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

Follow this and additional works at: https://ir.lib.uwo.ca/fimspub

Part of the Library and Information Science Commons

Citation of this paper:
https://ir.lib.uwo.ca/fimspub/35
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 .................................................................................................................................... i
Executive Summary .......................................................................................................................... ii
Key Findings ..................................................................................................................................... 1
  Context ......................................................................................................................................... 1
  Implications ................................................................................................................................... 2
  Approach ....................................................................................................................................... 2
  Background ................................................................................................................................... 3
Knowledge or Expertise Gaps ......................................................................................................... 5
Regulatory Environment ................................................................................................................ 8
Workplace/Employer demand ......................................................................................................... 11
  Key Competencies for Information Management .................................................................... 13
Additional Resources ..................................................................................................................... 19
Further Research and Research Gaps ............................................................................................. 19
Knowledge mobilization .................................................................................................................. 19
References ....................................................................................................................................... 21
Appendix I: Complete bibliography ............................................................................................... 34
Appendix 2: Methods ......................................................................................................................... 66
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*. 

iii
**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 fulfill 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 (Veltos, 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 & McCrohan, 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 (Roos, 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.
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

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 be disabled to prevent copying of content; software use could require a registration key; e-books may be limited in terms of 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 website 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 Indeed², 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

<table>
<thead>
<tr>
<th>Competency or Skill Type</th>
<th>Description</th>
<th>Intellectual Property</th>
<th>Information Privacy</th>
<th>Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conceptual foundations</td>
<td>Introduction to fundamental concepts and components in each of the three key areas.</td>
<td>Develop an understanding of the components of information ownership: the principles of copyright, fair dealing and fair use.</td>
<td>Develop an understanding of the components of privacy: types of personal information; principles of fair information practices; information life cycle.</td>
<td>Develop an understanding of the requirements for effective information security governance: threats; information security strategy; organisational alignment</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>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.</td>
<td>Assess business-to-business (b2b) threats to organization’s IP, onsite and off. Secure IP through R&amp;D and production, and in storage.</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Tool and techniques for threat responses</td>
<td>Introduction to the tools and techniques for responding to threats in the three key areas</td>
<td>Develop an understanding of the tools and techniques used to license information ownership, such as Creative Commons; knowledge regarding appropriate citation practices</td>
<td>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.</td>
<td>Develop an understanding of the of tools and techniques used to mitigate privacy threats: monitoring of behavioural tracking,</td>
</tr>
<tr>
<td>Communications</td>
<td>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.</td>
<td>Develop written materials describing firm’s policies regarding its IP holdings and communicate on this topic with internal and external stakeholders.</td>
<td>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).</td>
<td>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</td>
</tr>
<tr>
<td>Contract Negotiation and Compliance</td>
<td>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.</td>
<td>Manage electronic resources, participate in and/or manage vendor/partner negotiation, end-user compliance, and licensing related to organization’s IP.</td>
<td>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.</td>
<td>Ensure that any contractual obligations the organization enters into comply with and protect organization’s information security, and that of staff and customers.</td>
</tr>
<tr>
<td>Evaluation and Assessment</td>
<td>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.</td>
<td>Ability to assess and evaluate organization’s IP program and its management; make recommendations in areas deemed to not meet performance standards.</td>
<td>Ability to assess and evaluate organization’s information privacy program and policies; make recommendations in areas deemed to not meet performance standards.</td>
<td>Ability to assess and evaluate organization’s information security program and policies; make recommendations in areas deemed to not meet performance standards.</td>
</tr>
<tr>
<td>Human Resource Management</td>
<td>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.</td>
<td>Ability to assess and meet organization’s needs in the area of IP staffing.</td>
<td>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.</td>
<td>Ability to assess and meet organization’s needs in the area of information security staffing. Develop and deliver information security training to staff.</td>
</tr>
<tr>
<td>Organizational Knowledge Management</td>
<td>Program participants will attain the ability to make strategic recommendations and to plan for the organization’s knowledge management</td>
<td>Work with operational employees and technologists to devise best practices for organization’s IP management,</td>
<td>Ensure that information privacy considerations are taken into account in the building, deployment and ongoing</td>
<td>Ensure that information security considerations are taken into account in the building, deployment and ongoing</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Planning</th>
<th>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.</th>
<th>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.</th>
<th>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.</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Awareness and Compliance</td>
<td>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.</td>
<td>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.</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Policy Development</td>
<td>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</td>
<td>Develop and implement policy framework around firm’s IP and business data utilization, access and storage (analogue and</td>
<td>Create and implement local policies that comply with regulatory frameworks pertinent to the organization at provincial,</td>
<td>Create, monitor and implement ethical guidelines and information-related codes of conduct for organization’s</td>
</tr>
<tr>
<td>Project Management</td>
<td>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.</td>
<td>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.</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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


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


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


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


Appendix I: Complete bibliography


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


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


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


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.


61


evander 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.


63


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 “regul*” 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
   - Searches:
     o “privacy” AND “regul*”
     o “security” AND (“curricul*” OR “training”)
     o “privacy” AND (“curricul*” OR “training”)
     o “social engineering” AND (“curricul*” OR “training”)
     o “security” AND (“issues” OR “trends”)
     o (“big data” or “ubiquitous computing”) and “privacy"
5) Citation tracking (both directions) using Web of Science, Scopus and Google Scholar