TECHNOLOGY TRANSIENCE AND LEARNER DATA
Shifting Notions of Privacy in Online Learning

Vanessa P. Dennen
Florida State University

The technologies that support online learning are continuously evolving, providing instructors and students with a continuous stream of new tools, features, and functionalities for existing tools. During an online course, instructors and students generate and share a tremendous amount of data using these tools. These data are often created in contexts where privacy concerns and safeguards are similarly evolving and uncertain. This article discusses online privacy concerns and emergent solutions in online learning contexts where technology transience is present. It focuses on issues such as legal rights, issues raised by emerging educational technologies, and manners by which institutions, instructors, and learners might mitigate both security risks and the level of personal discomfort that accompany these risks.

INTRODUCTION

Online instructors and students generate a tremendous amount of data as a byproduct of their learning activities. In a typical online class, members access online materials, upload and download files, and communicate with other class members. These activities leave behind a trail of digital data, of which only a portion is visible to the class participants. The visible data, such as typed words and uploaded documents, are consciously shared. The largely unseen data, such as digital records of each user's action on a web site, may be logged in a database without the user's knowledge or awareness.

Further complicating matters, online instructors and students operate in an ever-changing technological landscape. The tools that they use continuously evolve, resulting in a steady influx of new tools and features as well as new uses for familiar tools. Along with these tools and features often come new terms of service, as well as the possibility of new privacy and security risks. Keeping up with these changes and learning how to manage data privacy, online comfort and safety, and digital identities is now a necessary, though often

• **Vanessa P. Dennen**, Associate Professor of Instructional Systems and Learning Technologies, Florida State University. E-mail: vdennen@fsu.edu

The Quarterly Review of Distance Education, Volume 16(2), 2015, pp. 45–59 ISSN 1528-3518

overlooked, part of the online educational experience.

This article explores the tensions between technology adoption and privacy in online learning settings, with a specific focus on how institutions, instructors, and learners respond to operating in a dynamic environment. The first section provides an overview of issues related to privacy and technology transience in online learning contexts. The second section addresses privacy issues related to five currently emerging educational technology contexts: cloud computing; social media; mobile technology and bring your own device (BYOD) policies; learning analytics and big data; and data ownership and sharing. The last section presents some of the current and developing solutions for protecting privacy rights as well as ways to foster comfortable and safe technology-based learning environments.

EDUCATION, PRIVACY, AND USER COMFORT

In online learning settings, most students expect a certain degree of privacy. Typical class interactions are witnessed by a small number of people, all of whom are fellow members of the ongoing learning community. Students exchange their ideas and ask and answer questions, often not thinking about the how their words and actions are being digitally archived, and how this data could be later used or shared in another context—including a context outside the course. Some class-related interactions, such as discussions of grades and personal issues that affect class performance, ostensibly occur in private conversations. Everyone in a class likely has a different comfort level with the idea that their data may be archived and shared, but many students likely do not think much about privacy concerns unless directly confronted with an instance—whether personal or vicarious—in which a student experiences discomfort or harm due to data sharing.

Privacy issues can be conceptualized in terms of a continuum, with "public" residing at one end of the continuum, and "private" at the other (Elm, 2009). Most learners may easily understand the ends of this continuum, but the intermediate points may be less clear. For example, a blog with no privacy restrictions would be considered "public," but e-mail would be considered "private"—with the caveat that the sender or receiver could easily forward the e-mail, or blind carbon copy an additional party, violating that presumption of privacy. Semipublic online spaces are those that may be restricted in some way, but that anyone could potentially access. For example, listserv messages are only sent to subscribers; but, in many instances, anyone is free to become a subscriber to the listserv. In contrast, semiprivate online spaces may only be accessed by a defined membership. These spaces are not considered fully private, however, because communications within these spaces remain open to all members.

Using this classification system, most interactions in online classes taught via a learning management system (LMS) fall within the "semiprivate" portion of the privacy continuum. Certain tools, such as e-mail, messaging systems, and grade books, tend to foster private interactions, with access theoretically restricted to individuals who are involved in a particular transaction. Technical support staff are largely unseen and unnoticed within these settings, although they typically are present at some level and can access layers of data that instructors and students never see. For example, technical support personnel can access the log files in which records of all user activity (e.g., mouse clicks) are stored. However, these data typically are used in aggregate form to identify trends in system use, or to troubleshoot system problems. Technical support staff are unlikely to access and examine these data at the individual user level without an explicit administrative request to do so.

User comfort is related to privacy, but is best understood as a distinct issue. Privacy has to do with how personal data are classified and

whether or not they may be shared with others under a variety of circumstances. Privacy can be regulated legally, and personal data access—which is one component of privacy—can be controlled via software. In contrast, comfort reflects whether an individual finds the current situation acceptable. Comfort cannot be regulated legally or controlled by software, and comfort levels reflect personal perception of a situation.

Although instructors and institutions are not legally responsible for ensuring student comfort when online learning technologies are used, comfort is nonetheless an important consideration. When users are uncomfortable in an online setting, they may struggle to focus on the task at hand. When the task is communicating with others, such as during a class discussion, users who experience discomfort may feel tense, nervous, or afraid to share (Ledbetter, 2009). Thus, a learner's perception that privacy is at risk or uncertain in online environments can be counterproductive to learning.

Individual technology users may try to further control their online privacy by choosing levels and manners of interaction and self-disclosure that are within their own comfort zones. Markham (2012, p. 336) notes that "individual and cultural definitions and expectations of privacy are ambiguous, contested, and changing. People may operate in public spaces but maintain strong expectations of privacy." In this sense, desired levels of privacy can be subjective in nature, and a person's actions and privacy wishes may seem contradictory. Individuals may interact online in ways that make them feel uneasy because the perceived benefits outweigh the risks. Additionally, since people's perceptions of what information is private and too personal to discussion online varies widely, individuals may find themselves following the self-disclosure norms and examples set by others despite their personal discomfort. The challenge facing educators, then, is to ensure that student privacy is both secured and addressed in a manner that helps students feel comfortable participating in the learning experience.

Students are concerned about their privacy when using online technologies. For example, in one study of blog-based portfolios, some students did not want to participate in the learning activity because of privacy concerns (Tang & Lam, 2014). Specifically, these students did not want to share information about their interactions with and impressions of other people in a setting that, to them, did not feel sufficiently secure. Students in another study experienced discomfort sharing their personal beliefs, even within a semiprivate learning environment (Zdravkova, Ivanovic, & Putnik, 2013). In a survey study of students using the Moodle LMS, participants indicated that they wanted their personal information (e.g., e-mail and ID numbers) and their activity logs to remain private (Ivanović et al., 2013). In another study, students shared concerns about protecting their privacy and limiting the information that was shared with classmates, instructors, and the rest of the world (Dennen & Burner, 2013). Students in Dennen and Burner's (2013) study also expressed varying levels of comfort with different learning technologies and activities due to their privacy concerns. Essentially, within any given class, instructors may expect students who represent a wide range of privacy preferences and comfort levels when interacting in an online course.

DIGITAL FOOTPRINTS AND PRIVACY CONTROLS AND RIGHTS

A "digital footprint" is the collection of information about a person that exists online. Digital footprints, like physical ones, are unique to their owners. Essentially, a digital footprint is a holistic online identity, comprised of data shared by the individual, data collected based on the individual's online actions, and data collected and shared about the individual by third parties. Examples of this third type of data include public records (e.g., property

ownership, lawsuits, etc.), news reports, and items shared by family and friends.

Individuals may take action to exert control over some components of their digital footprints. For example, they may elect to use or not use particular tools, and within certain tools they may have the ability to adjust settings and indicate to whom their information might be displayed. In many instances, it up to the individual to determine his/her own privacy needs and to ensure that these needs are met (Garg, Patil, Kapadia, & Camp, 2013). For example, they may elect to opt-in or opt-out of allowing their data to be collected (Tene & Polonetsky, 2012), or they may engage in self-censoring practices, adjusting what they share because of audience concerns (Dennen, 2009). Education and personal diligence come into play here. One study of user e-mail practices found that individuals can, through their information-sharing behaviors, limit their privacy and security risks (Solic, Nenadic, & Galic, 2012). However not all users know how to control these risks, and the risks themselves are continuously changing. Not using a tool may seem like the most prudent approach to protecting privacy, but it can have its own negative consequences, such as limiting an individual's ability to fully engage in a community or a practice. Further, because of third party data sharing, even individuals who choose not to create an online presence are likely to find that they have a digital footprint.

Legal Privacy Rights

Citizens of different countries may be bound by national policies and experience specific legal rights related to online privacy. These rights are the focus of various legal scholars and consumer interest groups who seek to track and influence the ways in which technology is used by individuals, institutions, governments, and corporations. Tensions exist between the missions and best interests of each of these constituents, and educational settings are not immune to these conundrums.

In the United States, there are online privacy rights and protections that focus specifically on school contexts and children. Students of all ages have rights granted by the Family Educational Rights and Privacy Act (FERPA), passed in 1974. FERPA regulates the privacy of student personal information such as address and grades, restricting access to the student, his or her guardian (if under 18) or designee (if over 18), and relevant institutional personnel. Note, however, that deidentified, aggregate data are not covered by FERPA and may be shared with third parties. Additional protections are offered to children under the age of 13 through the Children's Online Privacy Protection Act (COPPA). This act, established in 1998, legislates the ability to collect online data from children. Both of these acts predate many of the digital tools currently deployed in educational settings, and were not designed to regulate their use. Institutions and educators may find it challenging to determine how to interpret and apply these laws in a technology context (Krueger, 2014).

In the European Union, privacy-oriented legislation focuses on the whole population, and citizens have the "right to be forgotten" on the Internet (Newman, 2015). Rosen (2012) explores the three ways in which this right my be exerted: (a) by deleting something one has posted; (b) by deleting something one originally posted that has subsequently been copied or shared by someone else; and (c) by deleting something about oneself that has been posted by someone else. This third category is the most controversial, but citizens of the European Union and other nations following this model have been successful at pressuring online companies to remove this kind of personal information from web sites and search engines, even when it contains factual information (e.g., information about past activities or legal issues).

Through the combination of user controls—whether technology-based or individual choices regarding personal self-disclosure—and the protection and rights offered via legal channels, some privacy concerns can and have

been addressed. Others remain out of individual control, and are further complicated by the Internet's lack of national boundaries and lack of clear, consistent regulation or legislation within and between countries. Regulation or legislation also may not be desirable in all situations, because it can limit good outcomes as well as negative ones, and the value of particular outcomes can be a matter of subjective judgment (Tene & Polonetsky, 2012).

TECHNOLOGY TRANSIENCE

An examination of even the recent past reveals numerous situations in which individuals failed to anticipate the ways that new technologies would affect their lives. Shirky (2008) recounts many tales of how Internet and mobile technologies were used in unanticipated ways by both individuals and networks (tracking down or publicly shaming criminals or amassing support for people in need). One of the major points that Shirky makes is that changes in technology can lead to changes in human behavior, both for the better and for the worse.

It is difficult to plan for technology transience and the changes in human behavior that come with it because no one is certain which technologies will become widely adopted and which will quickly disappear. Martin et al. (2011) examined technology trend forecasts and found that the accuracy of their predictions about the impact of future technologies on education was decidedly uneven. However, when reviewing the collected predictions over time it became clear that some predictions failed because certain technologies were either replaced or subsumed by other technologies with similar promises or features (e.g., *ubiquitous computing* was a forecast trend that preceded *mobile computing*; mobile computing, in the end, was the trend that materialized).

Technology transience in an educational context is not just about new technologies. Veletsianos (2010) discusses "emerging" technologies in education, pointing out that *new* and *emerging* are terms that are often conflated but do not mean the same thing. Emerging technologies, as Veletsianos defines them, are those whose use is still evolving, with as-of-yet unfulfilled potential and on which research and practices are still maturing. Technology adoption and trends in the general population are not always aligned with technology integration in education settings (Kukulska-Hulme, 2012), and a technology may be in a state of discovery or flux in an educational context for a decade or longer. Instructors and students have two interrelated needs in this area: one, to develop their technology knowledge, and two, to learn how to deal with privacy issues in a transient or emergent technology environment. Essentially, instructors and students need to learn both how to operate and integrate new and emerging technologies in the classroom, and also how to anticipate and address the limitations and concerns that will arise from the use of such technology.

Technology Transience and Knowledge

Because technology underpins so much of online learning, online instructors and learners need to have a basic degree of technological competence. At minimum, online instructors and learners need to know how to use the course technology (e.g., to navigate course web sites, and to interact with one another via communication tools). However, there is a range of other kinds of knowledge related to interaction in a technology-rich learning setting. For example, the TPACK Framework (Mishra & Koehler, 2006) represents the kinds of knowledge that are required for teaching in technology-enhanced environments. The three main parts of the TPACK framework are technology, pedagogy, and content. Teachers not only need to have knowledge in each of these three areas, but also in the areas where they intersect (e.g., technological content knowledge and technological pedagogical knowledge).

Of these three main categories of teacher knowledge, technology knowledge represents the most dynamic component of online learning. Technology knowledge extends beyond just knowing where to click on a screen or what buttons to push on a keyboard. It also includes such topics as the advantages and disadvantages of technology use. Technological pedagogical knowledge focuses on how technology use changes teaching and learning, and technological content knowledge focuses on how technology is used in particular content areas. The greater point to keep in mind is that as educational technology and its use changes, so does the need for change in teacher knowledge, as well.

Technology Transience and Privacy

Technology transience magnifies the privacy concerns related to technology use in educational contexts. When emerging technologies, such as Web 2.0 tools, are adopted for instructional purposes, it is important to consider how various elements in the learning ecosystem, including privacy and ethics, are altered (Greenhow, Robelia, & Hughes, 2009). Although the TPACK Framework does not explicitly address knowledge of technology-related privacy issues and solutions, a broad interpretation of both technology knowledge and technological pedagogical knowledge might incorporate this content.

Technology transience is typically thought of as a forward-moving phenomenon. In other words, with each new development the focus is on determining what can or should be done next, not reviewing and revising what has been done previously. However, two temporal privacy-related challenges exist. First, online tools typically require users to manage their privacy settings in a control panel, and then apply those settings moving forward. However, a user's ability to determine desired settings in this a priori manner, without any broader sense of how the tool will function in a particular setting, may be limited (Garg et al., 2013). Second, where privacy is concerned it is often necessary to look backward as well as forward, particularly when an individual has used a particular tool in the past in one context and is now is being asked to use the tool in the future in a new context. For these reasons, technology transience is an issue that requires consideration of past actions as well as future ones.

PRIVACY, TRANSIENCE, AND EDUCATIONAL TECHNOLOGIES

The impact of new and changing technologies on education settings varies by tool, particularly where privacy is concerned. Some of the issues related to privacy include who hosts and controls the software and data storage, who owns and supplies the devices, and how readily available and user-friendly privacy options are for end-users. This section discusses five educational technology areas that represent current trends, focusing on the privacy-related issues that have been raised in each area: cloud computing, social media, mobile technology and BYOD policies, learning analytics and big data, and data ownership and sharing.

In most cases, there are no definitive privacy solutions currently available; instead, the state of these emerging educational technologies remains in flux, as both new privacy solutions and the technologies themselves continue to develop. In this sense, each area represents an example of current technology transience issues.

Cloud Computing

Cloud computing is a technology consisting of a network of shared computers to store data, run servers, and host applications via the Internet. End users connect to service providers to accomplish computing tasks rather than relying solely on their local computer for these operations. Cloud computing services are widely used in educational settings, supporting both administrative and learning tasks (e.g., accounting services, benefits, library services,

and file sharing during a class project). Many institutions find cloud computing attractive for financial reasons, allowing some technology services to be outsourced (Ercan, 2010; Sultan, 2010). However, a consequence of outsourcing is loss of institutional control, and the individuals whose data are being stored and shared may be unaware that third-party agents are handling their private information (Krueger, 2014).

Instructors find third-party cloud computing services appealing because they offer access to technologies not currently supported by their institutions. In a class setting, cloud computing allows for easy distribution and sharing of files as well as collaborative work. However, although these services are often labeled "free," they actually do come at a cost. Currency may not directly exchange hands, but the transaction may effectively monetize user information; users get to use online tools in exchange for permitting the tool providers to use the data that they generate. Many free computing services and social media tools retain the rights to collect user data and make use of user files. For example, Google (2014) requires that users grant the company the ability to engage in a variety of activities with user content so long as the ultimate purpose is to develop and improve their services. Other tools, such as Facebook, have drawn upon user-uploaded content to support targeted advertising, a move which has led users to have increased privacy concerns (Tucker, 2014).

Cloud computing introduces a number of other privacy and security issues, such as phishing, identity theft, and problems related to shared access of a virtual machine (Modi, Patel, Borisaniya, Patel, & Rajarajan, 2012). Most prominent cloud computing systems have a security protocol in place to help prevent or lessen the likelihood of many of these issues, but cloud computing has required new considerations for security incident handling (Ab Rahman & Choo, 2015). Other, end-user security issues can arise as well (e.g., managing distinct private and shared folders, ensuring that shared folders are secure, and limiting administrative access to particular users). Recent studies suggest that student perceptions of the security and privacy of cloud computing tools affects their desire to use such tools (Arpaci, Kilicer, & Bardakci, 2015), and that a variety of issues need to be worked out in technical, legal, and training domains to make cloud computing a secure option for sensitive educational data (González-Martínez, Bote-Lorenzo, Gómez-Sánchez, & Cano-Parra, 2015).

Social Media

Social media tools are widely used in everyday life, and also have been integrated into learning contexts. Social media tools have made it easy for individuals to share information online in a variety of formats (e.g., written text, images, and videos). Many people have embraced the ability to share their snapshots of their life experiences and thoughts in this manner, but this sharing has come at a cost to user privacy. Rosen succinctly summarizes the problem: "It is very hard to escape your past on the Internet now that every photo, status update, and tweet lives on forever in the cloud" (2012, p. 88).

Determining social media privacy settings can be difficult for many users. This skill requires the ability to translate a personal preference or need into a specification offered by an interface (Garg et al., 2013). Many social media users have a poor understanding of privacy settings and have been unable to successfully set their privacy controls as intended (Hargittai, 2010; Madden, 2012; Madejski, Johnson, & Bellovin, 2012). Further, tools such as Facebook periodically change their terms of service and privacy settings, adding to user difficulties.

Facebook provides an excellent case for exploring privacy concerns. Facebook, a social network that was not originally intended as a pedagogical tool, has nonetheless been used to support both formal and informal learning interactions. Arguments have been made for

using Facebook to support learning because of the large number of students already using the system (Barczyk & Duncan, 2013), although that same factor also could conceivably be argued as a reason to *not* employ the system for pedagogical purposes. When asked in one study, learners were split about their interest in using Facebook with their learning networks; they were more comfortable connecting to instructors and classmates via the Groups feature than as friends, and about 10% were not and did not want to become Facebook users (Dennen & Burner, 2014). These individuals usually possess reasonably strong reasons for avoiding Facebook (Rymarczuk & Derksen, 2014).

Typical Facebook users create profiles and adjust privacy settings in a manner that meets the needs of their personal lives. These users may have privacy concerns, but those concerns are often tempered by the social costs of not having and maintaining a Facebook account (Raynes-Goldie, 2010). Asking students to use Facebook to interact with learning networks can cause some students discomfort by creating additional privacy concerns, or changing their natural activities through self-censoring or readjusting privacy settings. When nonusers are asked to join Facebook, they are being asked to expand their digital footprint. Facebook's terms of service specifies that it is a real name service and indicates that unless users take steps to adjust their privacy controls Facebook retains the rights to engage in a variety of activities with user-shared information and files (Facebook, 2015), and so student privacy concerns in this matter are not trivial. Additionally, Facebook's terms of service are complex and frequently updated, leading some users to not read them (Rymarczuk & Derksen, 2014).

These issues are not limited to students and are not limited to Facebook. In the K–12 realm, teachers have suffered negative consequences for legal personal activities (e.g., drinking alcohol) shared via private Facebook posts (Akiti, 2012). These issues have occurred even when teachers are neither networked with students nor using the tool for educational purposes. Even when teachers strive for privacy and for separation of personal and professional lives, their social networks could have only one or two degrees of separation from the social networks of students, parents, and administrators.

Students asked to use other popular personal social media tools such as Pinterest, Instagram, or Twitter in a learning context might find themselves facing a similar dilemma: they must decide how they feel about merging contexts. Essentially, students have two options. They can choose simplicity and use the same account, knowing that contacts and content from both parts of their life may now be connected, or they can create an account just for school purposes and shift between accounts and contexts. Either situation may add both stress and privacy concerns for learners.

In addition to managing one's networks and sharing in real time, digital footprints also are a privacy concern when social media are used. Learners who use social media accounts in their online classes may wish to remove class-related components of their digital footprints after their class ends (Dennen & Burner, 2013). However, these items may not disappear from the Internet even when the person who created it deletes the original version. For example, if a digital item is shared or archived online by others, online copies will continue to exist in other locations even after the original is deleted. Additionally, cached copies may exist on search engines like Google or in the Wayback Machine. In the case of Twitter, all public tweets are being archived by the Library of Congress. Thus, intentionally shared items may continue to exist even when individuals attempt to remove them.

Unintentionally shared information may also make learners and educators feel uncomfortable or put their privacy at risk. For example, many social media tools share location data when users post a message, and shared photographs also may contain location metadata embedded within the digital image file.

There are ways to avoid sharing these metadata, as well as ways to prevent the metadata from being recorded, but both require extra knowledge and effort on the part of end users. A prominent example of this phenomenon is "Toronto Jane," a Canadian woman whose tweets caught public attention and whose path was then followed as she traveled to Syria and Iraq and tweeted her way across the countries. Toronto Jane neglected to turn off the locater function on her mobile phone and transmitted geo-tagged data with every tweet (Bell, 2015). Although educational uses of Twitter and other social media tools are unlikely to attract media and political attention, students and instructors may be unwittingly sharing private information about where they live, work, and recreate when all they intend to do is complete course requirements.

Mobile Technology and BYOD Policies

Many educational institutions have embraced mobile technology, allowing both learners and employees to access institution-related resources via mobile web sites and applications. In many instances, the mobile access simply provides an alternate to using a computer; the same content is available, and the same user accounts and security protocols are used. Still, in Kukulska-Hulme's (2012) study at least one faculty participant noted that adopting mobile technology for teaching and learning could raise some privacy and ethical concerns. A readily apparent concern is the ease with which mobile technologies allow data capture and sharing. In physical classrooms, photographs or videos taken with mobile phones may violate fellow classmates' privacy. In online learning settings, covert photography and recording of instructors and classmates may be less of an issue, but concerns related to data security, device loss, and the merging of personal and educational data remain.

Device ownership—and in particular the bring-your-own-device (BYOD) movement—is a mobile technology-related issue affecting many educational institutions. As personal ownership of laptops, tablets, and smartphones rises, so does the use of these personal devices to support learning. Further, in most online learning contexts, the default expectation would be that learners are not using institution-owned devices but rather connecting to the course from personal, employer, or public (e.g., library-owned) devices, whether mobile or not.

When students are concerned, the major BYOD issues relate to providing technical support for a wide array of technology configurations. Students typically are expected to protect the security of their own institutional accounts (e.g., e-mail, course access) while having limited access to anyone else's information. When employees use personal devices, security and privacy concerns move to the forefront. Employees may wish to work from home, use their own computer at work, or simplify their lives by streamlining the number of devices they must carry. Some employees, such as adjunct instructors, may not be provided with an institution-owned personal computer, and thus must choose between using an institutional computer lab or using their own devices. Some instructors have class records stored on their home computers, and use personal mobile phones to access institution-related electronic mail. Given these conditions, the potential for private institutional or student data to be stored on a personal device that is lost, stolen, or otherwise in the possession of someone who does not work for the institution is great. [Two recent laptop thefts demonstrate the gravity of this issue. In one instance, a laptop containing the health records of 2,000 students was stolen out of a school nurse's car (Shapiro, 2013). In the other instance, a laptop stolen from a physician's car contained the personal information of 8,294 individuals (Fernandez, 2013).]

BYOD privacy concerns may work in the opposite direction, too. Most people have personal information stored on their personally owned devices. Using those devices for school and work purposes mixes data from both con-

texts on the same device, reducing the separation of the owner's personal and school or work life (Miller, Voas, & Hurlburt, 2012). When individual devices are used for multiple purposes, personal information may be inadvertently shared. For example, phone calls made from a personal phone may provide the recipient of the call with a personal phone number, and e-mail messages may be accidentally sent from personal accounts.

Although mobile devices are popular given their ability to connect individuals any time and any place, and BYOD practices may both be practical and save institutions money, BYOD policies may need to exclude employees who work extensively with sensitive or private data. Additionally, for some employees who either use employer-owned or personal mobile devices, it may be necessary to provide privacy and security training, develop acceptable use policies, and install software that will both secure and, if needed, allow for remote data backup and removal (French, Guo, & Shim, 2014).

Learning Analytics and Big Data

Learning analytics is the collection and subsequent use of learner data for the purpose of better understanding and supporting learning behaviors. Learning analytics may be focused on the micro level, looking at individual or class performance, or may involve large data sets aggregated across many learners and settings. In the context of learning analytics, big data refers to the macro level and an educational data set so large that it cannot be housed or processed by a single computer, instead requiring different methods to analyze it (Grossman & Siegel, 2014). Whereas local learning analytics are focused on specific individuals, big data learning analytics can be used to identify learner performance trends. In the big data context, individuals are neither identified nor important.

The field of learning analytics has gained much attention in the last 5 years because researchers, policy makers, and educators recognize the potential to assess and improve education based on the analysis of passively collected learner data. Learning analytics can be used both to support student performance and to identify areas in which a course might be improved (Dietz-Uhler & Hurn, 2013). However, when analytics are used covertly in an academic context, learners sometimes feel that their sense of privacy has been violated (Baepler & Murdoch, 2010). Although a particularly astute instructor might use observation and reflection to offer the same feedback or suggest the same changes to a course, the use of learning analytics for the same purpose changes the privacy context for some learners, especially when recommendations are based on data that are collected and analyzed without their prior knowledge or consent.

Public concern about privacy and the use of digitally collected learning data has perhaps been most documented in the K–12 realm. A company called inBloom contracted with several districts and departments of education in the United States to collect deidentified student learning data, which could then be used by companies developing learning products; however, parent outcry about privacy rights and commercialization led to the loss of contracts and eventually the company's closure (MacCarthy, 2014). Still, the societal benefits of collecting and using big data can outweigh the risks to individuals, who may not be in a good position to make an informed decision about those risks if asked to provide consent (Tene & Polonetsky, 2012).

Data Ownership and Sharing

To whom do our data belong? This question—which spans across tools, devices and platforms—initially appears to be a very simple one, but the issues surrounding data ownership are complex. In the United States, copyright laws protect an individual's intellectual property (e.g., words and images) in a variety of formats, but that protection only applies to ensuring attribution, and not privacy. Additionally, every user of an online

system generates data that are not protected by intellectual property laws.

When third-party tools are used, rights to user-generated and shared data may be addressed in the terms of service. Many online tools reserve the right to access and make use of data stored by users on their systems. Although the service provider's intent may be benign, digital privacy advocates have raised concerns over the broad-reaching data rights that individual citizens give to companies such as Facebook, Instagram, Google, and Dropbox in exchange for "free" use of their technology services.

Learning analytic data generated within an LMS also may be affected by data ownership and access issues (Dietz-Uhler & Hurn, 2013). These data are valuable to third parties, but at question is whether a school owns those student-generated data and has the rights to sell or share them. Vendor contracts may lack sufficient clauses to safeguard student privacy at the legally required level. Also, many parents and students object to businesses profiting from what they perceive to be private learning data (Polonetsky & Tene, 2014), even when those data are shared in aggregate form and with identifiers removed as is required by FERPA.

Determining the sharing rights for digital data at the individual level can be challenging, as well. One case to consider is a group photograph, with constituents including the photographer, camera owner and subjects potentially vying for the rights to share the image (Garg et al., 2013). Shifting the topic to an educational context, collaborative work products can cause similar confusion. What should be done when one student wants to share a group project in an online setting, giving proper attribution to his or her collaborators, but the collaborators do not wish to have their work product shared in a public forum?

PRIVACY SOLUTIONS

In all five of these emerging educational technology areas (i.e., cloud computing, social media, mobile/BYOD policies, data analytics/big data, and data ownership/sharing), there are more unsettled or ongoing issues than proposed solutions, and many of the solutions are imperfect. This situation reflects the nature of interacting and working in a dynamic, evolving area: individuals must have some degree of tolerance for trade-offs and errors, recognizing that domain-related technology knowledge (including technological pedagogical and technological content knowledge) is still being refined. Still, there are certain general solutions that can be proposed and used, with constant assessment and revision, to help secure privacy and avoid learner discomfort in online learning settings, even when new or emergent technologies are present, and technology transience is a concern.

Setting Norms and Expectations

In a community setting, such as an online course, upholding privacy rights is as much the responsibility of the group as it is the responsibility of individuals. Over time, groups typically develop norms for maintaining privacy expectations and will encourage members to maintain their privacy at the agreed-upon level (Dennen, 2014; Garg et al., 2013). Within a class, there typically is insufficient time for such norms to emerge. However, instructors can determine the norms in advance and share them with students in the form of guidelines and expectations, as well as modeling them through their own practices. Students look to instructors to provide this kind of leadership and they experience less apprehension about interacting online when it is provided (Ledbetter & Finn, 2013).

Guidelines for online learning privacy and expectations can cover a wide range of issues. They provide an opportunity to not only regulate student behavior but also to educate students about their privacy rights and options. Students can be taught options for managing their privacy settings and information sharing when using whatever tools the class has adopted. Students should be encouraged to

read all terms of service for any online tool for which they sign up, and urged to respect and uphold the privacy of classmates.

Digital Identity and Footprint Management

When learners interact on the Internet for class purposes, instructors have an opportunity to educate them about both how to manage their digital identity and footprint. Students and instructors alike may feel uncomfortable opening up elements of their private lives to observation by others in an educational context, and developing different types of connections or relationships. When students use preexisting accounts, the shift to a new context (e.g., from personal or work to school) may require them to change behavior and alter their preexisting identity on that social network (Krueger, 2014). Instructors can help students determine if they wish to merge contexts under one identify, or construct a new account and identity for use in the class.

Digital footprint management involves controlling four factors: what information is being shared, with whom those data are being shared, whether those data are being indexed and archived, and the longevity of those data. The first two factors concern self-disclosure and privacy settings. With respect to the last two factors, learners can be taught techniques for preventing data indexing and archiving, and reminded at the end of the course that they may remove their data and close their accounts once final grading is complete.

Institutional Guidance

Institutions can create policies to guide their constituents through the use of technology, but creating policy for an ever-changing technological landscape can be quite challenging. Additionally, presence of policies does not necessarily ensure that the policies are always followed and upheld. For example, FERPA is mentioned in many universities' social media policies (Erskine, Fustos, McDaniel, & Watkins, 2014), but one study showed that university faculty tend to have low or no awareness of FERPA, and mostly through self-initiated ways, such as choosing to read a handbook (Gilley & Gilley, 2006). Some of the recommendations for institutional guidance in this area include assigning a person to be responsible for compliance efforts, training all faculty and staff who handle data on a regular basis, and creating institutional norms and practices for privacy and security (Krueger, 2014). Institutions need to view their role in privacy guidance and education as a continuous task, and one in which they are both proactive about identifying potential concerns and reactive to problem situations. This continuous focus is particularly important given the highly transient nature of educational and administrative technology.

CONCLUSION

Technology transience, especially when combined with the desire to be innovative and engaging, can make it difficult to safeguard individual privacy. The responsibility for safeguarding that privacy in online learning occurs at three levels. First, institutions should provide leadership and education for both instructors and students, upholding privacy as both a right and a priority. Second, instructors should purposefully consider privacy issues along with technology, pedagogy, and content when planning class activities, and seize the opportunity to not only teach students about the course content, but also about how to manage their online identity and digital footprint. And third, students should be included in the conversation about privacy in online learning contexts. They should express their concerns, and help institutions and instructors as they develop policies to guide the instructional use of new and emerging technologies and seek secure methods for using new and emerging technologies in support of learning activities.

REFERENCES

Ab Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security, 49*, 45-69. doi:10.1016/j.cose.2014.11.006

Akiti, L. (2012). Facebook off limits? Protecting teachers' private speech on social networking sites. *Valparaiso University Law Review, 47*(1), 119–167.

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior, 45*, 93–98. doi:10.1016/j.chb.2014.11.075

Baepler, P., & Murdoch, C. J. (2010). Academic analytics and data mining in higher education. *International Journal for the Scholarship of Teaching and Learning, 4*(2).

Barczyk, C. C., & Duncan, D. G. (2013). Facebook in higher education courses: An analysis of students' attitudes, community of practice, and classroom community. *International Business and Management, 6*(1), 1–11. doi:10.3968/j.ibm.1923842820130601.1165

Bell, S. (2015, January 30). ISIS sympathizer's road to jihad—from Canada to Syria to Iraq—Racked one tweet at a time. *National Post*. Retrieved from http://news.nationalpost.com/2015/01/30/isis-sympathizers-road-to-jihad-from-canada-to-syria-to-iraq-tracked-one-tweet-at-a-time/

Dennen, V. P. (2009). Constructing academic alter-egos: Identity issues in a blog-based community. *Identity in the Information Society, 2*(1), 23–38. doi:10.1007/s12394-009-0020-8

Dennen, V. P. (2014). Becoming a blogger: Trajectories, norms, and activities in a community of practice. *Computers in Human Behavior, 36*, 350–358. doi:http://dx.doi.org/10.1016/j.chb.2014.03.028

Dennen, V. P., & Burner, K. J. (2013). *Boundaries, privacy, and social media use in higher education: What do students think, want, and do?* Paper presented at the Internet Research 14.0, Denver, CO.

Dennen, V. P., & Burner, K. J. (2014). *Facebook, "friends," and the higher education classroom: Student preferences and attitudes*. Paper presented at the Internet Research 15.0, Daegu, South Korea.

Dietz-Uhler, B., & Hurn, J. E. (2013). Using learning analytics to predict (and improve) student success: A faculty perspective. *Journal of Interactive Online Learning, 12*(1), 17-26.

Elm, M. S. (2009). How do various notions of privacy influence decisions in qualitative Internet research? In A. N. Markham & N. K. Baym (Eds.), *Internet inquiry: Conversations about method* (pp. 69–87). Los Angeles, CA: SAGE.

Ercan, T. (2010). Effective use of cloud computing in educational institutions. *Procedia - Social and Behavioral Sciences, 2*(2), 938–942. doi:10.1016/j.sbspro.2010.03.130

Erskine, M. A., Fustos, M., McDaniel, A., & Watkins, D. R. (2014). *Social media in higher education: Exploring content guidelines and policy using a grounded theory approach*. Paper presented at the Twentieth Americas Conference on Information Systems, Savannah, GA.

Facebook. (2015). Facebook Terms of Service. Retrieved January 30, 2015, from https://www.facebook.com/legal/terms

Fernandez, E. (2013, November 21). Laptop computer theft at UCSF. *University of California San Francisco News*. Retrieved from http://www.ucsf.edu/news/2013/11/110386/laptop-computer-theft-ucsf

French, A. M., Guo, C., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems, 35*, 191–197.

Garg, V., Patil, S., Kapadia, A., & Camp, L. J. (2013). Peer-produced privacy protection. *2013 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 147–154).

Gilley, A., & Gilley, J. W. (2006). FERPA: What do faculty know? What can universities do? *College and University Journal, 82*(1), 17–26.

González-Martínez, J. A., Bote-Lorenzo, M. L., Gómez-Sánchez, E., & Cano-Parra, R. (2015). Cloud computing and education: A state-of-the-art survey. *Computers & Education, 80*, 132–151. doi:10.1016/j.compedu.2014.08.017

Google. (2014). Google Terms of Service. Retrieved April 14, 2014, from http://www.google.com/intl/en/policies/terms/

Greenhow, C., Robelia, B., & Hughes, J. E. (2009). Learning, teaching, and scholarship in a digital age: Web 2.0 and classroom research: What path should we take now? *Educational Researcher, 38*(4). doi:10.3102/0013189X09336671

Grossman, R. L., & Siegel, K. P. (2014). Organizational models for big data and analytics. *Journal of Organization Design, 3*(1), 20–25. doi:10.7146/jod.3.1.9799

Hargittai, E. (2010). Digital na(t)ives? Variation in Internet skills and uses among members of the "Net Generation." *Sociological Inquiry, 80*(1), 92–113. doi:10.1111/j.1475-682X.2009.00317.x

Ivanović [illegible] Hölbl, M., & Schweighofer, T. (2013). Usability and privacy aspects of Moodle: Students' and teachers' perspective. *Informatica, 37*, 221–230.

Krueger, K. R. (2014). 10 steps that protect the privacy of student data. *T.H.E. Journal, 41*(6), 8.

Kukulska-Hulme, A. (2012). How should the higher education workforce adapt to advancements in technology for teaching and learning? *The Internet and Higher Education, 15*(4), 247–254. doi:10.1016/j.iheduc.2011.12.002

Ledbetter, A. M. (2009). Measuring online communication attitude: Instrument development and validation. *Communication Monographs, 76*(4), 463–486. doi:10.1080/03637750903300262

Ledbetter, A. M., & Finn, A. N. (2013). Teacher technology policies and online communication apprehension as predictors of learner empowerment. *Communication Education, 62*(3), 301–317. doi:10.1080/03634523.2013.794386

MacCarthy, M. (2014). Student privacy: Harm and context. *International Review of Information Ethics, 21*, 11–24.

Madden, M. (2012). Privacy management on social media sites. Washington, DC: Pew Research Center's Internet & American Life Project.

Madejski, M., Johnson, M., & Bellovin, S. M. (2012). *A study of privacy setting errors in online social network*. Paper presented at the Fourth International Workshop on SECurity and SOCial Networking, Lugano, Switzerland.

Markham, A. (2012). Fabrication as ethical practice. *Information, Communication & Society, 15*(3), 334–353. doi:10.1080/1369118x.2011.641993

Martin, S., Diaz, G., Sancristobal, E., Gil, R., Castro, M., & Peire, J. (2011). New technology trends in education: Seven years of forecasts and convergence. *Computers & Education, 57*(3), 1893–1906. doi:10.1016/j.compedu.2011.04.003

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012, September/October). BYOD: Security and privacy considerations. *IT Pro,* 53–55.

Mishra, P., & Koehler, M. J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. *Teachers College Record, 108*(6), 1017–1054. doi:10.1111/j.1467-9620.2006.00684.x

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2012). A survey on security issues and solutions at different layers of cloud computing. *The Journal of Supercomputing, 63*(2), 561-592.

Newman, A. L. (2015). What the "right to be forgotten" means for privacy in a digital age. *Science, 347*(6221), 507–508.

Polonetsky, J., & Tene, O. (2014). The ethics of student privacy: Building trust for ed tech. *International Review of Information Ethics, 21*, 25–33.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). doi:10.5210/fm.v15i1.2775

Rosen, J. (2012). Symposium issue: The right to be forgotten. *Stanford Law Review Online, 64*, 88–92.

Rymarczuk, R., & Derksen, M. (2014). Different spaces: Exploring Facebook as heterotopia. *First Monday, 19*(6). doi:10.5210/fm.v19i6.5006

Shapiro, T. R. (2013, July 29). Stolen laptop contained 2,000 Fairfax student health records. *The Washington Post*. Retrieved from http://www.washingtonpost.com/local/education/stolen-laptop-contained-2000-fairfax-student-health-records/2013/07/29/4298ba52-f88b-11e2-afc1-c850c6ee5af8_story.html

Shirky, C. (2008). *Here comes everybody*. New York, NY: Penguin.

Solic, K., Nenadic, K., & Galic, D. (2012). Empirical study on the correlation between user awareness and information security. *International Journal of Electrical and Computer Engineering Systems, 3*(2), 1–5.

Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management, 30*(2), 109–116. doi:10.1016/j.ijinfomgt.2009.09.004

Tang, E., & Lam, C. (2014). Building an effective online learning community (OLC) in blog-based teaching portfolios. *The Internet and Higher Education, 20*, 79-85. doi:10.1016/j.iheduc.2012.12.002

Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: A time for big decisions. *Stanford Law Review Online, 64*, 63–69.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562. doi:10.1509/jmr.10.0355

Veletsianos, G. (2010). A definition of emerging technologies for education. In G. Veletsianos

(Ed.), *Emerging technologies in distance education* (pp. 3–22). Athabasca, Canada: Athabasca University Press.

Zdravkova, K., Ivanović, M., & Putnik, Z. (2013). Experience of integrating Web 2.0 technologies. *Educational Technology Research & Development, 60*, 361-381. doi:10.1007/s11423-011-9228-z