Van der Veer Martens, B., & Hawamdeh, S. (2010). The professionalization of knowledge management. In E. Pankl, D. Theiss-White, & M. C. Bushing M. C. (Eds.), Recruitment, development, and retention of information professionals: Trends in human resources and knowledge management (pp. 139–156). Hershey, PA: IGI Global.

Veltsos, J. R. (2012). An analysis of data breach notifications as negative news. Business Communication Quarterly, 75(2), 192–207.

Vijayan, J. (2014, February 6). Target breach happened because of a basic network segmentation error. Computer World. Retrieved from http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html

Villasenor, J. (2012, November 27). Intellectual property awareness at universities: Why ignorance is not bliss. Forbes. Retrieved from http://www.forbes.com/sites/johnvillasenor/2012/11/27/intellectual-property-awareness-at-universities-why-ignorance-is-not-bliss/

Vilneff, A. (2015, June 2). Ontario woman wants her cut after Instagram photo sells for $90,000 without consent [Comment]. Facebook. Retrieved from https://www.facebook.com/hamiltonspectator/posts/10153265083197247

Wang, Y., & Zhou, H. (2012). Content analysis of library associations' privacy policies in some countries. International Journal of Digital Library Systems, 3(2), 1–12.

Warren, S, & Duckett, K, (2010). "Why does Google Scholar sometimes ask for money?" Engaging science students in scholarly communication and the economics of information. Journal of Library Administration, 50(4), 349-372.

Weatherley, M. (2014). Copyright Education and Awareness – A Discussion Document. Available online at http://www.mikeweatherleymp.com/wp-content/uploads/2014/10/11.pdf.

Webber, S., & Johnston, B. (2000). Conceptions of information literacy: New perspectives and implications. Journal of Information Science, 26, 381-397.

White, G., & Long, J. (2007). Thinking globally: Incorporating an international component in information security curricula. Information Systems Education Journal, 5(39), 3–12.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. Communictions of the ACM, 46(8), 91–95.

Wikipedia:Copyright violations. (2015, September 8). In Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Wikipedia:Copyright_violations&oldid=680083272

Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Computer Fraud & Security, 2004(1), 16–17.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. Journal of the American Society for Information Science and Technology, 58(2), 212–222.

Yankova, I., Vasileva, R., Stancheva, S., & Miltenoff, P. (2013). A bibliographical overview of "copyright literacy" as a key issue in memory institution management. In S. Kurbanoğlu, E. Grassian, D. Mizrachi, R. Catts, & S. Špiranec (Eds.), Worldwide commonalities and challenges in information literacy research and practice (pp. 655–661). Cham, Switzerland: Springer International Publishing.

Zafar, H., Ko, M., & Osei-Bryson, K. M. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. Information Resources Management Journal, 25(1), 21–37. Retrieved from http://digitalcommons.kennesaw.edu/facpubs/2476/

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. Information Management & Computer Security, 17(4), 330–340.

Appendix I: Complete bibliography

3D printing: Copyright and other intellectual property implications for libraries. (2015). Retrieved from https://www.accessola.org/WEB/OLAWEB/Events_ola/Signature_events/Copyright_Symposium.aspx

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behavior & Information Technology, 33(3), 237–248.

Abraham, S. (2011). Information security behavior: Factors and research directions. In 17th Americas Conference on Information Systems 2011, Paper 462. Retrieved from http://aisel.aisnet.org/amcis2011_submissions/462/

Access Copyright. (2013, April 8). Canada's writers and publishers take a stand against damaging interpretations of fair dealing by the education sector [Press release]. Retrieved from http://www.accesscopyright.ca/media/35670/2013-04-08_ac_statement.pdf

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior: Losses, gains, and hyperbolic discounting. In J. Camp & S. Lewis (Eds.), Economics of information security (Vol. 12, pp. 165–178). New York: Springer.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In D. Straub & S. Klein (Eds.), Proceedings of 27th Annual International Conference on Information Systems, paper 94.

Ad Hoc Committee on Fair Use and Academic Freedom. (2010). Clipping our own wings: Copyright and creativity in communication research. Retrieved from http://cmsimpact.org/sites/default/files/documents/pages/ICA_-_Clipping.pdf

Ajzen, I. (1991). Theories of cognitive self-regulation: The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.

Al-Hamdani, W. A. 2006. Assessment of need and method of delivery for information security awareness program. In Proceedings of the 3rd annual conference on Information security curriculum development (pp. 102–108). ACM, New York.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. In Proceedings from Hawaii International Conference on System Science 2012 (pp. 3317–3326).

Al-Shakhouri, N. S., & Mahmood, A. (2009). Privacy in the digital world: Towards international legislation. First Monday, 14(4). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/2146

Alberta Ministry of Education. (2006, December 28). Information and communication technology. Retrieved October 26, 2015, from https://education.alberta.ca/teachers/program/ict/programs.aspx

Albitz, R. S. (2013). Copyright information management and the university library: Staffing, organizational placement and authority. The Journal of Academic Librarianship, 39(5), 429–435.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & Security, 26(4), 276–289.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432–445.

Allen, J. (2009). Security is not just a technical issue. Build Security In. Department of Homeland Security. Retrieved from https://buildsecurityin.us-cert.gov/articles/best-practices/governance-and-management/security-is-not-just-a-technical-issue

Allen, M. (2006). Social engineering: A means to violate a computer system. Bethesda, MD: SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

Alleyn, P., Soleyn, S., & Harris, T. (2015). Predicting accounting students' intentions to engage in software and music piracy. Journal of Academic Ethics, 1-19.

Allman, L., Sinjela, M., & Takagi, Y. (2008). Recent trends and challenges in teaching intellectual property. In Y. Takagi, L. Allman, & M. A. Sinjela (Eds.), Teaching of intellectual property: principles and methods. Cambridge: Cambridge University Press.

Alzamil, Z. A. (2012). Information security awareness at Saudi Arabians' organizations: In information technology employee's perspective. International Journal of Information Security and Privacy, 6(3), 38–55.

Ambrose, M. L. (2014). Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception. Telecommunications Policy, 38(8-9), 800–811.

American Library Association. (1989). Presidential Committee on Information Literacy: Final report. Retrieved from http://www.ala.org/acrl/publications/whitepapers/presidential

An Act Respecting the Protection of Personal Information in the Private Sector, C.Q.L.R. 2015, c P-39.1. Retrieved from http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html

Appari, A., Anthony, D. L., & Johnson, M. E. (2009). HIPAA compliance: An examination of institutional and market forces. In Proceedings of the 8th Workshop on Economics of Information Systems. London, UK. Retrieved from http://apps.himss.org/foundation/docs/appari_etal2009_hipaacompliance_20091023.pdf

Armeding, T. (2014, December 15). The future of security: 11 predictions for 2015. Retrieved from http://www.csoonline.com/article/2857665/data-protection/the-future-of-security-11-predictions-for-2015.html

Ashrafi, N., & Kuilboer, J.-P. (2005). Online privacy policies: an empirical perspective on self-regulatory practices. Journal of Electronic Commerce in Organizations, 3(4), 61–74.

Association of College and Research Libraries. (2000). Information literacy competency standards for higher education. Retrieved from http://www.ala.org/acrl/standards/informationliteracycompetency

Association of Independent Video and Filmmakers, Independent Feature Project, International Documentary Association, National Alliance for Media Arts and Culture, & Women in Film and Video, Washington, D.C., Chapter. (2005). Documentary filmmakers' statement of best practices in fair use. Center for Social Media, American University. Retrieved from http://www.cmsimpact.org/fair-use/best-practices/documentary/documentary-filmmakers-statement-best-practices-fair-use

Atlantic Provinces Education Foundation. (2001). Technology education curriculum. Halifax, NS: Atlantic Provinces Education Foundation. Retrieved from http://www.gnb.ca/0000/publications/curric/techedfound.pdf

Aucher, G., Boella, G., & van der Torre, L. (2011). A dynamic logic for privacy compliance. Artificial Intelligence and Law, 19(2-3), 187–231.

Aurigemma, S. (2013). A composite framework for behavioral compliance with information security policies. Journal of Organizational and End User Computing, 25(3), 32–51.

Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. In Proceedings from Hawaii International Conference on System Science 2012 (pp. 3248–3257).

Ayenson, M. D., Wambach, D. J., Soltani, A., Good, N., & Hoofnagle, C. J. (2011). Flash cookies and privacy II: Now with HTML5 and ETag respawning (SSRN Scholarly Paper No. ID 1898390). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1898390

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. Journal of Information Privacy and Security, 8(2), 33–56.

Bailin, E. (2010). Copyright and fair use for digital learning teacher education initiative 2010. Media Education Lab, Temple University. Retrieved from http://mediaeducationlab.com/pub/copyright-and-fair-use-digital-learning-teacher-education-initiative-2010

Baker, W. H., & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. IEEE Security & Privacy, 5(1), 36–44.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/1394

Barry, D., Barstow, D., Glater, J. D., Liptak, A., & Steinberg, J. (2003, May 11). Correcting the record; Times reporter who resigned leaves long trail of deception. The New York Times. Retrieved from http://www.nytimes.com/2003/05/11/us/correcting-the-record-times-reporter-who-resigned-leaves-long-trail-of-deception.html

Bate, E. (2013, January 11). Verdict in for UW professor accused of plagiarism. Imprint. Retrieved from http://www.uwimprint.ca/article/2553-verdict-in-for-uw-professor-accused

Baumer, D. L., Earp, J. B., & Poindexter, J. C. (2004). Internet privacy law: A comparison between the United States and the European Union. Computers & Security, 23(5), 400–412.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. In Proceedings of the 2011 IEEE Symposium on Security and Privacy (pp. 96–111). Washington, DC: IEEE Computer Society.

Beckers, K., Krautsevich, L., & Yautsiukhin, A. (2015). Analysis of social engineering threats with attack graphs. In Data privacy management, autonomous spontaneous security, and security assurance (pp. 216–232). Cham, Switzerland: Springer International Publishing. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-17016-9_14

Benjamin, D. P., Border, C., Montante, R., & Wagner, P. J. (2003). Undergraduate cyber security course projects. In Proceedings of the 34th SIGCSE Technical Symposium on Computer Science Education (pp. 351–352). New York: ACM.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. Communications of the ACM, 48(4), 101–106.

Berson, Y., Oreg, S., & Dvir, T. (2008). CEO values, organizational culture and firm outcomes. Journal of Organizational Behavior, 29(5), 615–633.

Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. Government Information Quarterly, 29(1), 30–40.

Bezuidenhout, M., Mouton, F., & Venter, H. S. (2010). Social engineering attack detection model: SEADM. In Proceedings from Information Security for South Africa 2010 (pp. 1-8). Piscataway, NJ: IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5588500

Black, D. (2007). Copyright training in the corporate world. Information Outlook, 11(6), 12–18.

Blevins, J. (2013). Uncertainty as enforcement mechanism: The new expansion of secondary copyright liability to internet platforms. Cardozo Law Review, 34(5), 1821–1887.

Bloom, A. (2004, July 23). “Nurseries need copyright classes.” TES. Retrieved from https://www.tes.co.uk/article.aspx?storycode=397958

Blum, S. D. (2009). My word!: plagiarism and college culture. Ithaca, NY: Cornell University Press.

BMG Canada Inc. v. John Doe, 2005 FCA 193. Retrieved from http://canlii.ca/t/1kx1k

Board of Trade of Metropolitan Montreal. (2011). A look at Canadian university-industry collaboration. Montreal, QC. Retrieved from http://www.ccmm.qc.ca/documents/activities_pdf/autres/2010_2011/ccmm_rdvs-savoir_2011_en.pdf

Bogolea, B., & Wijekumar, K. (2004). Information security curriculum creation: A case study. In Proceedings of the 1st Annual Conference on Information Security Curriculum Development (pp. 59–65). New York: ACM. Retrieved October 25, 2015, from http://www.eicar.org/files/bogoleainformationsecuritycurriculumcreation.pdf

Borland, J. (2006, May 30). Last waltz for Grokster. CNET. Retrieved September 29, 2015, from http://www.cnet.com/news/last-waltz-for-grokster/

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151–164.

Bradshaw, J. (2012, October 17). The tricky business of funding a university. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/news/national/time-to-lead/the-tricky-business-of-funding-a-university/article4619883/

Bravender, P., McClure, H. D., & Schaub, G. (Eds.). (2015). Teaching information literacy threshold concepts: Lesson plans for librarians. Chicago: Association of College and Research Libraries.

Breaux, T. D., & Baumer, D. L. (2011). Legally “reasonable” security requirements: A 10-year FTC retrospective. Computers & Security, 30(4), 178–193.

Bridges, L., & Edmunson-Morton, T. (2011). Image-seeking preferences among undergraduate novice researchers. Evidence Based Library and Information Practice, 6(1), 24–40.

Brinded, L. (2015, April 15). Ashley Madison is staging its IPO in London because Britain has lower moral standards. Business Insider UK. Retrieved from http://uk.businessinsider.com/ashley-madison-aims-to-raise-200-million-in-london-ipo-2015-4

British Columbia Ministry of Education. (1996). Information technology: 8 to 12: Integrated resource package. Retrieved from https://www.bced.gov.bc.ca/irp/pdfs/applied_skills/1996infotech810.pdf

British Columbia Ministry of Education. (n.d.). Profile for digitally literate students. Retrieved from http://www.bced.gov.bc.ca/dist_learning/69profile.htm

Bruce, R. (2015, June 3). 5 information security trends DC SMBs need to know about [Blog post]. Retrieved October 26, 2015, from http://www.whymeridian.com/blog/5-information-security-trends-dc-smbs-need-to-know-about

BugMeNot. (n.d.). Terms of use. Retrieved August 30, 2015, from http://bugmenot.com/terms.php

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. In Proceedings from Americas Conference on Information Systems 2009. Paper 419. Retrieved from http://aisel.aisnet.org/amcis2009/419

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548.

Burkell, J., & Carey, R. (2011). Personal information and the public library: Compliance with Fair Information Practice Principles. Canadian Journal of Information and Library Science, 35(1), 1–16.

Callon, M. (1986). The sociology of an actor-network. In M. Callon, J. Law, & A. Rip (Eds.), Mapping the dynamics of science and technology (pp. 19–34). London: MacMillan.

Canadian Intellectual Property Office Information Branch. (2001). Survey of international best practices in intellectual property information dissemination. Hull, QC: Canadian Intellectual Property Office Information Branch.

Canadian network sovereignty (“boomerang routes”). (n.d.). Retrieved October 27, 2015, from https://ixmaps.ca/sovereignty

Canadian Press (2012, December 28). Personal information data of thousands of Canadians lost by federal government. National Post. Retrieved from http://news.nationalpost.com/2012/12/28/personal-information-data-of-thousands-of-canadians-lost-by-federal-government/

Capitol Records, Inc. v. Thomas-Rasset, 692 F (3d) 899 (8th Cir. 2012). Retrieved from https://scholar.google.ca/scholar_case?case=8202023323419999031

Cappelli, D., Moore, A., & Trzeciak. (2012). The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). Boston, MA: Addison-Wesley Professional.

Case C. J., King, D. L., & Gage, L. M. (2015). Online privacy and security at the Fortune 500: An empirical examination of practices. ASBBS E-Journal, 11(1).

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce, 9(1), 69–104. Retrieved from https://www.utdallas.edu/~huseyin/paper/market.pdf

Cegielski, C. G. (2008). Toward the development of an interdisciplinary information assurance curriculum: knowledge domains and skill sets required of information assurance professionals. Decision Sciences Journal of Innovative Education, 6(1), 29–49.

Certificate in copyright management. (2015). Retrieved May 25, 2015, from https://www.sla.org/learn/certificate-programs/cert-copyright-mgmt/

Chan, Y. (2003). Competing through information privacy. In J.N. Luftman (Ed.), Competing in the Information Age: Align in the sand (2nd ed.). New York: Oxford University Press.

Chang, E. S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345-361.

Chang, E. S., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438–458.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345–361.

Charbonneau, D. H., & Mcglone, J. (2013). Faculty experiences with the National Institutes of Health (NIH) public access policy, compliance issues, and copyright practices. Journal of the Medical Library Association, 101(1), 21–25.

Charbonneau, D. H., & Priehs, M. (2014). Copyright awareness, partnerships, and training issues in academic libraries. Journal of Academic Librarianship, 40(3/4), 228–233.

Chase, M. E. (1994). An analysis of the knowledge levels of media directors concerning relevant copyright issues in higher education (Unpublished doctoral dissertation). University of Pittsburgh: Pittsburgh, PA.

Chen, C. C., Medlin, B. D., & Shaw, R. (2008). A cross-cultural investigation of situational information security awareness programs. Information Management & Computer Security, 16(4), 360–376.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Information Technology, Learning & Performance Journal, 24(1), 1–14.

Chen, H., Maynard, S. B., & Ahmad, A. (2013). A comparison of information security curricula in China and the USA. In Proceedings of the 11th Australian Information Security Management Conference. Perth, WA: SRI Security Research Institute. Retrieved from http://ro.ecu.edu.au/ism/153/

Chen, T.-C., Stepan, T., Dick, S., & Miller, J. (2014). An anti-phishing system employing diffused information. ACM Transactions on Information and System Security, 16(4), 16:1–16:31.

Cheng, S., & Winter, C. (2014). Copyright skills in academic libraries. Feliciter, 60(2), 8–12.

Chester, J. (2012). Cookie wars: How new data profiling and targeting techniques threaten citizens and consumers in the "big data" era. In S. Gutwirth, R. Leenes, P. D. Hert, & Y. Poullet (Eds.), European data protection: In good health? (pp. 53–77). Dordrecht: Springer Netherlands.

Cheuk, B. (2008). Delivering business value through information literacy in the workplace. Libri, 58(3), 137–143.

Chiang, E., & Assane, D. (2002). Software copyright infringement among college students. Applied Economics, 34(2), 157-166.

Chiang, E., & Assane, D. (2002). Software copyright infringement among college students. Applied Economics, 34(2), 157–166.

Chinien, C., & Boutin, F. (2011). Defining essential digital skills in the Canadian workplace: Final report. Ottawa, ON: Human Resources and Skills Development Canada. Retrieved from http://www.nald.ca/library/research/digi_es_can_workplace/digi_es_can_workplace.pdf

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719–731.

Choo, K.-K. R., Smith, R. G., & McCusker, R. (2007). Future directions in technology-enabled crime: 2007-09 (Research and public policy series no. 78). Canberra, ACT: Australian Institute of Criminology. Retrieved from http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.html

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. Computers & Security, 24(7), 519–527.

Clement, G., & Brenenson, S. (2013). Theft of the mind: An innovative approach to plagiarism and copyright education. In S. Davis-Kahl & M. K. Hensley (Eds.), Common ground at the nexus of information literacy and scholarly communication (pp. 45–74). Chicago: Association of College and Research Libraries.

Code of best practices in fair use for media literacy education. (n.d.). Center for Social Media, American University. Retrieved October 6, 2015, from http://mediaeducationlab.com/code-best-practices-fair-use-media-literacy-education-0

Computer Security Institute. (2004). Issues, trends 2004: CSI/FBI Computer abuse and security survey. Retrieved from http://www.issa-sac.org/docs/FBI2004.pdf

Concordia University of Edmonton. (n.d.). Master's of Information Security and Assurance at Concordia University of Edmonton. Retrieved October 26, 2015 from http://infosec.concordia.ab.ca/

Condon v. Canada, 2014 FC 250. Retrieved from http://canlii.ca/t/g69g7

Cooney, M., & Hiris, L. (2003). Integrating information literacy and its assessment into a graduate business course: A collaborative framework. Research Strategies, 19(3-4), 213–232.

Copyright Act, R.S.C. 1985, c. C-42. Retrieved from http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-42/latest/rsc-1985-c-c-42.html

Copyright and accessibility: Intrinsically connected. (2015). Retrieved from https://www.accessola.org/web/OLA/iCore/Events/Event_Display.aspx?EventKey=EIW150825&WebsiteKey=74e8da94-41c7-4ad1-9741-aa129f6a2c2c

Copyright Clearance Center. (n.d.). Certificate programs. Danvers, Mass.: Copyright Clearance Center. Retrieved from https://www.copyright.com/content/cc3/en/toolbar/education/certificate_program.html

Copyright for educators and librarians. (n.d.). Retrieved October 6, 2015, from https://www.coursera.org/learn/copyright-for-education

Corriss, L. (2010). Information security governance: Integrating security into the organizational culture. In Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies (pp. 35–41). New York: ACM.

Council of Ministers of Education, Canada. (2008). Education in Canada: An overview. Retrieved from http://www.cmec.ca/299/Education-in-Canada-An-Overview/

Council of Ministers of Education, Canada. (2011, February 23). Canada's Ministers of Education move ahead on pan-Canadian priorities [Press release]. Retrieved from http://www.cmec.ca/278/Press-Releases/Canada's-Ministers-of-Education-Move-Ahead-on-Pan-Canadian-Priorities.html?id_article=256

Courant Rife, M. (2008). “Fair use”, copyright law, and the composition teacher. In C. Eisner & M. Vicinus (Eds.), Originality, imitation, and plagiarism: Teaching writing in the digital age (pp. 145–156). Ann Arbor, MI: University of Michigan Press.

Craig, P. A., Federici, E., & Buehler, M. A. (2010). Instructing students in academic integrity. Journal of College Science Teaching, 40(2), 50–55.

Cranor, L., & Sadeh, N. (2013). Privacy engineering emerges as a hot new career. IEEE Potentials, 32(6), 7–9.

Crews, K. D. (2014). Copyright and universities: Legal compliance or advancement of scholarship? (The growth of copyright). IPR Info, 2014(2). Retrieved from http://ssrn.com/abstract=2457292

Cushing, T. (2014, September 23). Study indicates college textbook piracy is on the rise, but fails to call out publishers for skyrocketing prices. Techdirt. Retrieved August 26, 2015, from https://www.techdirt.com/articles/20140921/19385328596/study-indicates-college-textbook-piracy-is-rise-fails-to-call-out-publishers-skyrocketing-prices.shtml

D’Arcy, J., & Hovav, A. (2007). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. Journal of Information Systems Security, 3(2), 1–30.

D’Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. Journal of Business Ethics, 89(1), 59–71.

D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98.

Dachis, A. (2012, February 27). How you’re breaking the law every day (and what you can do about it). Lifehacker. Retrieved August 7, 2015, from http://lifehacker.com/5888488/how-youre-breaking-the-law-every-day-and-what-you-can-do-about-it

Datig, I., & Russell, B. (2014). Instructing college students on the ethics of information use at the reference desk: a guide and literature review. Reference Librarian, 55(3), 234–246.

Datig, I., & Russell, B. (2015). “The fruits of intellectual labor”: International student views of intellectual property. College & Research Libraries, 76(6), 811–830.

Davison, R. M., Clark, R., Smith, H. J., Langford, D., & Kuo, F.-Y. (2003). Information privacy in a globally networked society: Implications for information systems research. Communications of the Association for Information Systems, 12, 341–365.

De Palma, P., Frank, C., Gladfelter, S., & Holden, J. (2004). Cryptography and computer security for undergraduates. In Nrdings of the 35th SIGCSE Technical Symposium on Computer Science Education (pp. 94–95). New York: ACM.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83–108.

Deloitte, & National Association of State Chief Information Officers. (2014). State governments at risk: Time to move forward. New York: Deloitte. Retrieved from http://www2.deloitte.com/us/en/pages/public-sector/articles/2014-deloitte-nascio-cybersecurity-study.html

Deloitte. (2013). Blurring the lines: 2013 TMT global security study. New York: Deloitte. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/dttl_TMT_GlobalSecurityStudy_English_final_020113.pdf

Determann, L., & Sprague, R. (2011). Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States. Berkeley Technology Law Journal, 26(2): 979–1036.

Di Valentino, L. (2014, February 7). Canadian university fair dealing policies, part two [Blog post]. Retrieved from http://fairdealingineducation.com/2014/02/07/canadian-university-fair-dealing-policies-part-two/

DiCola, P., & Sag, M. (2012). An information-gathering approach to copyright policy. Cardozo Law Review, 34(1), 173–247.

DiDio, L. (2014, February 7). Careless, reckless staff are corporate security's biggest threat. E-Commerce Times. Retrieved from http://www.ecommercetimes.com/story/79930.html

Digital Privacy Act, S.C. 2015, c. 32. Retrieved from http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=8057593&File=9

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386–408.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22(3), 295–316.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. Computers & Security, 28(3–4), 189–198.

Dodge, L., & Sams, J. (2011). Innovative copyright. College & Research Libraries News, 72(10), 596–599.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management, 29(6), 449–457.

Dourado, E., & Castillo, A. (2014). Why the cybersecurity framework will make us less secure. Arlington, VA: Mercatus Center at George Mason University. Retrieved from http://mercatus.org/publication/why-cybersecurity-framework-will-make-us-less-secure

Dourish, P., & Anderson, K. (2006). Collective information practice: Emploring privacy and security as social and cultural phenomena. Human-Computer Interaction, 21(3), 319–342.

Dow, M. J., Boettcher, C. A., Diego, J. F., Karch, M. E., Todd-Diaz, A., & Woods, K. M. (2015). Case-based learning as pedagogy for teaching information ethics based on the Dervin sense-making methodology. Journal of Education for Library & Information Science, 56(2), 141–157.

Dritsas, S., Gritzalis, D., & Lambrinoudakis, C. (2006). Protecting privacy and anonymity in pervasive computing: trends and perspectives. Telematics and Informatics, 23(3), 196–210.

Drummond, C. M. (2005). Guiding learners to ethical use of information in an online learning environment. Journal of Interactive Instruction Development, 18(2), 17–25.

Dryden, J. (2011). Learning about law in library school: A snapshot. Journal of Education for Library & Information Science, 52(3), 184–197.

Duhigg, C., Gaither, C., & Chmielewski, D. C. (2006, September 28). Creator of Morpheus is found liable. Los Angeles Times. Retrieved from http://articles.latimes.com/2006/sep/28/business/fi-morpheus28

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67–87.

EC, Commission Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [2005] OJ, L 281/1. Retrieved from http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046

Edge, C., & Stamey, J. (2010). Security education on a budget: Getting the most "bang for the buck" with limited time and resources. In 2010 Information Security Curriculum Development Conference (pp. 29–35). New York: ACM.

Egeberg, M., Trondal, J., & Vestlund, N. M. (2015). The quest for order: unravelling the relationship between the European Commission and European Union agencies. Journal of European Public Policy, 22(5), 609–629.

Eloff, J., & Eloff, E. (2005). Information security architecture. Computer Fraud & Security, 2005(11), 10–16.

Enrolment by university. (2014). Retrieved from http://www.univcan.ca/canadian-universities/facts-and-stats/enrolment-by-university/

Environics Research Group. (2008). Looking for leadership: Canadian attitudes toward intellectual property. Retrieved from http://www.wipo.int/ip-outreach/en/tools/research/details.jsp?id=160

European Commission. (2013, February 7). EU Cybersecurity plan to protect open internet and online freedom and opportunity – Cyber security strategy and proposal for a directive. Retrieved October 20, 2015, from http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Evans v. The Bank of Nova Scotia. 2014 ONSC 2135. Retrieved from http://canlii.ca/t/g79cg

Executive Office of the President (2007, May 22). Safeguarding against and responding to the breach of personally identifiable information. Retrieved from https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

EY (2014). Get ahead of cybercrime: EY's global information security survey 2014. London: EY. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

EY (2014). Privacy trends 2014: Privacy Protection in the age of technology. London: EY. Retrieved from: http://www.ey.com/Publication/vwLUAssets/EY_-_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf

Eye, J. (2013). Knowledge level of library deans and directors in copyright law. Journal of Librarianship & Scholarly Communication, 2(1), 1–14.

Fahy, B. (Ed.). (2014). Security leader insights for information protection: Lessons and strategies from leading security professionals. Amsterdam: Elsevier.

Farrell, M. (2015, July 20). How hackers may have hurt a possible Ashley Madison IPO. The Wall Street Journal. Retrieved from http://blogs.wsj.com/moneybeat/2015/07/20/can-ashley-madison-still-go-public-post-hacking/

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541. Retrieved October 26, 2015, from https://www.law.cornell.edu/uscode/text/44/3541

Ferullo, D. L. (2014). Managing copyright in higher education: A guidebook. Lanham, MD: Rowman & Littlefield.

Ficsor, M. (2008). Teaching copyright and related rights. In Y. Takagi, L. Allman, & M. A. Sinjela (Eds.), Teaching of intellectual property: Principles and methods (pp. 33–62). Cambridge: Cambridge University Press.

Fine, C. R., & Ottavio Castagnera, J. (2003). Should there be corporate concern? Examining American university intellectual property policies. Journal of Intellectual Capital, 4(1), 49–60.

Foege, A. (2013, February 5). Chief privacy officer profession grows with big data field. Retrieved from http://data-informed.com/chief-privacy-officer-profession-grows-with-big-data-field/

Fomenkova, G. I. (2012). For your eyes only? A “Do Not Track” proposal. Information & Communications Technology Law, 21(1), 33–52.

Fornaciari, F. (2014). Pricey privacy: Framing the economy of information in the digital age. First Monday, 19(12). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/5008

Fraillon, J., Schulz, W., Friedman, T., Ainley, J., & Gebhardt, E. (2015). International Computer and Information Literacy Study 2013 technical report. Amsterdam: IEA. Retrieved from http://www.iea.nl/fileadmin/user_upload/Publications/Electronic_versions/ICILS_2013_Technical_Report.pdf

Francia, G. A., III. (2011). Critical infrastructure security curriculum modules. In Proceedings of the 2011 Information Security Curriculum Development Conference (pp. 54–58). New York: ACM.

Francis, L. P. (2015). Privacy and health information: The United States and the European Union. Kentucky Law Journal, 103. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2590477

Freeman, S. (2015, January 8). Canada’s new unauthorized downloading rules: A Q & A with Michael Geist. The Huffington Post. Retrieved from http://www.huffingtonpost.ca/2015/01/08/michael-geist-copyright-modernization-act_n_6436584.html

Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: An exploratory investigation. Information Management & Computer Security, 11(3), 106–114.

Furnell, S. (2007). Making security usable: Are things improving? Computers & Security, 26(6), 434–443.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? Computer Fraud & Security, 2008(4), 6–9.

Furnell, S. (2010). Jumping security hurdles. Computer Fraud & Security, 2010(6), 10–14.

Furnell, S. M., Clarke, N., Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice. Information Management & Computer Security, 17(1), 53–63.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. Computers & Security, 25(1), 27–35.

Furnell, S., & Moore, L. (2014). Security literacy: the missing link in today's online society? Computer Fraud & Security, 2014(5), 12–18.

Furnell, S., & Thomson, K.-L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud & Security, 2009(2), 5–10.

Futcher, L., Schroder, C., & von Solms, R. (2010). Information security education in South Africa. Information Management and Computer Security, 18(5), 366–374.

Garcia, A. (2015, August 28). CEO of Ashley Madison parent company steps down after hack. CNN Money. Retrieved from http://money.cnn.com/2015/08/28/news/ashley-madison-ceo-hack/

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. Information Management & Computer Security, 11(2), 74–83.

Gasaway, L. N. (2002). Drafting a faculty copyright ownership policy. The Technology Source, (March/April 2002). Retrieved from http://technologysource.org/article/drafting_a_faculty_copyright_ownership_policy/

Gatlin, R., & Arn, J. V. (1999). AACSB deans’ understanding of multimedia copyright laws and guidelines. Journal of Education for Business, 74(6), 368–371.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. Risk Management and Insurance Review, 13(1), 61–83.

Geist, M. (2009, March 12). Angus Reid surveys find public against new media and file sharing ISP levies [Blog post]. Retrieved from http://www.michaelgeist.ca/2009/03/angus-reid-survey/

Geist, M. (2013). Fairness found: How Canada quietly shifted from fair dealing to fair use. In M. Geist (Ed.), The copyright pentalogy: How the Supreme Court of Canada shook the foundations of Canadian copyright law (pp. 157–186). Ottawa, On.: University of Ottawa Press.

Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it (1st ed.). London; Toronto: Bantam Press.

Gould, T. H., Lipinski, T. A., & Buchanan, E. A. (2005). Copyright policies and the deciphering of fair use in the creation of reserves at university libraries. The Journal of Academic Librarianship, 31(3), 182–197.

Graham, R. (2014). Recalibrating some copyright conceptions: Toward a shared and balanced approach to educational copying. Partnership: The Canadian Journal of Library & Information Practice & Research, 9(2), 1–19.

Granbery, M. T. (2013). Copyright education: The impact of training for school librarians (Unpublished doctoral dissertation). The University of North Carolina at Chapel Hill: Chapel Hill, NC.

Gratton, E. (2015a). 2015 privacy class actions in Canada. Retrieved from http://www.eloisegratton.com/blog/2015/06/23/2015-privacy-class-actions-in-canada/

Gratton, E. (2015b). Top five mistakes when drafting website privacy policies [Blog post]. Retrieved from http://www.eloisegratton.com/blog/2015/07/06/top-five-mistakes-when-drafting-website-privacy-policies/

Gray, K. (2012). Stealing from the rich to entertain the poor?: A survey of literature on the ethics of digital piracy. The Serials Librarian, 63(3-4), 288–295.

Greenaway, K. E., Chan, Y. E. (2005). Theoretical explanations for firms' information privacy behaviors. Journal of the Association for Information Systems, 6(6), article 7.

Greenaway, K. E., Chan, Y. E. (2013). Designing a customer information privacy program aligned with organizational priorities. MIS Quarterly Executive, 12(3), 137–150.

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: A conceptual framework. Information Systems Journal, 25(6), 579–606.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of Internet hazards. Educational Gerontology, 36(3), 173–192.

Gritzalis, D., Theoharidou, M., & Kalimeri, E. (2005). Towards an interdisciplinary information security education model. In 4th IFIP World Conference on Information Security Education (pp. 22–35). Moscow: Moscow Engineering Physics Institute. Retrieved from http://scholar.google.com/scholar?cluster=15410215740882931598&hl=en&oi=scholarr

Gronau, I. (2015, June 29). Implementing precision privacy, security, and ownership policies [Blog post]. Retrieved from: http://www.precisionfarmingdealer.com/articles/1516-implementing-precision-data-privacy-security-and-ownership-policies

Gulenko, I. (2013). Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness. Information Management and Computer Security, 21(2), 91–101.

Gunasekara, G. (2009). The "final" privacy frontier? Regulating trans-border data flows. International Journal of Law and Information Technology, 17(2), 147–179.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems, 28(2), 203–236.

Gupta, M., & Sharman, R. (2008). Social and human elements of information security: Emerging trends and countermeasures. Hershey, PA: IGI Global.

Hackett, R. (2015, August 26). What to know about the Ashley Madison hack. Fortune. Retrieved from http://fortune.com/2015/08/26/ashley-madison-hack/

Hadnagy, C. (2011). Social engineering: the art of human hacking. Indianapolis, IN: John Wiley & Sons, Inc.

Hadnagy, C. (2014). Unmasking the social engineer: the human element of security. Indianapolis, IN: John Wiley & Sons, Inc.

Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. Information Management and Computer Security, 17(5), 388–407.

Hamel, A. van (2011). The Privacy Piece: Report on privacy competencies in digital literacy programs in Canada, Britain, Australia, America, and Brazil. Ottawa, ON: Office of the Privacy Commissioner of Canada. Retrieved from https://www.priv.gc.ca/information/research-recherche/2011/hamel_201111_e.asp

Hammoudeh, A. (2013, February 11). VPN pivoting. Retrieved from http://resources.infosecinstitute.com/vpn-pivoting/

Hane, P. J. (2011). Privacy concerns for the Web and beyond. Information Today, 28(2), 8.

Hanson, M., Johansson, T., Lindgren, C., & Oehme, R. (2015). Information security – trends 2015: A Swedish perspective. Karlstad, Sweden: Swedish Civil Contingencies Agency. Retrieved from https://www.msb.se/RibData/Filer/pdf/27584.pdf

Harnesk, D., & Lindstrom, J. (2011). Shaping security behaviour through discipline and agility: Implications for information security management. Information Management and Computer Security, 19(4), 262–276.

Harper, M. (2007). How physical design can influence copyright compliance. Knowledge Quest, 35(3), 30–32.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Ullah Khan, S. (2015). The rise of "big data" on cloud computing: Review and open research issues. Information Systems, 47, 98–115.

Henderson, M., De Zwart, M., Lindsay, D., & Phillips, M. (2010). Legal risks for students using social networking sites. Australian Educational Computing, 25(1), 3–7 Retrieved from http://acce.edu.au/journal/25/1/legal-risks-students-using-social-networking-sites

Hentea, M., Dhillon, H., & Dhillon, M. (2006). Towards changes in information security education. Journal of Information Technology Education: Research, 5(1), 221–233.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154–165.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125.

Herbert, W. A. (2011). Workplace consequences of electronic exhibitionism and voyeurism. IEEE Technology and Society Magazine, 30, 25–33. Retrieved from http://works.bepress.com/william_herbert/16/

Herman, M. L. (2002). Managing technology risks: Staying on course and out of trouble. Retrieved from http://www.betterimpact.com/wp-content/uploads/2015/05/Managing-Technology-Risks-Staying-On-Course-and-Out-of-Trouble.pdf

Herold, R. (2005). Managing an information security and privacy awareness and training program. Boca Raton, FL: CRC Press.

Herther, N. K. (2014). Global efforts to redefine privacy in the age of big data. Information Today, 31(6), 1, 34–36.

HEW Advisory Committee on Automated Data Systems. (1973). The code of fair information practices. Washington, DC.

Hill, K. (2014, December 4). Sony Pictures hack was a long time coming, say former employees. Retrieved from http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/

Hobbs, R. (2010). Copyright clarity: how fair use supports digital learning. Thousand Oaks, CA: Corwin.

Hobbs, R., Jaszi, P., & Aufderheide, P. (2007). The cost of copyright confusion for media literacy. Retrieved from http://eric.ed.gov/?id=ED499465

Hoeschmann, M., & DeWaard, H. (2015). Mapping digital literacy policy and practice in the Canadian education landscape. Ottawa, ON: MediaSmarts. Retrieved from http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/mapping-digital-literacy.pdf

Hoffman, M. E., & Blake, J. (2003). Computer literacy: Today and tomorrow. Journal of Computing Sciences in Colleges, 18(5), 221–233.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? (SSRN Scholarly Paper). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1589864

Hsu, C. (2006). Privacy concerns, privacy practices and web site categories: Toward a situational paradigm. Online Information Review, 30(5), 569–586.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615–660.

Humphries-Smith, T., & Adrian, A. (2012). Intellectual property education–thinking outside the box meets colouring within the lines. International Journal of Learning and Intellectual Capital, 9(3), 337–350.

Humphries, D. (2014, June 11). Survey: Consumer confidence in the security-breach era [Blog post]. Retrieved from http://intelligent-defense.softwareadvice.com/consumer-confidence-security-breach-era-0614/

Hynes v. Western Regional Integrated Health Authority, 2014 NLTD(G) 137. Retrieved from http://canlii.ca/t/gf8z9

Ibata, D. (2011, October 11). Ruling goes against Barrow teacher who lost job over Facebook posting. Atlanta Journal-Constitution. Retrieved from http://www.ajc.com/news/news/local/ruling-goes-against-barrow-teacher-who-lost-job-ov/nQMb8/

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95.

Industry Canada (2010a). Improving Canada's digital advantage: Strategies for sustainable prosperity. Retrieved from http://publications.gc.ca/collections/collection_2010/ic/Iu4-144-2010-eng.pdf

Industry Canada. (2007). Canadian small and medium sized enterprises: Baseline awareness of intellectual property. Retrieved from https://www.ic.gc.ca/eic/site/icgc.nsf/eng/04362.html

Industry Canada. (2010b). Building digital skills for tomorrow. Retrieved from https://www.ic.gc.ca/eic/site/028.nsf/eng/00041.html

International Association of Privacy Professionals. (2010). A call for agility: The next-generation privacy professional. York, ME: International Association of Privacy Professionals. Retrieved from http://www.huntonprivacyblog.com/uploads/file/IAPP_Future_of_Privacy.pdf

International Association of Privacy Professionals. (2013). Canadian privacy certification: Outline of the body of knowledge for the Certified Information Privacy Professional/Canada. Portsmouth, N.H.: International Association of Privacy Professionals. Retrieved from https://iapp.org/media/pdf/certification/CIPP_C_BoK.pdf

International Association of Privacy Professionals. (2013). Privacy manager certification: Outline of the body of knowledge for the Certified Information Privacy Manager. Portsmouth, N.H.: International Association of Privacy Professionals. Retrieved from https://iapp.org/media/pdf/certification/CIPM_BoK.pdf

International Organization for Standardization. (2014). ISO/IEC 27000:2014 (3rd ed.). Geneva: ISO.

International Systems Security Certification Consortium. (2010). (ISC)2 CBK: The compendium of information security topics. Clearwater, FL: ISC2.

Internet of Things: How to overcome the legal obstacles. (2015). Retrieved from https://www.cbapd.org/details_en.aspx?id=ON_15TEC1102T

Iqbal, S., Awad, A. I., & Thapa, D. (2014). Design principles for online information security laboratory. In IRIS: Selected papers of the Information Systems Research Seminar in Scandinavia, 5. Retrieved from http://aisel.aisnet.org/iris2014/6/

ISACA, & RSA Conference. (2015). State of cybersecurity: Implications for 2015. Rolling Meadows, IL: ISACA. Retrieved from http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

ISACA. (2008). Top business/technology issues survey results. Rolling Meadows, IL: ISACA. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Top-Business-Technology-Issues-Survey-Results-2008_res_Eng_0808.pdf

ISACA. (2012). ISACA model curriculum for information security management (2nd ed.). Rolling Meadows, Ill.: ISACA. Retrieved from http://www.isaca.org/Knowledge-Center/Academia/Documents/Model-Curriculum-InfoSecMgmt-2ndEd.pdf

James, A. F. (1981). Educator attitudes concerning copyright (Unpublished doctoral dissertation). University of Arkansas: Fayetteville, AR.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. Behavior & Information Technology, 32(6), 584–593.

Jaszi, P. A., & Aufderheide, P. (2008). Code of best practices in fair use for online video. Retrieved from http://digitalcommons.wcl.american.edu/pijip_copyright/1/

Jenkins, J. L., Durcikova, A., & Burns, M. B. (2013). Simplicity is bliss: Controlling extraneous cognitive load in online security training to promote secure behavior. Journal of Organizational and End User Computing, 25(3), 52–66.

Jensen, C. (2003). The more things change, the more they stay the same: Copyright, digital technology, and social norms. Stanford Law Review, 56(2), 531–570.

Johnson, D. (2008). Who's afraid of the big bad ©? School Library Journal, 54(10), 44–48.

Johnson, D., & Simpson, C. (2005). Are you the copy cop? Learning & Leading with Technology, 32(7), 14–20.

Johnson, E. C. (2006). Security awareness: Switch to a better programme. Network Security, 2006(2), 15–18.

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. IEEE Security & Privacy, 5(3), 16–24.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure Online. Human–Computer Interaction, 25(1), 1–24.

Joint, N. (2006). Teaching intellectual property rights as part of the information literacy syllabus. Library Review, 55(6), 330–336.

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? Journal of Computer Information Systems, 53(2), 22–30.

Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky business: Students and smartphones. TechTrends, 58(6), 73–83.

Kabay, M. E. (2002). Using social psychology to implement security policies. In S. Bosworth & M. E. Kabay (Eds.), Computer security handbook (4th ed.) (pp. 35.1–35.22). New York: John Wiley & Sons.

Kandiuk, M., & Lupton, A. (2012). Digital images in teaching and learning at York University: Are the libraries meeting the needs of faculty members in fine arts? Evidence Based Library and Information Practice, 7(2), 20–48.

Kapitzke, C., Dezuanni, M., & Iyer, R. (2011). Copyrights and Creative Commons licensing: Pedagogical innovation in a higher education media literacy classroom. E-Learning and Digital Media, 8(3), 271.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. Journal of the Association for Information Systems, 12(8), 518–555.

Katsanos, K. (2014, December 8). Top information security trends for 2015. Retrieved from http://pivotpoint.io/en-us/article/top-information-security-trends-for-2015#.Vi2NDaJ4Pas

Katz, F. H. (2010). Curriculum and pedagogical effects of the creation of a minor in Cyber Security. In 2010 Information Security Curriculum Development Conference (pp. 49–51). New York: ACM.

Katz, F. H. (2012). The creation of a minor in Cyber Security: The sequel. In Proceedings of the 2012 Information Security Curriculum Development Conference (pp. 75–81). New York: ACM. http://doi.org/10.1145/2390317.2390330

Kelly, G., & McKenzie, B. (2002). Security, privacy, and confidentiality issues on the internet. Journal of Medical Internet Research, 4(2), e12. Retrieved from http://www.jmir.org/2002/2/e12/

Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management and Computer Security, 22(1), 115–126.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. Information Management & Computer Security, 14(1), 24–36.

Koehler, W. (2008). In the matter of plagiarism... Practice makes imperfect. Journal of Library Administration, 47(3/4), 111–124.

Kohno, T., & Johnson, B. D. (2011). Science fiction prototyping and security education: Cultivating contextual and societal thinking in computer security education and beyond. In Proceedings of the 42nd ACM Technical Symposium on Computer Science Education (pp. 9–14). New York: ACM.

Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law. International Review of Law, Computers & Technology, 28(2), 159–171.

Kordsmeier, W., Gatlin-Watts, R., & Arn, J. V. (2000). University administrators' understanding of multimedia copyright guidelines. Educational Technology & Society, 3(1). Retrieved from http://www.ifets.info/journals/3_1/multimedia_copyright.html

Korovessis, P. (2011). Information security awareness in academia. International Journal of Knowledge Society Research, 2(4), 1–17.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences, 110(15), 5802–5805. Retrieved from http://www.pnas.org/content/110/15/5802.full

KPMG. (2014). KPMG SAP Cyber Security 2014. Amsterdam: KPMG.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics, 38(2), 143–154.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), 509-520.

Kravets, D. (2012, May 21). Supreme Court lets stand $675,000 file-sharing verdict. Wired. Retrieved from http://www.wired.com/2012/05/supreme-court-file-sharing/

Krebs, B. (2014, January 10). Target: Names, emails, phone numbers on up to 70 million customers stolen. Retrieved from http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/

Kroener, I., & Wright, D. (2014). A strategy for operationalizing privacy by design. The Information Society, 30(5), 355–365.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013). social engineering attacks on the knowledge worker. In Proceedings of the 6th International Conference on Security of Information and Networks (pp. 28–35). New York: ACM.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296.

Kruger, H. A., Drevin, L., & Steyn, T. (2006). A framework for evaluating ICT security awareness. In Proceedings of the 2006 ISSA Conference (pp. 1–11).

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. Telecommunications Policy, 38(11), 1134–1145.

Kush, A., & Singh, S. (2005). A model curriculum for security aspects in IT education. DESIDOC Bulletin of Information Technology, 25(5&6), 11–16.

Kvedar, D., Nettis, M., & Fulton, S. P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. Journal of Computing Sciences in Colleges, 26(2), 80–87.

Labrecque, M., & Dionne, J. (2014). Preparing for life in a digital age: Results for Ontario and Newfoundland and Labrador. Toronto, ON: Council of Ministers of Education, Canada. Retrieved from http://cmec.ca/Publications/Lists/Publications/Attachments/340/ICILS2013_CdnReport_EN.pdf

Lacey, D. (2009). Managing the human factor in information security: How to win over staff and influence business managers. Hoboken, NJ: Wiley.

Lampert, L. D. (2004). Integrating discipline-based anti-plagiarism instruction into the information literacy curriculum. Reference Services Review, 32(4), 347–355.

Langheinrich, M. (2009). Privacy in ubiquitous computing. In J. Krumm (Ed.), Ubiquitious computing fundamentals (pp. 95–160). Boca Raton, FL: CRC Press. Retrieved from https://vs.inf.ethz.ch/events/dag2001/slides/marc.pdf

Lau, E. K. W. (2003). An empirical study of software piracy. Business Ethics: A European Review, 12(3), 233–245.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. Systems Practice, 5(4), 379–393.

Lebek, B., Uffen, J., Breitne, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. In Proceedings of the 46th Hawaii International Conference on System Sciences (pp. 2978–2987).

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review, 37(12), 1049–1092.

Leese, M. (2015). Privacy and security – On the evolution of a European conflict. In S. Gutworth, R. Leenes, & P. de Hert (Eds.), Reforming European data protection law (pp. 271–289). Dordrecht: Springer Netherlands.

LeFebvre, R. (2012). The human element in cyber security: A study on student motivation to act. In Proceedings of the 2012 Information Security Curriculum Development Conference (pp. 1–8). New York: ACM.

Lenhart, A., & Madden, M. (2007). Teens, privacy and online social networks: How teens manage their online identities and personal information in the age of MySpace. Retrieved from http://www.pewinternet.org/2007/04/18/teens-privacy-and-online-social-networks/

Leon, P. G., Cranshaw, J., Cranor, L. F., Graves, J., Hastak, M., Ur, B., & Xu, G. (2012). What do online behavioral advertising privacy disclosures communicate to users?. In Proceedings of the 2012 ACM workshop on Privacy in the electronic society (pp. 19-30).

Li, Y., Stweart, W., Zhu, J., & Ni, A. (2014). Online privacy policy of the thirty Dow Jones corporations: Compliance with FTC Fair Information Practice Principles and readability assessment. Communications of the IIMA, 12(3), article 5. Retrieved from http://scholarworks.lib.csusb.edu/ciima/vol12/iss3/5/

Liu, C., & Arnett, K. P. (2002). An examination of privacy policies in Fortune 500 Web sites. American Journal of Business, 17(1), 13–22.

Long, J., & White, G. (2010). On the global knowledge components in an information security curriculum – A multidisciplinary perspective. Education and Information Technologies, 15(4), 317–331.

Lundevall-Unger, P., & Tranvik, T. (2011). IP addresses – Just a number? International Journal of Law and Information Technology, 19(1), 53–73.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. Information Resources Management Journal, 24(3), 1–8.

Mabrouk, P. A. (2013). An investigation of the evolution of high school and undergraduate student researchers' understanding of key science ethics concepts. Journal of College Science Teaching, 43(2), 93–99.

MacDougall, W. (2003). Survey of international best practices in intellectual property information dissemination. World Patent Information, 25(1), 11–17.

MacKay, G. (2015, September 22). The latest Social Media Donkey award unveiled… [Blog post]. Retrieved from http://mackaycartoons.net/2015/09/22/the-latest-social-media-donkey-award-unveiled/

Magi, T. J. (2007). The gap between theory and practice: A study of the prevalence and strength of patron confidentiality policies in public and academic libraries. Library & Information Science Research, 29(4), 455–470.

Magi, T. J. (2010). A content analysis of library vendor privacy policies: do they meet our standards? College & Research Libraries, 71(3), 254–272.

Magnuson, L. (2011). Promoting privacy: Online and reputation management as an information literacy skill. College & Research Libraries News, 72(3), 137–140.

Manitoba Department of Education. (n.d.). Literacy with information and communication technology across the curriculum: A model for 21st century learning from K-12. Retrieved October 26, 2015, from http://www.edu.gov.mb.ca/k12/tech/lict/index.html

Mann, I. (2012). Hacking the human: Social engineering techniques and security countermeasures. Farnham, UK: Gower.

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.

Marias, G. F., Papazafeiropoulos, G., Priggouris, N., Hadjiefthymiades, S., & Merakos, L. (2006). An innovative gateway for indoor positioning. EURASIP Journal on Applied Signal Processing, 2006, 161–161.

Martinez-Moyano, I. J., Conrad, S. H., & Andersen, D. F. (2011). Modeling behavioral considerations related to information security. Computers & Security, 30(6), 397-409.

Matzner, T. (2014). Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". Journal of Information, Communication and Ethics in Society, 12(2), 93–106.

May, C. (2008). Approaches to user education. Network Security, 2008(9), 15–17.

McCollum, K. (1999, September 3). Oregon student is convicted of providing pirated music on university web site. The Chronicle of Higher Education, A48.

McCord, M. (2014, February 21). Risks continue to grow for small organizations' IT infrastructure. New Hampshire Business Review. Retrieved from http://www.nhbr.com/February-21-2014/Risks-continue-to-grow-for-small-organizations-IT-infrastructure/

McCullagh, K. (2009). Protecting "privacy" through control of "personal" data processing: A flawed approach. International Review of Law, Computers & Technology, 23(1-2), 13–24.

McDonald, A., & Cranor, L. F. (2010). Beliefs and behaviors: Internet users' understanding of behavioral advertising (SSRN Scholarly Paper No. ID 1989092). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1989092

McDowell, W. C., Smith, W. W., & Zhang, L. (2009). Examining digital piracy: self-control, punishment, and self-efficacy. Information Resources Management Journal, 22(1), 24–44.

McGrail, E., & McGrail, J. P. (2010). Copying right and copying wrong with Web 2.0 tools in the teacher education and communications classrooms. Contemporary Issues in Technology & Teacher Education, 10(3), 257–274.

McGuire, P. (2013, June 10). Canadians should be concerned about the NSA and PRISM. VICE. Retrieved October 28, 2015, from http://www.vice.com/en_ca/read/canadians-should-be-concerned-about-the-nsa-and-prism

McLean, K. (1992). Information security awareness – Selling the cause. In Proceedings of the IFIP TC11, Eighth International Conference on Information Security: IT security: The need for international cooperation (pp. 179–193). Amsterdam: North-Holland Publishing Co.

McNeely, C. L., & Hahm, J. (2014). The big (data) bang: Policy, prospects, and challenges. The Review of Policy Research, 31(4), 304–310.

Media Awareness Network. (2010). Digital literacy in Canada: From inclusion to transformation. Retrieved from http://www.ic.gc.ca/eic/site/028.nsf/eng/00537.html?Open&pv=1

MediaSmarts. (2012). Young Canadians in a wired world, phase III: Talking to youth and parents about life online. Retrieved from http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/ycwwiii-youth-parents.pdf

MediaSmarts. (2015). Teacher resources. Retrieved May 24, 2015, from http://mediasmarts.ca/teacher-resources

MediaSmarts. (2015a, September). Media education in Alberta. Retrieved October 26, 2015, from http://mediasmarts.ca/teacher-resources/digital-media-literacy-outcomes-province-territory/media-education-alberta

MediaSmarts. (2015b, September). Media education in British Columbia. Retrieved October 26, 2015, from http://mediasmarts.ca/teacher-resources/media-education-outcomes-province/british-columbia

MediaSmarts. (2015c, September). Media education in Manitoba. Retrieved October 26, 2015, from http://mediasmarts.ca/teacher-resources/media-education-outcomes-province/manitoba

MediaSmarts. (2015d, September). Media education in Ontario. Retrieved October 26, 2015, from http://mediasmarts.ca/teacher-resources/digital-media-literacy-outcomes-province-territory/media-education-ontario

MediaSmarts. (2015e, September). Media education in Quebec. Retrieved October 26, 2015, from http://mediasmarts.ca/teacher-resources/media-education-outcomes-province/quebec

MediaSmarts. (2015f, September). Media education in Saskatchewan. Retrieved October 26, 2015, from http://mediasmarts.ca/teacher-resources/media-education-outcomes-province/saskatchewan

MediaSmarts. (n.d.-a). Digital literacy fundamentals. Retrieved from http://mediasmarts.ca/digital-media-literacy-fundamentals/digital-literacy-fundamentals

MediaSmarts. (n.d.-b). Privacy issues. Retrieved from http://mediasmarts.ca/digital-media-literacy/digital-issues/privacy/privacy-issues

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. Academy of Information and Management Sciences Journal, 14(2), 91–116.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. Communication Research, 33(3), 155–179.

MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). Retrieved from https://scholar.google.ca/scholar_case?case=8647956476676426155

Microsoft. (2015). Microsoft security intelligence report (No. 18). Redmond, Washington: Microsoft. Retrieved from http://www.microsoft.com/security/sir/default.aspx

Milliken & Co. v. Interface Flooring Systems (Canada) Inc., [1998] 3 F.C.R. 103. Retrieved from http://canlii.ca/t/4cnf

Moore, O., & Chiose, S. (2013, January 10). TDSB director resigns over plagiarism, PhD dissertation includes unattributed passages. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/news/national/education/tdsb-director-resigns-over-plagiarism-phd-dissertation-includes-unattributed-passages/article7167752/

Mount Royal University. (2011, April 4). Use of copyright materials policy. Retrieved from http://www.mtroyal.ca/Library/Research/Copyright/index.htm

Mukhopadhyay, D., & Chakraborty, R. S. (2015). Hardware security: design, threats, and safeguards. Boca Raton, FL: CRC Press.

Murray, L. J. (2008). Plagiarism and copyright infringement: The costs of confusion. In C. Eisner & M. Vicinus (Eds.), Originality, imitation, and plagiarism: Teaching writing in the digital age (pp. 173–182). Ann Arbor, MI: University of Michigan Press.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security, 34, 47–66.

Myr, P. (2015, August 20). Class-action lawsuit filed in Canada against Ashley Madison. Global News. Retrieved from http://globalnews.ca/news/2176979/class-action-lawsuit-filed-in-canada-against-ashley-madison/

Nanos. (2008). Canadians on intellectual property. Retrieved from http://www.nanosresearch.com/library/polls/POLNAT-S08-T295.pdf

National Conference of State Legislatures. (2015). Security breach notification laws. Washington, DC: National Conference of State Legislatures. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#2

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. Gaithersburg, MD. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology. (n.d.). Federal Information Security Management Act: Detailed overview. Gaithersburg, MD. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/overview.html

National Science Foundation. (2014, December 26). Grant general conditions (GC-1). Retrieved from http://www.nsf.gov/awards/managing/general_conditions.jsp

Newfoundland and Labrador Department of Education. (2012). Technology education: A curriculum guide. Retrieved from http://www.ed.gov.nl.ca/edu/k12/curriculum/guides/teched/gr8production/g8_prodtech_full.pdf

Nissenbaum, H. F. (2010). Privacy in context: technology, policy, and the integrity of social life. Stanford, CA: Stanford Law Books.

Nohlberg, M. (2008). Securing information assets: understanding, measuring and protecting against social engineering attacks. Kista, Sweden: Institutionen för data- och systemvetenskap. Retrieved from http://www.diva-portal.org/smash/record.jsf?pid=diva2:200190

Nova Scotia Department of Education. (2012). Learning outcomes framework: Grades 10–12. Retrieved from http://srhs.ednet.ns.ca/Dept%20docs/outcomes%2010-12.pdf

Nugent, J. (2015, February 5). Cybersecurity trends to watch in 2015. Forbes. Retrieved from http://www.forbes.com/sites/riskmap/2015/02/05/cybersecurity-trends-to-watch-in-2015/

Nyman, N. J. (2005). Risky business: What must employers do to shield against liability for employee wrongdoings in the internet age? Shidler Journal of Law, Commerce, and Technology, 1, No. 7.

O'Brien, D. (2015, October 5). No safe harbor: how NSA spying undermined U.S. tech and Europeans' privacy. Retrieved October 28, 2015, from https://www.eff.org/deeplinks/2015/10/europes-court-justice-nsa-surveilance

Oakley, B., Pittman, B., & Rudnick, T. (2008). Tackling copyright in the digital age: An initiative of the University of Connecticut Libraries. Journal of Access Services, 5(1/2), 265–283.

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. European Journal of Information Systems, 23(2), 126–150.

Office for Harmonization in the Internal Market (Trade Marks and Designs). (2013). European citizens and intellectual property: Perception, awareness and behaviour. Alicante, Spain: European Union. Retrieved from https://oami.europa.eu/ohimportal/en/web/observatory/ip_perception

Office of the Privacy Commissioner of Canada. (2001). PIPEDA Case Summary #2001-25: A broadcaster accused of collecting personal information via Web site. Retrieved from https://www.priv.gc.ca/cf-dc/2001/cf-dc_011120_e.asp

Office of the Privacy Commissioner of Canada. (2005). PIPEDA Case Summary #2005-315: Web-centred company's safeguards and handling of access request and privacy complaint questioned. Retrieved from https://www.priv.gc.ca/cf-dc/2005/315_20050809_03_e.asp

Office of the Privacy Commissioner of Canada. (2008). PIPEDA Case Summary #2008-394: Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers. Retrieved October 28, 2015, from https://www.priv.gc.ca/cf-dc/2008/394_20080807_e.asp

Office of the Privacy Commissioner of Canada. (2009). PIPEDA Case Summary #2009-010: Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection. Retrieved from https://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.asp

Office of the Privacy Commissioner of Canada. (2013). Interpretation bulletin: Personal information. Retrieved from https://www.priv.gc.ca/leg_c/interpretations_02_e.asp

Office of the Privacy Commissioner of Canada. (2014). Fact sheet: Privacy legislation in Canada. Retrieved from https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp

Office of the Privacy Commissioner of Canada. (2015, May 7). Oversight offices and government organizations. Retrieved from https://www.priv.gc.ca/resource/prov/index_e.asp

Ohaya, C. (2006). Managing phishing threats in an organization. In Proceedings of the 3rd Annual Conference on Information Security Curriculum Development (pp. 159–161). New York: ACM.

Olavsrud, T. (2014, December 10). 5 information security trends that will dominate 2015. Retrieved from http://www.cio.com/article/2857673/security0/5-information-security-trends-that-will-dominate-2015.html

Oliver, G. (2011). Organisational culture for information managers. Oxford: Chandos Publishing.

Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22575 et seq. (2003). Retrieved from http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

Ontario College of Teachers. (2013, April). Additional qualification course guideline: Teaching communication technology: Interactive new media and animation. Retrieved from http://www.oct.ca/-/media/PDF/Additional%20Qualifications/EN/Schedule%20F/Draft/teaching_communication_technology_interactive_new_media_and_animation_e.pdf

Ontario College of Teachers. (2014, May). Additional qualification course guideline: Intermediate division: Music instrumental. Retrieved from http://www.oct.ca/-/media/PDF/Additional%20Qualifications/EN/Schedule%20A/Draft/intermediate_music_instrumental_e.pdf

Ontario Ministry of Education. (2006a). The Ontario curriculum, grades 9 and 10: Business studies. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/secondary/business.html

Ontario Ministry of Education. (2006b). The Ontario curriculum, grades 11 and 12: Business studies. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/secondary/business.html

Ontario Ministry of Education. (2007a). The Ontario curriculum, grades 9 and 10: English. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/secondary/english.html

Ontario Ministry of Education. (2007b). The Ontario curriculum, grades 11 and 12: English. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/secondary/english.html

Ontario Ministry of Education. (2008a). The Ontario curriculum, grades 9 and 10: Science. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/secondary/science.html

Ontario Ministry of Education. (2008b). The Ontario curriculum, grades 11 and 12: Science. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/secondary/science.html

Ontario Ministry of Education. (2009a). The Ontario curriculum, grades 1-8: The arts. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/elementary/arts.html

Ontario Ministry of Education. (2009b). The Ontario curriculum, grades 11 and 12: Technological education. Retrieved from https://www.edu.gov.on.ca/eng/curriculum/secondary/teched.html

Ontario Ministry of Education. (2010a). The Ontario curriculum, grades 9 and 10: The arts. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/secondary/arts.html

Ontario Ministry of Education. (2010b). The Ontario curriculum, grades 11 and 12: The arts. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/secondary/arts.html

Ontario Ministry of Education. (2013). The Ontario curriculum, grades 1-6: Social studies. Retrieved from http://www.edu.gov.on.ca/eng/curriculum/elementary/sshg.html

Organisation for Economic Co-operation and Development. (2013). Guidelines on the protection of privacy and transborder flows of personal data. Paris: OECD. Retrieved from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In Proceedings of the 5th Conference on Information Technology Education (pp. 177–181). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1029577

Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers & Security, 31(5), 673–680.

Paganini, P. (2014, November 24). Sony Pictures corporate network compromised by a major attack. Retrieved from http://securityaffairs.co/wordpress/30498/cyber-crime/sony-pictures-corporate-network-compromised-major-attack.html

Paganini, P. (2015, February 5). Sony Pictures hacked by Russian blackhats, it now emerges. Retrieved from http://securityaffairs.co/wordpress/33143/cyber-crime/sony-pictures-hacked-russian-blackhats.html

Palfrey, J., & Gasser, U. (2008). Born digital: Understanding the first generation of digital natives. New York: Basic Books.

Palfrey, J., Gasser, U., Simun, M., & Barnes, R. F. (2009). Youth, creativity, and copyright in the digital age. International Journal of Learning and Media, 1(2), 79–97. Retrieved from https://dash.harvard.edu/handle/1/3128762

Panel on Responsible Conduct of Research. (2011, November 23). Tri-Agency framework: Responsible conduct of research. Ottawa, ON: Government of Canada. Retrieved from http://www.rcr.ethics.gc.ca/eng/policy-politique/framework-cadre/

Park, S. K., Jun, H. J., & Kim, T. S. (2015). Using online job postings to analyze differences in skill requirements of information security consultants: South Korea versus United States. PACIS 2015 Proceedings, paper 111. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1145&context=pacis2015

Park, Y. J. (2011). Provision of Internet privacy and market conditions: An empirical analysis. Telecommunications Policy, 35(7), 650–662.

Peltier, T. R. (2014). Information security fundamentals (2nd ed.). Boca Raton, FL: CRC Press, Taylor & Francis Group.

Pendegraft, N., Rounds, M., & Stone, R. W. (2010). Factors influencing college students' use of computer security. International Journal of Information Security and Privacy, 4(3), 51–60.

Perrott, E. (2011). Copyright in the classroom: Why comprehensive copyright education is necessary in United States K-12 education curriculum. Intellectual Property Brief, 2(3), 5–18.

Personal Health Information Act, S.N.L. 2008, c. P-7.01. Retrieved October 26, 2015, from http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

Personal Health Information Privacy and Access Act, S.N.B. 2009, c. P-7.05. Retrieved October 26, 2015, from http://laws.gnb.ca/en/showfulldoc/cs/P-7.05/20121030

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A. Retrieved October 26, 2015, from http://www.ontario.ca/laws/statute/04p03

Personal Information Protection Act, S.B.C. 2003, c. 63. Retrieved from http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. Retrieved from http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

Peslak, A. R. (2005). Internet privacy policies: A review and survey of the Fortune 50. Information Resources Management Journal, 18(1), 29–41.

Petrova, K., Philpott, A., Kaskenpalo, P., & Buchan, J. (2004). Embedding information security curricula in existing programmes. In Proceedings of the 1st Annual Conference on Information Security Curriculum Development (pp. 20–29). New York: ACM.

Phillips, T., & Street, J. (2015). Copyright and musicians at the digital margins. Media, Culture & Society, 37(3), 342–358.

Piechocinski, T. J. (2009). What do university students really think about copyright issues? A look at student-designed guidelines for copyright compliance. MEIEA Journal, 9(1), 161–179.

Pike, G. H. (2011). The online privacy debate: How to get to "No". Information Today, 28(11), 24.

Pitkethly, R. H. (2012). Intellectual property awareness. International Journal of Technology Management, 59(3/4), 163–179.

Plachkinova, M., & Andrés, S. (2015). Improving information security training: An intercultural perspective. PACIS 2015 Proceedings, No. 167. Retrieved from http://aisel.aisnet.org/pacis2015/167/

Polonetsky, J., & Tene, O. (2013). Privacy and big data: Making ends meet. Stanford Law Review Online, 66(25), 25–33. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2628412

Ponemon Institute. (2011). Reputation impact of a data breach: Executive summary. Retrieved from http://f6ce14d4647f05e937f4-4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/ponemon-institute-study-reputation-impact-data-breach-pdf-w-540.pdf

Ponemon Institute. (2012). 2011 cost of data breach study: United States. Retrieved from http://www.ponemon.org/blog/2011-cost-of-data-breach-united-states

Popescu, M., & Baruh, L. (2013). Captive but mobile: Privacy concerns and remedies for the mobile environment. The Information Society, 29(5), 272–286.

Power, L. G. (2009). University students' perceptions of plagiarism. The Journal of Higher Education, 80(6), 643–662.

Pratt, J. H., & Conger, S. (2009). Without permission: Privacy on the line. International Journal of Information Security and Privacy, 3(1), 30–44.

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping ubiquitous computing to yourself: A practical model for user control of privacy. International Journal of Human-Computer Studies, 63(1-2), 228–253.

PricewaterhouseCoopers. (2013). The Global State of Information Security survey 2014: Defending yesterday. London: PwC. Retrieved from http://www.pwchk.com/home/eng/rcs_info_security_2014.html

PricewaterhouseCoopers. (2014). The Global State of Information Security survey 2015: Managing cyber risks in an interconnected world. London: PwC. Retrieved from http://www.pwchk.com/home/eng/rcs_info_security_2015.html

PricewaterhouseCoopers. (2015). The Global State of Information Security survey 2016: Turnaround and transformation in cybersecurity. London: PwC. Retrieved from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Prillman, J. S. (2012). Incorporating the fifth standard of ACRL's information literacy competency standards for higher education into information literacy curriculum. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2030958

Privacy Act, R.S.C., 1985, c. P-21. Retrieved from http://laws-lois.justice.gc.ca/eng/acts/p-21/

Probert, E. (2009). Information literacy skills: Teacher understandings and practice. Computers & Education, 53(1), 24–33.

Puhakainen, P. (2006). A design theory for information security awareness (Unpublished doctoral dissertation). University of Oulu, Oulu, Finland. Retrieved from http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757–778.

Quartey, S. (2007). Developing a campus copyright education program: Conquering the challenge. Journal of Interlibrary Loan, Document Delivery & Electronic Reserves, 18(1), 93–100.

Québec Ministère d'Éducation, Enseignement supérieur et Recherche. (2001). Québec education program (primary). Retrieved from http://www1.mels.gouv.qc.ca/sections/programmeFormation/primaire/pdf/educprg2001/educprg2001.pdf

Québec Ministère d'Éducation, Enseignement supérieur et Recherche. (2004). Québec education program (secondary): Cross-curricular competencies. Retrieved from http://www1.mels.gouv.qc.ca/sections/programmeFormation/secondaire1/index_en.asp?page=qepsecfirstcycle

Rader, E., Wash, R., & Brooks, B. (2012). Stories as informal lessons about security. In SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security (Article no. 6). Retrieved from https://cups.cs.cmu.edu/soups/2012/proceedings/a6_Rader

Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. M. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4), 606–622.

Ralevich, V., & Martinovic, D. (2010). Designing and implementing an undergraduate program in information systems security. Education and Information Technologies, 15(4), 293–315.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research, 20(1), 121–139. Retrieved from http://www.cs.unh.edu/~it666/reading_list/ZeroDay/RansbothamMitra_2009.pdf

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How effective is your security awareness program? An evaluation methodology. Information Security Journal: A Global Perspective, 21(6), 328–345.

Rawlinson, D. R., & Lupton, R. A. (2007). Cross-national attitudes and perceptions concerning software piracy: A comparative study of students from the United States and China. Journal of Education for Business, 83(2), 87–93.

Reidenberg, J. R. (2005). Technology and Internet jurisdiction. University of Pennsylvania Law Review, 153(6), 1951–1974.

Renaud, K., & Cutts, Q. (2013). Teaching human-centered security using nontraditional techniques. ACM Transactions on Computing Education, 13(3), 11:1–11:23.

Renner, J. R. (2005). Knowledge level of postsecondary educators regarding copyright and copyright-related issues. In Center for Intellectual Property in the Digital Environment (Ed.), Colleges, code, and copyright: the impact of digital networks and technological controls on copyright and the dissemination of information in higher education (pp. 90–115). Chicago, IL: Association of College and Research Libraries.

Reuters. (2015, January 12). Canada to copyright holders: Stop threatening Canadians illegally downloading your stuff with penalties that don't exist. Financial Post. Retrieved from http://business.financialpost.com/news/canada-to-copyright-holders-stop-threatening-canadians-illegally-downloading-your-stuff-with-penalties-that-dont-exist

Richardson, R. (2007). 2007 CSI computer crime and security survey. Orlando, FL: Computer Security Institute. Retrieved from http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

Robinson, R. (2014, January 9). Three lessons from the Target hack of encrypted PIN data. Retrieved from https://securityintelligence.com/target-hack-encrypted-pin-data-three-lessons/

Rodriguez, J. E., Greer, K., & Shipman, B. (2014). Copyright and you: copyright instruction for college students in the digital age. Journal of Academic Librarianship, 40(5), 486–491.

Roose, K. (2014, December 2). More from the Sony Pictures hack: Budgets, layoffs, HR scripts, and 3,800 social security numbers. Retrieved from http://fusion.net/story/30850/more-from-the-sony-pictures-hack-budgets-layoffs-hr-scripts-and-3800-social-security-numbers/

Rudraswamy, V., & Vance, D. A. (2001). Transborder data flows: Adoption and diffusion of protective legislation in the global electronic commerce environment. Logistics Information Management, 14(1/2), 127–137.

Ruiter, J., & Warnier, M. (2011). Privacy regulations for cloud computing: Compliance and implementation in theory and practice. In S. Gutwirth, Y. Poullet, P. de Hert, & R. Leenes (Eds.), Computers, privacy and data protection: An element of choice (pp. 361-376). Dordrecht: Springer.

Sampson, F. (2006). A penny for your thoughts, a latte for your password. Interactions, 13(1), 8–9.

San Nicolas-Rocca, T., & Olfman, L. (2013). End user security training for identification and access management. Journal of Organizational and End User Computing, 25(4), 75–103.

San Nicolas-Rocca, T., Schooley, B., & Spears, J. L. (2014). Exploring the effect of knowledge transfer practices on user compliance to IS security practices. International Journal of Knowledge Management, 10(2), 62–78.

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

Sattar, A. H. M. S., Li, J., Liu, J., Heatherly, R., & Malin, B. (2014). A probabilistic approach to mitigate composition attacks on privacy in non-coordinated environments. Knowledge-Based Systems, 67, 361–372.

Scardilli, B. (2014). Ten tips for Internet of Things security in homes and businesses. Information Today, 31(5), 36. Retrieved from http://www.infotoday.com/IT/jun14/Scardilli--Securing-the-Internet-of-Things.shtml

Schlipp, J. (2008). Coaching teaching faculty: Copyright awareness programs in academic libraries. Kentucky Libraries, 72(3), 18–22.

Schlipp, J. (2010). Creative thinking: A student-centered approach to plagiarism and copyright. Kentucky Libraries, 74(3), 28–32.

Schlipp, J., & Kocis, L. (2013). Using popular fiction to spark student creativity and to teach intellectual property information literacy. Kentucky Libraries, 77(1), 26–32.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world (1st ed.). New York, NY: W.W. Norton & Company.

Schrems v. Data Protection Commissioner, C‑362/14, [2015] ECR I–1. Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en

Schulich School of Medicine and Dentistry. (n.d.). 2015-2016 workshops. Retrieved September 23, 2015, from https://www.schulich.uwo.ca/continuingprofessionaldevelopment/faculty_staff_development/fsd-workshops.html

Schweitzer, D., & Boleng, J. (2009). Designing Web labs for teaching security concepts. Journal of Computing Sciences in Colleges, 25(2), 39–45.

Service Alberta. (n.d.). About the Personal Information Protection Act. Retrieved October 26, 2015, from http://servicealberta.ca/pipa-overview.cfm

Shane, S. L. (1999). An analysis of the knowledge levels of California K-12 teachers concerning copyright issues related to classroom multimedia projects (Unpublished doctoral dissertation). Pepperdine University, Malibu, CA.

Shankar, K. (2010). Pervasive computing and an aging populace: Methodological challenges for understanding privacy implications. Journal of Information, Communication and Ethics in Society, 8(3), 236–248.

Shaw, G. (2015, January 14). Cutting through the confusion about Canada's Internet piracy rules. Vancouver Sun. Retrieved from http://www.vancouversun.com/technology/Cutting+through+confusion+about+Canada+Internet+piracy+rules+with+video/10716603/story.html

Sherif, E., Furnell, S., and Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. In T. Tryfonas and I. Askoxylakis (Eds.), Human aspects of information security, privacy, and trust (pp. 436-448). Berlin: Springer.

Shing, M.-L., Shing, C.-C., Chen, K. L., & Lee, H. (2007). Issues in information security curriculum: Collaborative learning and team teaching. International Journal of Innovation and Learning, 4(5), 516–529.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.

Silvernagel, C., Schultz, R. R., Moser, S. B., & Aune, M. (2009). Student-generated intellectual property: Perceptions of ownership by faculty and students. Journal of Entrepreneurship Education, 12, 13–33.

Simon Fraser University. (2015, July 27). What is copyright infringement? Retrieved from http://www.lib.sfu.ca/help/academic-integrity/copyright/infringement

Sinha, R. K., & Mandel, N. (2008). Preventing digital music piracy: The carrot or the stick? Journal of Marketing, 72(1), 1–15.

Sinnreich, A., & Aufderheide, P. (2015). Communication scholars and fair use: The case for discipline-wide education and institutional reform. International Journal of Communication, 9. http://ijoc.org/index.php/ijoc/article/view/3657/1329

Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31–41.

Siponen, M. T. (2000b). Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice. Library Computing, 19(3/4), 256–269.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. von Solms (Eds.), New approaches for security, privacy and trust in complex environments (pp. 133–144). Boston, MA: Springer.

Siraj, A., Taylor, B., Kaza, S., & Ghafoor, S. (2015). Integrating security in the computer science curriculum. ACM Inroads, 6(2), 77–81.

Slauson, G. J., Carpenter, D., & Snyder, J. (2008). Copyright ethics: Relating to students at different levels of moral development. Information Systems Education Journal, 6(8), 1–6.

Slovensky, R., & Ross, W. H. (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, W. P., & Kidder, D. L. (2010). You've been tagged! (Then again, maybe not): Employers and Facebook. Business Horizons, 53(5), 491–499.

Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy? The Academy of Management Perspectives, 23(4), 33–48.

Soetendorf, R. (2008). Teaching intellectual property to non-law students. In Y. Takagi, L. Allman, & M. A. Sinjela (Eds.), Teaching of intellectual property: Principles and methods (pp. 230–267). Cambridge: Cambridge University Press.

Software Alliance. (n.d.). News listing. Retrieved September 29, 2015, from http://www.bsa.org/news-and-events/news

Software piracy costs Connon Nurseries. (2014, December 11). The Belleville Intelligencer. Retrieved from http://www.intelligencer.ca/2014/12/11/software-piracy-costs-connon-nurseries

Solms, B. v., & Solms, R. v. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371–376.

Solms, S. H. v., & Solms, R. v. (2009). Information security governance. Boston, MA: Springer.

Solove, D. J. (2003). The virtues of knowing less: Justifying privacy protections against disclosure. Duke Law Journal, 53(3), 967–1065. Retrieved from http://scholarship.law.duke.edu/dlj/vol53/iss3/2/

Solove, D. J. (2008). The future of privacy. American Libraries, 39(8), 56–59.

Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2009). Flash cookies and privacy (SSRN Scholarly Paper No. ID 1446862). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1446862

Sony BMG Music Entertainment v. Tenenbaum, 660 F (3d) 487 (1st Cir. 2011). Retrieved from https://scholar.google.ca/scholar_case?case=6349690935852737851

Souza, E. d., & Prafullchandra, H. (2015, July 15). Should this be the era of the Chief Security Privacy Officer? Retrieved from: https://iapp.org/news/a/should-this-be-the-era-of-the-chief-security-privacy-officer

Special Libraries Association. (2015). Certificate in copyright management. Alexandria, Virg.: Special Libraries Association. Retrieved from https://www.sla.org/learn/certificate-programs/cert-copyright-mgmt/

Stanton, J. M., Stam, K. R., Guzman, I., and Caldera, C. (2003). Examining the linkage between organizational commitment and information security. In Proceedings of the IEEE Systems, Man, and Cybernetics Conference (pp. 2501–2506).

Starkey, L., Corbett, S., Bondy, A., & Davidson, S. (2010). Intellectual property: what do teachers and students know? International Journal of Technology and Design Education, 20(3), 333–344.

Starkman, N. (2008). Do the (copy)right thing. T H E Journal, 35(3), 22–25.

Stedman, A. (2014, December 9). Leaked Sony emails reveal nasty exchanges and insults. Variety. Retrieved from http://variety.com/2014/film/news/leaked-sony-emails-reveal-nasty-exchanges-and-insults-1201375511/

Steinmetz, K., & Gerber, J. (2014). "It doesn't have to be this way": Hacker perspectives on privacy. Social Justice, 41(3), 29–51. Retrieved from http://www.socialjusticejournal.org/archive/137_41_3/137_02_Steinmetz.pdf

Stoddart, J. (2004). Privacy implications of the USA Patriot Act. Canadian Parliamentary Review, 27(4), 17–24.

Stone, B. (2009, July 18). Amazon erases Orwell books from Kindle. The New York Times. Retrieved from http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html

Straub, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255–276.

Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Iliffe, U., Oppenheim, C., & Hardy, R. (2003). User privacy in the digital library environment: An investigation of policies and preparedness. Library Management, 24(1/2), 44–50.

Sukhai, N. B. (2004). Hacking and cybercrime. In Proceedings of the 1st Annual Conference on Information Security Curriculum Development (pp. 128–132). New York: ACM. http://doi.org/10.1145/1059524.1059553

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review, 26(4), 391–397.

Svärd, P. (2014). Information culture in three municipalities and its impact on information management amidst e-government development. IFLA journal, 40(1), 48–59.

Symantec. (2015). 2015 Internet security threat report: Appendices. Mountain View, CA: Symantec. Retrieved from https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf

Taia Global. (2015). The Sony breach: From Russia, no love. McLean, VA: Taia Global. Retrieved from https://taia.global/wp-content/uploads/2015/02/SPE-Russia-Connection_Final.pdf

Takagi, Y., Allman, L., & Sinjela, M. A. (Eds.). (2008). Teaching of intellectual property: Principles and methods. Cambridge: Cambridge University Press.

Tan, M., & Sagala Aguilar, K. (2012). An investigation of students' perception of Bluetooth security. Information Management & Computer Security, 20(5), 364–381.

Tatnall, A. D. (2010). Using actor-network theory to understand the process of information systems curriculum innovation. Education and Information Technologies, 15(4), 239–254.

Taylor, S., Ishida, C., & Wallace, D. (2009). Intention to engage in digital piracy: A conceptual model and empirical test. Journal of Service Research, 11(3), 246–262.

Techvibes NewsDesk. (2014, October 9). How Canada's privacy laws differ from those in US, Europe. Retrieved from http://www.techvibes.com/blog/how-canadas-privacy-laws-differ-from-those-in-us-europe-2014-10-09

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empirical study of students' computer security practices/perceptions. Journal of Computer Information Systems, 47(3), 105–110.

Tene, O., & Polonetsky, J. (2012a). Big data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property, 11(5), 238–273. Retrieved from http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/

Tene, O., & Polonetsky, J. (2012b). Privacy in the age of big data: A time for big decisions. Stanford Law Review Online, 64, 63–69. Retrieved from http://www.stanfordlawreview.org/online/privacy-paradox/big-data

Tene, O., & Polonetsky, J. (2013a). Judged by the tin man: Individual rights in the age of big data. Journal on Telecommunications and High Technology Law, 11, 351–368. Retrieved from http://jthtl.org/articles.php?volume=11

Tene, O., & Polonetsky, J. (2013b). Theory of creepy: Technology, privacy and shifting social norms. Yale Journal of Law & Technology, 16, 59–102. Retrieved from http://yjolt.org/theory-creepy-technology-privacy-and-shifting-social-norms

The Canadian Copyright Licensing Agency ("Access Copyright") v. York University (8 April 2013), Toronto T-578-13 (FCTD) (Statement of Claim). Retrieved from http://www.scribd.com/doc/134926954/AC-v-York-Statment-of-Claim-T-578-13-Doc1

The Canadian Press. (2012, December 28). Personal info for thousands lost by federal government: Privacy commissioner notified about loss affecting about 5,000 Canadians. Retrieved from. http://www.cbc.ca/news/canada/story/2012/12/28/privacy-commissioner-hrdsc-lost-info-personal.html

Theoharidou, M., & Gritzalis, D. (2007). Common body of knowledge for information security. IEEE Security & Privacy, 5(2), 64–67.

Thibeault, M. D. (2012). From compliance to creative rights in music education: Rethinking intellectual property in the age of new media. Music Education Research, 14(1), 103–117.

Thomas, C., & McDonald, R. H. (2005). Millennial net value(s): Disconnects between libraries and the information age mindset. In M. Halbert (Ed.), Free Culture and the Digital Library Symposium proceedings (pp. 93–105). Atlanta, GA: MetaScholar Initiative at Emory University. Retrieved from http://www.researchgate.net/profile/Robert_Mcdonald5/publication/228452528_Millennial_net_value_(s)_Disconnects_between_libraries_and_the_information_age_mindset/links/00b7d5230d35bc0d7f000000.pdf

Thompson, S. T. (2006). Helping the hacker? Library information, security, and social engineering. Information Technology and Libraries, 25(4), 222-225. Retrieved from http://ejournals.bc.edu/ojs/index.php/ital/article/view/3355

Thornburgh, T. (2004). Social engineering: The "Dark Art". In Proceedings of the 1st Annual Conference on Information Security Curriculum Development (pp. 133–135). New York: ACM.

Totterdale, R. L. (2010). Globalization and data privacy: An exploratory study. International Journal of Information Security and Privacy, 4(2), 19–35.

Treasury Board of Canada. (2006, March 28). Frequently asked questions: USA PATRIOT ACT comprehensive assessment results. Retrieved October 28, 2015, from http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/usapa/faq-eng.asp

Tredwell, S. (2015, June 19). Copyright and clarity [Blog post]. Retrieved from http://www.slaw.ca/2015/06/19/copyright-and-clarity/

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), Reforming European data protection law (pp. 333–365). Dordrecht: Springer Netherlands.

Trusteer. (n.d.). Glossary: Remote access trojan (RAT). Retrieved October 26, 2015, from https://www.trusteer.com/glossary/remote-access-trojan-rat

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. Information Technology & People, 25(3), 327–352.

Turner, C. F., Taylor, B., & Kaza, S. (2011). Security in computer literacy: A model for design, dissemination, and assessment. In Proceedings of the 42nd ACM Technical Symposium on Computer Science Education (pp. 15–20). New York: ACM.

Turow, J. (2003). Americans & online privacy: The system is broken. Philadelphia, PA: Annenberg Public Policy Center of the University of Pennsylvania. Retrieved from http://repository.upenn.edu/asc_papers/401/

Turow, J., Feldman, L., & Meltzer, K. (2005). Open to exploitation: American shoppers online and offline. Philadelphia, PA: Annenberg Public Policy Center of the University of Pennsylvania. Retrieved from http://repository.upenn.edu/asc_papers/35/

U.S. Department of Justice. (1999, August 20). First criminal copyright conviction under the "No Electronic Theft" (NET) Act for unlawful distribution of software on the Internet [Press release]. Retrieved from http://www.justice.gov/archive/opa/pr/1999/August/371crm.htm

Univerisity of Toronto, Mississauga. (n.d.). Information Security. Retrieved October 26, 2015, from https://www.utm.utoronto.ca/math-cs-stats/prospective-students/information-security

Universities UK. (2013). Cyber security and universities: Managing the risk. Retrieved from http://www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf

University of Calgary. (n.d.). Concentration in Information Security. Retrieved October 26, 2015, from http://www.cpsc.ucalgary.ca/undergrad/courses_progression/concentration?conc=security

University of Ontario Institute of Technology. (n.d.). Information Technology Security. Retrieved October 26, 2015, from http://gradstudies.uoit.ca/future_students/masters_programs/information_technology_security/

University of Regina. (2015, May 6). Use of copyrighted materials. Retrieved from http://www.uregina.ca/policy/browse-policy/policy-GOV-050-010.html

University of Saskatchewan. (n.d.). Copyright FAQ. Retrieved October 27, 2015, from http://www.usask.ca/copyright/compliance/faq/index.php

University of Winnipeg. (n.d.). Information Assurance and Security Certificate. Retrieved October 26, 2015, from http://pace.uwinnipegcourses.ca/information-assurance-and-security-certificate

Uppuluri, P., Pittges, J., & Chase, J. (2014). Scare and prepare: Increasing awareness, safety, and passion for cyber-security. In Proceedings of the 45th ACM Technical Symposium on Computer Science Education (pp. 720–720). New York: ACM.

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: perceptions of online behavioral advertising. In SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security (Article no. 4). Retrieved from https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12007.pdf

Valentine, J. A. (2006). Enhancing the employee security awareness model. Computer Fraud & Security, 2006(6), 17–19.

van der Sloot, B. (2015). How to assess privacy violations in the age of big data? Analysing the three different tests developed by the ECtHR and adding for a fourth one. Information & Communications Technology Law, 24(1), 74–103.

Van der Veer Martens, B., & Hawamdeh, S. (2010). The professionalization of knowledge management. In E. Pankl, D. Theiss-White, & M. C. Bushing M. C. (Eds.), Recruitment, development, and retention of information professionals: Trends in human resources and knowledge management (pp. 139–156). Hershey, PA: IGI Global.

Veltsos, J. R. (2012). An analysis of data breach notifications as negative news. Business Communication Quarterly, 75(2), 192–207.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.

Viana, J., & Maicher, L. (2015). Designing innovative tools for improving literacy on intellectual property among SMEs. Technology Analysis & Strategic Management, 27(3), 314–333.

Vijayan, J. (2014, February 6). Target breach happened because of a basic network segmentation error. Computer World. Retrieved from http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html

Villasenor, J. (2012, November 27). Intellectual property awareness at universities: Why ignorance is not bliss. Forbes. Retrieved from http://www.forbes.com/sites/johnvillasenor/2012/11/27/intellectual-property-awareness-at-universities-why-ignorance-is-not-bliss/

Vilneff, A. (2015, June 2). Ontario woman wants her cut after Instagram photo sells for $90,000 without consent [Comment]. Facebook. Retrieved from https://www.facebook.com/hamiltonspectator/posts/10153265083197247

Volokh, E. (2000). Freedom of speech and information privacy: The troubling implications of a right to stop people from speaking about you. Stanford Law Review, 52(5), 2–65. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200469

Voltage Pictures LLC v. John Doe, 2014 FC 161. Retrieved from http://canlii.ca/t/g6x9l

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191–198.

Wallace, K. (2009, January 10). Textbook piracy thriving around city's campuses. The Toronto Star. Retrieved from http://www.thestar.com/news/gta/2009/01/10/textbook_piracy_thriving_around_citys_campuses.html

Wang, Y., & Zhou, H. (2012). Content analysis of library associations' privacy policies in some countries. International Journal of Digital Library Systems, 3(2), 1–12.

Warner, J., & Chun, S. A. (2009). Privacy protection in government mashups. Information Polity, 14(1-2), 75–90.

Warren, S., & Duckett, K. (2010). "Why does Google Scholar sometimes ask for money?" Engaging science students in scholarly communication and the economics of information. Journal of Library Administration, 50(4), 349–372. Retrieved from http://surface.syr.edu/sul/78/

Watson, G., Mason, A., & Ackroyd, R. (2014). Social engineering penetration testing: Executing social engineering pen tests, assessments and defense. Burlington, MA: Elsevier Science.

Weatherley, M. (2014). Copyright education and awareness: A discussion document. Retrieved from https://oami.europa.eu/ohimportal/delegate/webcontent-services/admindocs/wsdocumentdl/N7IOWIGLMRV5525U2DU36BHHNNPZE6VDV4R75YL7QZRLSJGVCIUZUALAVE4BTMBUQNPMTX5MRPYJY

Webber, S., & Johnston, B. (2000). Conceptions of information literacy: New perspectives and implications. Journal of Information Science, 26(6), 381–397.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30.

Weber, R. H. (2015a). Internet of Things: Privacy issues revisited. Computer Law & Security Review, 31(5), 618–627.

Weber, R. H. (2015b). The digital future – A challenge for privacy? Computer Law & Security Review, 31(2), 234–242.

Wecker, M. (2012, May 2). 10 high-profile people whose degrees were revoked. US News & World Report. Retrieved from http://www.usnews.com/education/best-global-universities/articles/2012/05/02/10-high-profile-people-whose-degrees-were-revoked

Weiser, M. (1999). The computer for the 21st Century. ACM SIGMOBILE Mobile Computing and Communications Review, 3(3), 3–11.

Werner, L. (2005). Redefining computer literacy in the age of ubiquitous computing. In Proceedings of the 6th conference on Information Technology Education (pp. 95–99). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1095738

White, G., & Long, J. (2007). Thinking globally: Incorporating an international component in information security curricula. Information Systems Education Journal, 5(39), 3–12.

White, G., & Long, J. (2015). Thinking globally: Incorporating an international component in information security curriculums. In Proceedings of ISECON 2006 (pp. 1–12). Retrieved from http://proc.isecon.org/2006/2324/ISECON.2006.White.pdf

Whitman, M. E. (2003). Enemy at the gate: threats to information security. Communictions of the ACM, 46(8), 91–95.

Wikipedia:Copyright violations. (2015, September 8). In Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Wikipedia:Copyright_violations&oldid=680083272

Wikipedia:Training/For students/Copyright and plagiarism. (2015, January 6). In Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Wikipedia:Training/For_students/Copyright_and_plagiarism&oldid=641290316

Wilson, M., & Hash. (2003). Building an information technology security awareness and training program (NIST Special Publication 800-50). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Wood, C. C. (1995). Writing infosec policies. Computers & Security, 14(8), 667–674.

Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Computer Fraud & Security, 2004(1), 16–17.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. Journal of the American Society for Information Science and Technology, 58(2), 212–222.

World Intellectual Property Organization. (n.d.). WIPO Academy. Retrieved October 6, 2015, from http://www.wipo.int/academy/en/

Wright, D. (2013). Making privacy impact assessment more effective. The Information Society, 29(5), 307–315.

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. International Review of Law, Computers & Technology, 28(3), 277–298.

Wu, Y., Lau, T., Atkin, D. J., & Lin, C. A. (2011). A comparative study of online privacy regulations in the U.S. and China. Telecommunications Policy, 35(7), 603–616.

Wyatt, A. M., & Hahn, S. E. (2011). Copyright concerns triggered by web 2.0 uses. Reference Services Review, 39(2), 303–317.

Yankova, I., Vasileva, R., Stancheva, S., & Miltenoff, P. (2013). A bibliographical overview of "copyright literacy" as a key issue in memory institution management. In S. Kurbanoğlu, E. Grassian, D. Mizrachi, R. Catts, & S. Špiranec (Eds.), Worldwide commonalities and challenges in information literacy research and practice (pp. 655–661). Cham, Switzerland: Springer International Publishing.

Zafar, H., Ko, M., & Osei-Bryson, K. M. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. Information Resources Management Journal, 25(1), 21–37. Retrieved from http://digitalcommons.kennesaw.edu/facpubs/2476/

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. Information Management & Computer Security, 17(4), 330–340.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75–89. Retrieved from http://www.hbs.edu/faculty/Pages/item.aspx?num=49122

Appendix 2: Methods

Literature review methodology: Intellectual property

Search string (adapted for the syntax of the particular database):

[(copyright OR "intellectual property" OR patent OR trademark OR “trade mark” OR ((information OR knowledge) N2 ownership)) AND (curricul* OR instruct* OR pedagog* OR literacy OR knowledge OR aware* OR perce* OR ignor* OR attitude* OR perce*)]

Time frame: no limit

Academic databases:

- Library Literature & Information Science Full Text
- Scopus
- Academic OneFile
- Academic Search Complete
- Education Research Complete

Search engines:

- Google
- Google Scholar

Literature review methodology: Privacy and security

1) Industry reports on the state of information security
   - Google searches for “information security” or “cyber security” and report or survey
   - Then focalised searches for each of the “Big Four” (Deloitte, EY, KPMG, PricewaterhouseCoopers)
   - Time limit: 2010-2015 (oldest reports found are from 2013)

2) Information security incidents
   - Google searches for “information security” or “cyber security” and “incidents” or “hack”
   - Time limit 2013-2015
   - Then focalised searches for Ashley Madison, Sony and Target

3) Regulatory frameworks
   - Google searches for “security” or “privacy” and “law” or “regula*” and “Canada” or “United States” or European Union”

4) Security and privacy issues and training
   - Databases used: Library & Information Science Abstracts and ACM Digital Library
   - Limits: 2005-2015; English, French.
   - Searches:
     - “privacy” AND “regul*”
     - “security” AND (“curricul*” OR “training”)
     - “privacy” AND (“curricul*” OR “training”)
     - “social engineering” AND (“curricul*” OR “training”)
     - “security” AND (“issues” OR “trends”)
     - (“big data” or “ubiquitous computing”) and “privacy”

5) Citation tracking (both directions) using Web of Science, Scopus and Google Scholar