Computers & Education 103 (2016) 124–133

Contents lists available at ScienceDirect

Computers & Education

journal homepage: www.elsevier.com/locate/compedu

Beyond identifying privacy issues in e-learning settings – Implications for instructional designers

Hui-Lien Chou*, Chao-Hsiu Chen

Institute of Education, National Chiao Tung University, 1001 Ta-Hsueh Rd., Hsinchu, 30010, Taiwan, ROC

ARTICLE INFO

Article history:
Received 19 January 2016
Received in revised form 3 October 2016
Accepted 7 October 2016
Available online 11 October 2016

Keywords:
Instructional design
Data protection
Privacy
E-learning

ABSTRACT

Players in the digital economy increasingly rely on the large-scale collection or exchange of personal data. Because online data can be persistent and immense, e-learning researchers and educators should advise people to make constructive use of online data and to disclose the data with caution. However, few studies have indicated that data protection issues are particular concerns in e-learning practices. Drawing on a systematic literature review, this paper examines personal data protection issues related to instructional design and e-learning. We aim to understand the online data protection-related issues that instructors or instructional designers encounter rather than reiterating that users must be aware of the informative and persistent characteristics of online data. The themes that emerged from the literature review can be classified into two typologies. One typology refers to the identification of privacy issues as a particular concern in the instructional design of e-learning, and the second typology is the implementation of data protection as a subject matter in the pedagogical design for e-learning. The results of the review and their implications for further research are then discussed.

1. Introduction

The emphasis on educational transformation via technology, such as teachers' required professional development in information communication technologies (ICTs), the application of innovative technology in various educational settings, and the integration of creative technology and instruction, urges instructors to utilize the Internet to any extent possible. The high level of Internet penetration and the substantial repository of information stored online facilitate learning and raise several issues (Stavrositu & Sundar, 2008; Underwood & Szabo, 2003). Among the issues raised, the persistence and extensibility of the data posted online have profound effects. Except for users' lack of competence in searching or validating the information, their reckless behaviors of sharing data online also pose a threat. Research has indicated that students engage in risky Internet behavior on social community websites by neglecting their personal data (Vanderhoven, Schellens, & Valcke, 2013). Internet fraud and even cyberbullying often result from the careless divulgation of personal data. To tackle these problems, researchers stress the importance of information literacy (McClure, 1994). However, among the skills subsumed by information literacy, data protection seems less rendered. Most of the studies often claim that data protection issues (more generally, privacy issues) warrant further investigation but do not focus on these issues (e.g., Mike & Roy, 2014; Terry, 2011). Alternatively,

* Corresponding author.
E-mail addresses: hlien.tw@gmail.com (H.-L. Chou), chaohsiuchen@mail.nctu.edu.tw (C.-H. Chen).

http://dx.doi.org/10.1016/j.compedu.2016.10.002
0360-1315/

researchers adhere to anonymity when analyzing questionnaires and, thus, claim that they ensure subjects' privacy (Manero, Torrente, Serrano, Martínez-Ortiz, and Fernández-Manjón (2015)).

Using the Internet leaves indelible tracks, such as log files, cookies and posts. In the face of these indelible tracks, a sense of psychological safety can put users at ease. A substantial amount of research on e-commerce has found that a safe e-commerce environment helps to increase shoppers' willingness to make online purchases. These studies further propose several strategies to improve the customized shopping experience without intruding on a purchaser's privacy, e.g., Chellappa and Pavlou (2002) and Patton and Jøsang (2004), to name a few. In line with this perspective, we need to understand how the climate of a safe e-learning environment helps to increase learners' willingness to engage in online learning or to utilize the Internet. We also need to be acquainted with strategies that help educate learners on essential skills in ICTs use and optimize the customized learning experience without intruding on learners' privacy.

Drawing on a systematic literature review, we identified and selected peer-reviewed research papers concerning issues of data protection related to instructional design as well as e-learning. We then synthesized the related evidence. The present study aims to understand the online data protection-related issues that instructors or instructional designers encounter rather than reiterating that users have to be aware that the technologies in common use are informative and generate persistent data. The results of the systematic literature review and their implications for further research and for relevant instructional design are then discussed.

2. Concept clarification

2.1. Privacy, informational privacy and personal data protection

Before we present the literature review, we would like to further discuss the relationship between privacy and data protection. There exist difficulties in giving a clear-cut concept of privacy (McCloskey, 1980). In the late 18th century, people stridently requested penalties for the unauthorized use of portraits and ruthless publicity. The right to privacy emerged as a result of the inadequacy of the existing legislation. The right to privacy was derived from “the right to life”, which evolved into “the right to enjoy life”, and then became “the right to be left alone” (Warren & Brandeis, 1890). As mentioned by Warren and Brandeis (1890), new rights will be recognized as changes occur in political, social and economic phases. With the advent of ICTs, the right to privacy is currently associated with informational privacy right (Tavani, 2009, pp. 131–164).

Informational privacy right is regarded as the right to control one's personal information and is closely related to several aspects of private life. People have the privilege of determining how to compose their personal data, store the data, and utilize the information independently (Westin, 2003). The emergence of informational privacy right from the right to privacy is inevitable in modern society. Passive protection against the invasion of one's land becomes *active defense* (italics for emphasis) against any decision related to an individual's personal data. All personal facts, communications, opinions, and even sensitive data such as health records are reasonably expected to be private. Thus, people wish to restrict the dissemination of this information.

Several researchers constructed the concept of privacy in e-learning on the basis of informational privacy. They adopted items such as “accessing files with the aim of reading or altering” to measure the construct of informational privacy invasion (Friedman, 1997), “getting junk email or unwanted mail” to measure the perceived vulnerability to privacy risks (Youn, 2005), and “being concerned about submitting my personal information in social networking sites” to measure the construct of informational privacy concern (Mohamed & Ahmad, 2012).

Some people labeled informational privacy as (personal) data protection. In the early stages, personal data protection regulations were linked to the data processed by computers. For example, in 1981, the Council of European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data distinguished “automatic processing” from manual processing. However, the current legislation has abandoned this distinction. All data processed either automatically or manually are protected under the relevant legislations. Whether data are subject to the legislation depends on whether the data are related to an identifiable individual. The EU Data Protection Directive is widely viewed as a far-reaching data protection regulation. Article 25 of EU Directive 95/46/EC requires Member States to transfer the data to a third country only if the third country in question ensures an adequate level of protection. Following the development of this regulation, individual European nations must not only enact data protection laws but also be careful of transborder data flows. The EU Data Protection Directive even applies to the non-EU countries, such as Iceland, Liechtenstein and Norway. Many countries around the world, such as Canada and Taiwan, consider the core ideas presented in the Directive when enacting their own related legislations. The central idea in the Directive is that the processing of personal data should be accurate, up-to-date, relevant, and not excessive in relation to the purposes for which they are processed (European Commission, 2016). Based on this big idea, subjects can request the retrieval, revision, and deletion of their personal data.

In what follows, we will use the terms privacy, informational privacy and data protection interchangeably.

2.2. Information literacy and articulation of privacy issues

Many available lists help define information literacy (e.g., the seven pillars of information literacy from the Society of College, National and University Libraries (SCONUL) in the UK; the six core standards from the Australian and New Zealand Institute for Information Literacy (ANZIL); information literacy competency standards for higher education from Association

for College Research Libraries (ACRL) in the US). Haythornthwaite and Andrews (2011, pp. 125–142) summarize the aforementioned standards as that an individual is able to identify the information need, to locate the information, to evaluate the information located, and to apply that information appropriately. In the past, librarians often played a vital role in teaching and aiding users in acquiring such skills (Rader, 1999). Currently, information literacy is almost becoming a prerequisite when using the Internet (Edward, 2005). The literature even validates that information literacy can be imparted to students (Ng, 2012).

Another definition is provided by Johnston and Webber (2003),

> 'Information literacy is the adoption of appropriate information behaviour to obtain, through whatever channel or medium, information well fitted to information needs, together with critical awareness of the importance of wise and ethical use of information in society.' (p.336)

Perhaps the meaning of the "ethical use of information" is open to interpretation. More often, researchers address ethical use of the information as users' understanding of intellectual property, copyright, and fair use of copyrighted material (e.g., Nicholas (2006); Wen and Shih (2008);). However, the so-called ethical use of information is also related to the articulation of privacy issues. According to the performance indicators suggested by the ACRL (Association for College Research Libraries, 2016), an information-literate person would be able to (1) identify and discuss issues related to privacy and security in both the print and electronic environments; and (2) legally obtain, store, and disseminate text, data, images, or sounds. Similarly, based on the expected learning outcomes suggested by the ANZIL (ANZIL., 2016), an information-literate person would be able to (1) identify and articulate issues related to privacy and security in the print and electronic environments; and (2) obtain, store, and disseminate text, data, images, or sounds in a legal manner.

All of the above leads to the importance of users' articulation of privacy issues in regard to information literacy.

3. Methods of the literature search

We conducted a search of the databases Education Research Information Center (via EBSCOhost) and Social Science Citation Index (SSCI) to identify peer-reviewed studies in the field of educational research published before Dec. 2015. To identify the implications of e-learners' online data protection for instructional designers and instructors, we first performed a keyword search of combinations of the following sets of terms. The first set includes privacy and its related terms, such as disclosure and data protection. The second set includes instruction and its alternative keywords, such as instructional design, education and teaching. The articles' years of publication were restricted to within the past 10 years in an attempt to reflect a certain level of advancement in ICTs in the educational setting. Abstracts were retrieved and browsed to determine whether the articles targeted e-learning and matched our interest. Articles concerning e-government, e-business, system designs of information security, and general privacy issues were excluded. We then screened the available full-text articles of potentially relevant papers to determine whether they qualified for inclusion in our literature review. Eligible studies must indicate that privacy is a particular concern for instructors/instructional designers in the educational contexts rather than as conceptual concerns of the researchers. For example, Bower and Sturman (2015) addressed privacy protection of wearable technologies as foreseeable issues in educational application by qualitatively analyzing educators' responses in the open-ended questions. Respondents in their research illustrate that people are able to surreptitiously take photos and record videos and thereby invade privacy. This kind of article did not present what actually happened, and thus was not qualified for further examination in this research. Studies were also included in the review if they adopted data protection as the pedagogical content. The reference lists of included articles were further examined to locate additional relevant papers. After several rounds of reading and discussion, 19 original research articles were included in the literature review. Although all of the articles contribute to our understanding of data protection in e-learning, most of them do not include experimental designs with statistical analyses. As a result, they are not suitable for a meta-analysis.

4. Results

Guided by the research objective, the literature review on instructional designs and privacy/personal data protection issues can be divided into two typologies. One typology refers to the identification of privacy issues as a main concern in the instructional design of e-learning, and the second typology is promoting a sense of data protection in the e-learning environment through pedagogical design. The first typology foregrounds the existence of privacy issues when implementing e-learning, and the second typology directs us to cultivate e-learners' senses of personal data protection in the e-learning environment.

4.1. Privacy issues as a particular concern of instructors/instructional designers

Several studies adopted qualitative research methods to understand the issues that instructors/instructional designers face in the e-learning context (see Table 1). In their early work involving focus group interviews, McPherson and Baptista Nunes (2006) identified robust security, data protection and intellectual property protection as critical success factors in implementing e-learning in higher education. Raitman, Ngo, Augar, and Zhou (2005) presented a case study and showed that students valued a sense of security on the wiki platform and, hence, were more willing to collaboratively edit work online. A

similar logic was applied in the case study that Wang and Smith (2013) conducted on m-learning. The instructional designer found that students' low level of participation in quizzes resulted from their privacy/security concerns. Additionally, according to the ethnographic content analysis performed by Schultz (2012), the members, including teachers and developers, of the 'Security and Privacy' discussion forum of the Moodle learning management system (LMS) addressed the topic of user privacy when running the LMS.

The privacy issues presented in the research are multifaceted. The interviewees suspected that they had been divulging learners' personal data to unauthorized third parties and attempted to curtail their inclination to track learners' online activities (Lin, 2007). Fear of unauthorized or circuitous access to personal information stored on the Internet was another concern (Kuzu, 2009). Moreover, when existing social media were fully incorporated into formal learning, educators were concerned about students' improper posts on SNSs. Specifically, they were concerned that students' online posts of improper materials might harm their career opportunities and that the educators' identity as professional educators might be ruined (Chen & Bryer, 2012).

Recently, Plesch, Kaendler, Rummel, Wiedmann, and Spada (2013) ran a three-year international Delphi study to determine the obstacles resulting from the inclusion of ICT in education. The researchers collected visionary statements and asked domain experts to iteratively evaluate them. The authors then identified five tensions impeding the inclusion of technology in learning. The tension between data tracking and data privacy plays a role in this research. The authors further suggested that it is necessary to teach learners data literacy skills to ensure their maximum control over their personal data and to enable personalized learning. Analogously, Siu Cheung et al. (2014) reviewed literature on e-learning in school education and suggested that stakeholders should consider the privacy/legal issues of learning data in the e-learning process.

4.2. Data protection as a subject matter in the pedagogical design

Various methods were adopted to cultivate learners' sense of data protection through the pedagogical design of e-learning. One method utilized direct instruction with information technology, and another applied dialectics to alter pre-service teachers' perception of privacy. Similar instructional approaches were implemented by adopting a video-based intervention. In addition, another method designed a privacy-aware e-learning environment to reinforce users' senses of right to informational privacy (see Table 2.). Generally, there are increasing studies on the pedagogical design for data protection as a subject matter. Additionally, the implemented pedagogies were diverse, but the findings all indicated positive learning effects.

Among the pedagogical designs, the study of Vanderhoven, Schellen, and Valcke (2014) is the only one we found that adopted the sample in secondary education. The authors employed several guidelines, such as discussion and authentic learning, to develop materials educating pupils on the risks involved in using social networking sites (SNSs). The risks caused by various forms of problematic behavior on SNSs were incorporated into the materials. The quasi-experiment intervention revealed that a 1-h course on "content risks" posted on the SNSs led the pupils to change their privacy settings of the content of their profile, including their pictures, interests, and personal information. A 1-h course on "contact risks" guided the students to alter the privacy settings of their contact information. Students modified their privacy and account settings after completing the commercial risks course. Thus, the courses lent themselves to transform adolescents' behavior.

University students are the main audience when it comes to data protection pedagogy. As far back as 2009, Foulger, Ewbank, Kay, Popp, and Carter (2009) foresaw the imperative for pre-service teachers to utilize social networks and to

Table 1
Overview of the literature identifying privacy issues in e-learning (arranged by year).

Author	Research method	Specific privacy issues
Raitman et al. (2005)	A case study on two groups of students in tertiary education: one group used a wiki platform with a user login, while the other group did not	Sense of security enhances students' willingness to collaboratively edit work online
McPherson and Baptista Nunes (2006)	Focus group interviews with practitioners in fields related to educational technology and e-learning	Data protection is a critical factor in successfully implementing e-learning in higher education
Lin (2007)	Interviews with 20 professional technologists of educational institutes	The specialists were susceptible to revealing learners' information and inclined to track learners' activities
Kuzu (2009)	Interviews with 20 graduates of computer education and instructional technologies departments working as computer teachers or software experts	The Internet allowed unauthorized or circuitous access to personal information
Chen and Bryer (2012)	Interviews with 57 public administration faculty members, including professors employed by the university	Students' posts of improper material on SNSs had negative consequences
Schultz (2012)	An ethnographic content analysis of the discussions on a 'Security and Privacy' discussion forum of the Moodle learning management system	The topic of user profile/privacy was frequently discussed in the forum
Plesch et al. (2013)	International Delphi study with researchers with various professional backgrounds from 16 European research institutions	There is tension between data tracking (recording of personal learning) and data privacy
Wang and Smith (2013)	A case study on m-learning of English reading and grammar	Students' concerns about privacy led to low levels of engagement
Siu Cheung et al. (2014)	Literature review on e-learning in school education	The learning data that is tracked during the learning process should be considered at the policy level

Table 2
Overview of research adopting data protection as the pedagogical content (arranged by year).

Authors	Learning objectives	Pedagogy	Measurement of learning effectiveness	School level	Highlights
Kennewell (2001)	Help students understand the data protection law and the principles behind it	Comparison of three pedagogies: guided web search with written report assignments, non-guided web search with written report assignment, and group discussion and presentation	Teachers' reflection on and evaluation of their teaching activities	Not available	Meta-cognitive and literacy skills were greatest in the pedagogy of group discussion and presentation; no meta-cognitive and literacy skills were reflected in the direct instruction
Foulger et al. (2009)	Have pre-service teachers not only utilize the SNSs but also recognize the visibility of their online behavior	Case-based reasoning with iterative articulation and reflection in response to the inquiry questions	Pre- and post-test responses to two parallel scenarios	Pre-service teachers	Pre-service teachers have limited awareness of what they rendered in the SNSs; they also ask for clear guidelines and school-wide policies on teachers' conduct in the virtual world
Anwar and Greer (2011)	Enhance students' awareness of data protection and willingness to share information	Adopt a privacy-aware discussion forum with controversial topics for students to discuss under different identities	Post-use survey	College students	Students gained knowledge of data protection and were more willing to share privacy-preserving information
Chang (2011)	Improve students' information ethics values	Groupware-supported synchronous discussion for the teacher and students with information ethics course training	Scenario-based survey with open-ended questions	College students	The course was effective in improving all students' value of privacy, students considered privacy breaches to be immoral, and the majority of students refused to violate privacy in the scenario-based survey
Wills and Zeljkovic (2011)	Educate users on what information is obtained and inferred about them via behavioral tracking	A website for users to browse; the researchers then obtained users' visiting history and location information. The users were then shown the collected data	Users' feedback after they are shown their visiting history	Volunteer users aged 25-44 years	The majority of users demonstrated concern for the web tracking and reported a willingness to use ad blocker tools and delete their cookie histories periodically
Nosko et al. (2012)	Examine whether content of Facebook profiles differed as a function of priming story and gender	One of three priming stories (anecdotal, legal or neutral) presented to participants prior to constructing a profile for either a male or a female	Adopt previously established scoring tools to assess online disclosure and privacy settings.	Freshmen at a university	Females disclosed less sensitive information than males after reading the anecdotal privacy story
Vanderhoven et al. (2014)	Educate pupils on the risks involved in using SNS	Direct instruction with specially designed materials and real-life examples	Pre- and post-tests	11- to19-year-old pupils	The pupils changed their privacy settings on Facebook
Noh (2014)	Have the librarians realize general privacy concepts and infringements of users' privacy	Direct instruction with privacy infringement cases and a discussion session	Pre- and post-tests	Librarians	The librarians were concerned with the protection of users' privacy, such as perceived users' privacy infringement and data storage period, and demand for privacy education increased
Walton et al. (2015)	Help students recognize the visibility of their Facebook profiles and the importance of informational privacy	Lecture, presentation of data, introduction to search skills and small group discussion	Feedback questionnaires and pre-/post- Facebook profile search	Students in medical education	Students agreed with the importance of the topic of informational privacy on SNSs; the post-Facebook profile search revealed that many students modified their privacy settings as a result of the course
Archer et al. (2015)	Determine how the instructional intervention altered non-/experienced users' decision on data disclosure online	Video instruction to encourage users to make greater use of privacy settings and to set more restrictive privacy settings	Alteration of privacy settings	Freshman at a university	The experienced users adopted more restrictive privacy settings after watching the videos but continued to disclose more data than the novice users

recognize the visibility of their online behavior. Case-based reasoning was adopted as an intervention to alter pre-service teachers' perceptions of SNSs and, thus, to inhibit them from overly exposing themselves online. The authors presented the case-based coursework in three phases. Phase 1 helped the learners (pre-service teachers) understand the tools of SNSs. Phase 2 introduced them to the adoption of SNS tools for educational purposes. The pros and cons of such tools were demonstrated as well. Phase 3 revealed how the educational institutions condemned SNSs. Through iterative articulation and reflection in response to the inquiry questions, the learners became conscious of the complexity of SNSs. Learners' responses to two parallel scenarios with different superficial features were coded as pre- and post-test measures. The two scenarios involved the negative consequences of teachers' utilization of social networks, as well as multiple ethical issues, such as teachers' jurisdiction over students' online data and students' rights to privacy. The coursework intervention led the learners to not only develop a multi-perspective reasoning but also to recognize the tensions among stakeholders. Participants'

neglect of social contract issues (i.e., social networking media are not true public spaces and teachers are examined by a higher standard of conduct) highlighted pre-service teachers' limited awareness of the information they provided in the SNSs. The statistically significant pre-post change in this research demonstrated pre-service teachers' desire for clear guidelines and school-wide policies on teachers' conduct in the virtual world.

Social networking sites (SNSs) are the common scenario where researchers intervened in data protection pedagogy. Except for the previous two studies, Nosko et al. (2012); Walton, White, and Ross (2015) and Archer et al. (2015) considered the nuance of privacy settings as evidence of effective pedagogy. In the study of Archer et al. (2015), for example, an video-based intervention was employed to discourage users from disclosing too much data on SNSs. Archer et al. (2015) conducted an experiment with random assignment to test whether an instructional intervention altered users' decisions regarding data disclosure online. Experienced/novice users watched a 15-min video on the data disclosed on Facebook and were asked to make an informed decision on this topic. The video encouraged users to make greater use of privacy settings and to set more restrictive privacy settings. The results showed that experienced users adopted more restrictive privacy settings after watching the videos but continued to disclose more data than the novice users.

To deter users from exposing themselves too much on SNSs, Walton et al. (2015) incorporated an educational activity addressing the accessibility of information on SNSs. The faculty member, who was not a “friend” or “friend of a friend” of any member of a specific medical class, systematically searched for the public Facebook profile of each member in the class. The researcher then presented the collected data to the class in a session. The session included a lecture, presentation of the data, an introduction to search skills and small group discussion. Students were required to submit a written reflection at the end of the session. The feedback questionnaire, which was administered at the end of the session, demonstrated that students agreed with the importance of informational privacy on SNSs. One month later, the researchers conducted the search again and found that many students had modified their privacy settings.

Another approach to the data protection pedagogy attached to SNSs was taken by Nosko et al. (2012). Three different types of materials were provided to the participants before they registered a Facebook account. The material included priming stories (i.e., anecdotal, legal, and neutral), target person profiles and a Facebook privacy setting booklet. The anecdotal story described a stalking incident, the legal story summarized a ‘typical’ online privacy statement, and the neutral story was unrelated to privacy. Participants were required to construct a profile for either a male or female after reading the story. The online disclosure and privacy statuses that the participants set were then assessed according to the previously established scoring guidelines. The statistical analysis revealed that females in the neutral group disclosed significantly more sensitive information than those in the legal group. Approximately half of the participants who utilized the privacy setting booklet reported that they learned something new about privacy settings.

In-class discussion and discussion forums are often-seen means for researchers to facilitate learners' senses of data protection. Anwar and Greer (2011) designed a privacy-aware asynchronous discussion forum such that users can assume different partial identities or even anonymous identities. The researchers generated seven controversial topics in the discussion forum and recruited 35 students to post on the forum. Twenty of the students completed the post-use survey and reported that they acquired knowledge of data protection and were more willing to share privacy-preserving information due to the privacy-aware mechanism. Chang (2011) also implemented a groupware-supported synchronous communication system in her information ethics class. The system enabled the teacher and students to share knowledge in the chat room, where the instructor could also provide immediate feedback on students' questions. The coding of the open-ended questionnaires revealed that students learned the values of “respect rules,” “privacy”, “accessibility” and “intellectual property” from the course. Compared with the students who did not take information ethics courses, only a small proportion of the students who took these courses were willing to infringe on others' privacy.

The aforementioned research either contrasts the post-instruction behavioral intention or compares pre- and post-behavior after carrying out a unitary pedagogy. Nevertheless, Kennewell (2001) tried to compare three different pedagogies in one study. He designed a data protection course on students' web searching, information organization and presentation. The learning objective of this instructional design is to promote students' understanding of the data protection law and the principles behind it. Three teachers served as mentors and employed different methods to scaffold students' intentional Internet search. One of the teachers instructed students to perform a keyword search, designed partially-complete PowerPoint slides with questions to be answered, and finally displayed the complete slides to students to clarify their understanding. Following their web search, students wrote reports on data protection. The second teacher presented the completed slides and directly instructed the students. He then asked students to write reports on data protection. The third teacher created his own slides with several questions about privacy issues. He then asked students to form groups, create reports and present the reports to the entire class. According to the teachers' reflections and evaluations, the assessment tasks revealed that students displayed greater attainment through the third teaching method than through the first and second methods. The second teacher confessed that the students in his group did not exhibit meta-cognitive and literacy skills in the assessment tasks.

Two studies adopted adults as the target audience, and the effectiveness of the pedagogy was checked by contrasting the pre- and post-behavioral intention/attitude. Wills and Zeljkovic (2011) constructed a website and invited potential users to utilize the website. The authors collected users' visiting history and predicted their location and profile. The researchers then sent the data to the users and requested their feedback on web-tracking tools. More than half of the users reported that they were concerned about third parties' monitoring activities, and approximately half of the users reported concern about their

location information and inference of demographic information. The majority of the users reported that they were willing to use ad blocker tools or delete cookies periodically.

Noh (2014) developed an education program to educate librarians about library users' privacy. The educational program was divided into three hour-long parts. The first part was a general introduction to privacy-related concepts and privacy infringements. The second part focused on privacy issues affecting digital library services. The first and second sections were implemented via direct instruction. Discussions on library privacy protection policy and relevant legislations were held in the third section. Pre- and post-tests were adopted to evaluate learning outcomes, and the results revealed that the librarians' concern with the protection of users' privacy, such as perceived users' privacy infringement and data storage period, and demand for privacy education increased following the intervention program.

In sum, several researchers have developed tertiary education pedagogies to cultivate learners' sense of data protection. To our knowledge, the study by Vanderhoven et al. (2014) is the only research that relied on a sample of high school students. With the development of web 2.0 technologies and services, an increasing number of people express themselves and interact with others online. It appears as though increasing researchers and educators have become aware of the importance of data protection education, especially the data protection on SNSs. The majority of pedagogical methods that were adopted are "direct instruction". The real-life cases/examples often attached to the pedagogy of direct instructions for further discussion.

Notably, the researchers focused the pedagogy contents on passive protection rather than active defense. Users were educated not to disclose too much information online. The researchers also addressed how to set SNSs' privacy settings such that users' personal data would not be accessed arbitrarily. However, it is not unusual that Internet users posted others' data online recklessly. To remedy this situation, users can request that the service providers delete or correct the data. The active defense against others' malicious use of the data is not instructed in these studies.

5. Implications for instructional designers

5.1. Moving beyond the identification of privacy issues

Computers automate and, thus, inform (Haythornthwaite & Andrews, 2011, pp. 125–142). Most educators consider privacy concerns when implementing or designing e-learning courses. This literature review foregrounds privacy as a primary concern in e-learning from the perspective of instructional designers in higher education. Little research depicted instructional designers' strategies of coping with the privacy concerns. Lin (2007) reported that the most commonly employed strategies are referring the problems to a collaboration team or related laws/policies. The results of the interviews conducted by Kuzu (2009) suggested that education on computer ethics and ethical principles, such as technical solutions, personal discreet conduct and legal precautions, is needed. Foulger et al. (2009) concluded that pre-service teachers requested clear guidelines or school-wide policies regarding their conduct in the virtual world.

In light of the overwhelming privacy concerns in e-learning and the lack of clear guidelines, further research should be conducted on instructors/instructional designers' coping strategies. How these coping strategies lead to successful or defeasible e-learning practices could be examined. In some cases, instructors/instructional designers implemented technical solutions, such as the utilization of passwords, to prevent the propagation of privacy issues (Lin, 2007). However, an over-reliance on the technical solution, rather than treating the online data protection seriously, is detrimental. This research field could be extended through an examination of the ways in which specific technological features mediate the consideration of privacy issues in educational contexts. Moreover, factors fostering or impeding instructors/instructional designers' sense of data protection (e.g., Chou and Chou (2016)) warrant investigation.

5.2. Heading toward multifarious pedagogies of data protection

Previous work has identified discrepancies between users' intention and behavior in regards to privacy-related decisions (e.g., Norberg, Horne, and Horne (2007)). Learners should be warned about the risks of divulging data online. It is feasible to create specific courses that educate learners about data protection. We have provided several examples of studies facilitating a sense of data protection, manifesting how the approaches can enrich learners' understanding of data protection. Studies on data protection education have increased in recent years. The methods that were introduced included dialectics, direct instruction, video-based intervention, and learning by doing. Discussion attached to situational cases also helped strengthen learners' understanding of data protection. The pedagogy did not indicate the same effects for different audience. Archer et al. (2015) found the effectiveness of the pedagogy was different for experienced and novice users. Nosko et al. (2012) found the effectiveness of the pedagogy was different for female and male users.

Generally, the instruction methods introduced in our literature review indicated positive learning effects. In this regard, we tentatively conclude that pedagogies are effective partly due to learners' lack of a sense of data protection. Consequently, such literacy skills cannot be ignored. However, the pedagogical research pertaining to data protection relied mostly on samples from tertiary education. Input from primary and secondary school educators might be needed because the Internet is utilized across these school levels. Moreover, a more refined audience segmentation in the pedagogy pertaining to data protection is needed. Careful segmentation of the audience, by gender or by experience, lends support to identifying an individual's perception and competence specific to the data protection domain.

Although the relevant research and educational programs have emerged in recent years, the pedagogies introduced seem to not be theory-based. Such instructional design models, such as the ARCS (attention, relevance, confidence and satisfaction, Keller (1987)) or ADDIE(analyze, design, develop, implement and evaluate) models, were not presented in the studies. In addition to the instructional design model, several theories related to data protection, such as "fear appeal" or "protection motivation theory (PMT)", are also missing in the literature on data protection pedagogy. The study by Wills and Zeljkovic (2011) that we introduced is actually associated with fear-appeal theory. By revealing to users their Internet log files, the authors appealed for data protection. Arachchilage and Love (2014) ever adopted the PMT to explore users' awareness of information security and proposed the factor model to design instructional materials. Certainly, instructional design is an admittedly pragmatic field. We support any creative teaching methods that cultivate learners' sense of data protection. Theory-grounded pedagogy was also recommended. We further recommend that educators incorporate the related concepts into every e-learning context to help learners develop well-reasoned responses to privacy issues. Concepts of data protection could be infused into school curricula to form the underlying structure of information literacy in e-learning.

Finally, most people have a limited sense of online data protection. Users were educated to post information online with caution and to set privacy settings on SNSs. Beyond the passive protection of limiting the data presented, learners can ask service providers to offer, modify, or delete stored data. Recently, several cases asking Internet or social network service providers to delete users' previously stored data have been filed in Europe. This right was termed "the right to be forgotten" (Ausloos, 2012). These concepts of data protection, passive defense or active defense, should be integrated into school curricula as a foundation of information literacy in e-learning.

6. Conclusion

Due to the unbounded dissemination of online data, many legislations concerning data protection have been passed. The phenomenon of coping with data protection legislation in the setting of e-learning has received comparatively less attention in the literature. The studies introduced in this literature review indicated that data protection issues are particular concerns in e-learning practices without mentioning how the instructors coped with these issues. Instructional designers lack the competence to address them. Such cases will be common occurrences when instructional designers innovatively integrate ICT into education. Experts of wearable technology in education suspected the related privacy issues (Bower & Sturman, 2015). Researchers indicated that data privacy should be incorporated into IT education to ensure that application designs comply with the international data protection legislative trends (Romney & Romney, 2004). We recommend that data protection be incorporated into learners' education as a basic literacy skill. Furthermore, pre-service and in-service teachers – and even instructional designers – should develop such literacy skills through formative education (Beycioglu, 2009).

Players in the digital economy increasingly rely on the large-scale collection or exchange of personal information. As e-learning researchers or educators, we must address the fact that online data are persistent and immense, and we should make constructive use of these data and disclose personal data with caution. Learning analytics designers have begun to take data protection compliance into account when developing learning analytics toolkits (Dyckhoff, Zielke, Bültmann, Chatti, & Schroeder, 2012). A certain level of data disclosure enhances the bonds of trust in groups and benefits the immune system (Ioinson & Paine, 2007). Online data protection does not necessarily eliminate the social presence in e-learning environments (Tu, 2002). Taking these perspectives into account, we would like to consider privacy issues as learning opportunities rather than threats. Preparing learners with essential literacy skills in data protection contributes to constructive data circulation.

We present various data protection pedagogies. In particular, learners are instructed not to expose themselves too much online and to be aware of safe practices in utilizing SNSs in less-regulated contexts outside of school. The active defense against data misuse is rarely addressed in the past research. The concepts of data protection, passive protection and active defense, should be integrated into school curricula as a foundation for information literacy in e-learning. We look forward to further elaboration on these pedagogies based on theories or instructional design models. Careful segmentation of the audience, by gender, experience or schooling level, lends support to identifying an individual's needs and facilitating learning effects.

Instructional design is an admittedly pragmatic domain, and thus the designers in the previous research seldom relied solely on a single theory or conducted an experiment to conclude the casual effect. Contexts and learning contents matter much as far as the learning effectiveness is concerned . We also expect visionary pedagogical methods to cultivate learners' sense of data protection in different contexts. For example, the incorporation of data protection into mobile learning and situated learning opens up avenues for further research. In addition, when the pedagogies on data protection mature, comparative research could examine which pedagogy is more suitable for a specific privacy issue.

Acknowledgements

This research was supported by the Ministry of Science and Technology of Taiwan [Project No. MOST 103-2511-S-009-009-MY2].

References

Anwar, M., & Greer, J. (2011). Role-and relationship-based identity management for privacy-enhanced E-learning. *International Journal of Artificial Intelligence in Education, 21*(3), 191–213.

ANZIL. (2016). *Australian and New Zealand information literacy framework*. Retrieved from. http://www.caul.edu.au/caul-programs/information-literacy/publications.
Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312. http://dx.doi.org/10.1016/j.chb.2014.05.046.
Archer, K., Wood, E., Nosko, A., De Pasquale, D., Molema, S., & Christofides, E. (2015). Disclosure and privacy settings on social networking Sites: Evaluating an instructional. *Standards and Standardization: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications, 287*. http://dx.doi.org/10.4018/ijcbpl.2014040101.
Association for College Research Libraries. (2016). *Information literacy competency standards for higher education*. Retrieved from http://www.ala.org/acrl/standards/informationliteracycompetency#stan.
Beycioglu, K. (2009). A cyberphilosophical issue in education: Unethical computer using behavior – The case of prospective teachers. *Computers & Education, 53*(2), 201–208. http://dx.doi.org/10.1016/j.compedu.2009.01.009.
Bower, M., & Sturman, D. (2015). What are the educational affordances of wearable technologies? *Computers & Education, 88*, 343–353. http://dx.doi.org/10.1016/j.compedu.2015.07.013.
Chang, C. L.-h. (2011). The effect of an information ethics course on the information ethics values of students – A chinese guanxi culture perspective. *Computers in Human Behavior, 27*(5), 2028–2038. http://dx.doi.org/10.1016/j.chb.2011.05.010.
Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358–368.
Chen, B., & Bryer, T. (2012). Investigating instructional strategies for using social media in formal and informal learning. *The International Review of Research in Open and Distributed Learning, 13*(1), 87–104.
Chou, H.-L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65*, 334–345. http://dx.doi.org/10.1016/j.chb.2016.08.034.
Dyckhoff, A. L., Zielke, D., Bültmann, M., Chatti, M. A., & Schroeder, U. (2012). Design and implementation of a learning analytics toolkit for teachers. *Journal of Educational Technology & Society, 15*(3), 58–76.
Edward, K. O. A. (2005). Debating definitions of information literacy: Enough is enough! *Library Review, 54*(6), 366–374. http://dx.doi.org/10.1108/00242530510605494.
European Commission. (2016). *Protection of personal data*. Retrieved from http://ec.europa.eu/justice/data-protection/.
Foulger, T. S., Ewbank, A. D., Kay, A., Popp, S. O., & Carter, H. L. (2009). Moral spaces in MySpace: Preservice teachers' perspectives about ethical issues in social networking. *Journal of Research on Technology in Education, 42*(1), 1–28.
Friedman, B. (1997). Social Judgments and technological innovation: Adolescents' understanding of property, privacy, and electronic information. *Computers in Human Behavior, 13*(3), 327–351. http://dx.doi.org/10.1016/S0747-5632(97)00013-7.
Haythornthwaite, C., & Andrews, R. (2011). *Sociotechnical Perspectives, E-learning theory and practice* (pp. 125–142). Sage Publications.
Ioinson, A. N., & Paine, C. B. (2007). *Self-disclosure, privacy and the Internet. The Oxford handbook of Internet psychology*, 2374252.
Johnston, B., & Webber, S. (2003). Information literacy in higher education: A review and case study. *Studies in Higher Education, 28*(3), 335.
Keller, J. M. (1987). Development and use of the ARCS model of instructional design. *Journal of instructional development, 10*(3), 2–10. http://dx.doi.org/10.1007/BF02905780.
Kennewell, S. (2001). Using affordances and constraints to evaluate the use of information and communications technology in teaching and learning. *Journal of Information Techology for Teacher Education, 10*(1–2), 101–116.
Kuzu, A. (2009). Problems Relatedto Computer Ethics: Originsofthe Problemsand Suggested Solutions. *Turkish Online Journal of Educational Technology, 8*(2), 91–110.
Lin, H. (2007). The ethics of instructional technology: Issues and coping strategies experienced by professional technologists in design and training situations in higher education. *Educational Technology Research and Development, 55*(5), 411–437. http://dx.doi.org/10.1007/s11423-006-9029-y.
Manero, B., Torrente, J., Serrano, Á., Martínez-Ortiz, I., & Fernández-Manjón, B. (2015). Can educational video games increase high school students' interest in theatre? *Computers & Education, 87*, 182–191. http://dx.doi.org/10.1016/j.compedu.2015.06.006.
McCloskey, H. J. (1980). Privacy and the right to privacy. *Philosophy, 55*(211), 17–38.
McClure, C. R. (1994). Network literacy: A role for libraries? *Information Technology and Libraries, 13*(2), 115.
McPherson, M., & Baptista Nunes, M. (2006). Organisational issues for e-learning: Critical success factors as identified by HE practitioners. *International Journal of Educational Management, 20*(7), 542–558. http://dx.doi.org/10.1108/09513540610704645.
Mike, S., & Roy, P. (2014). Mobile learning. In K. Sawyer (Ed.), *The Cambridge handbook of the learning sciences* (pp. 501–521). New York: Cambridge University Press.
Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366–2375. http://dx.doi.org/10.1016/j.chb.2012.07.008.
Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education, 59*(3), 1065–1078. http://dx.doi.org/10.1016/j.compedu.2012.04.016.
Nicholas, J. (2006). Teaching intellectual property rights as part of the information literacy syllabus. *Library Review, 55*(6), 330–336. http://dx.doi.org/10.1108/00242530610674730.
Noh, Y. (2014). Digital library user privacy: Changing librarian viewpoints through education. *Library Hi Tech, 32*(2), 300–317. http://dx.doi.org/10.1108/LHT-08-2013-0103.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy Paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. http://dx.doi.org/10.1111/j.1745-6606.2006.00070.x.
Nosko, A., Wood, E., Kenney, M., Archer, K., De Pasquale, D., Molema, S., et al. (2012). Examining priming and gender as a means to reduce risk in a social networking context: Can stories change disclosure and privacy setting use when personal profiles are constructed? *Computers in Human Behavior, 28*(6), 2067–2074. http://dx.doi.org/10.1016/j.chb.2012.06.010.
Patton, M. A., & Jøsang, A. (2004). Technologies for trust in electronic commerce. *Electronic Commerce Research, 4*(1–2), 9–21.
Plesch, C., Kaendler, C., Rummel, N., Wiedmann, M., & Spada, H. (2013). Identifying Areas of Tension in the field of technology-enhanced learning: Results of an international Delphi study. *Computers & Education, 65*, 92–105. http://dx.doi.org/10.1016/j.compedu.2013.01.018.
Rader, H. B. (1999). The learning environment-then, now and later: 30 years of teaching information skills. *Reference Services Review, 27*(3), 219–224.
Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). *Security in the online e-learning environment*. Paper presented at the Advanced Learning Technologies, 2005. ICALT 2005. Fifth IEEE International Conference.
Romney, V. W., & Romney, G. W. (2004). Neglect of information privacy instruction: A case of educational malpractice?. In *Paper presented at the Proceedings of the 5th conference on Information technology education*.
Schultz, C. (2012). Information security trends and issues in the Moodle e-learning Platform: An ethnographic content analysis. *Journal of Information Systems Education, 23*(4), 359–371.
Siu Cheung, K., Tak-Wai, C., Griffin, P., Ulrich, H., Ronghuai, H., Kinshuk, … Shengquan, Y. (2014). E-Learning in school education in the coming 10 Years for developing 21st century Skills: Critical research issues and policy implications. *Journal of Educational Technology & Society, 17*(1), 70–78.
Stavrositu, C., & Sundar, S. S. (2008). If Internet credibility is so iffy, why the heavy Use? The relationship between medium use and credibility. *CyberPsychology & Behavior, 11*(1), 65–68. http://dx.doi.org/10.1089/cpb.2007.9933.
Tavani, H. T. (2009). *Informational Privacy: Concepts, theories, and controversies the handbook of information and computer ethics* (pp. 131–164). John Wiley & Sons, Inc.
Terry, A. (2011). Neworks, Web 2.0, and the Connected learner. In R. A. Reiser, & J. V. Dempsey (Eds.), *Trends and issues in instructional design and technology*. Pearson Merrill Prentice Hall (pp. 308).

Tu, C.-H. (2002). The relationship between social presence and online privacy. *The Internet and Higher Education, 5*(4), 293–318.
Underwood, J., & Szabo, A. (2003). Academic offences and e-learning: Individual propensities in cheating. *British Journal of Educational Technology, 34*(4), 467–477. http://dx.doi.org/10.1111/1467-8535.00343.
Vanderhoven, E., Schellens, T., & Valcke, M. (2013). Exploring the usefulness of school education about risks on social network sites: A survey study. *Journal of Media Literacy Education, 5*(1), 2.
Vanderhoven, E., Schellen, T., & Valcke, M. (2014). Educating teens about the risks on social network sites. *An intervention study in Secondary Education, 22*(43), 123–131. http://dx.doi.org/10.3916/C43-2014-12.
Walton, J. M., White, J., & Ross, S. (2015). What's on YOUR Facebook profile? Evaluation of an educational intervention to promote appropriate use of privacy settings by medical students on social networking sites. *Medical Education Online, 20*.
Wang, S., & Smith, S. (2013). Reading and grammar learning through mobile phones. *Language Learning and Technology, 17*(3), 117–134.
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.
Wen, J. R., & Shih, W. L. (2008). Exploring the information literacy competence standards for elementary and high school teachers. *Computers & Education, 50*(3), 787–806. http://dx.doi.org/10.1016/j.compedu.2006.08.011.
Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431–453. http://dx.doi.org/10.1111/1540-4560.00072.
Wills, C. E., & Zeljkovic, M. (2011). A personalized approach to web privacy: Awareness, attitudes and actions. *Information Management & Computer Security, 19*(1), 53–73.
Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86–110. http://dx.doi.org/10.1207/s15506878jobem4901_6.