CONSIDERATIONS FOR SOCIAL NETWORK SITE (SNS) USE IN EDUCATION

Alan S. Weber, PhD
Weill Cornell Medical College in Qatar
Box 24144
Education City
Doha, State of Qatar
alw2010@qatar-med.cornell.edu

ABSTRACT

Social Networking Sites (SNSs) such as Facebook, Google+, Myspace, LinkedIn and Twitter have now become commonplace in international virtual space. Approximately 75% of all online adults maintain at least one social network profile. As SNSs are becoming more ubiquitous, they are also becoming more sophisticated and many operate on a free service model based on advertising revenues. Free services are obviously attractive to educational institutions in the developing world with small education budgets. With the exception of sites such as Edmodo, SNSs, however, are generally commercially driven and educational goals and purposes were not part of their original design: educational uses have generally been the result of the creative adaptation of SNSs by educators and application builders. Therefore some serious issues of data privacy, trust, and security have arisen since both the educational, medical, and medical education realms operate in the U.S. under strict data protection laws such as HITECH, HIPAA, FERPA, and COPPA. Potential educational advantages of SNSs are similar to general e-learning benefits such as: anytime / anywhere instruction, lower cost for institutions, knowledge crowdsourcing, interconnectivity and facilitation of online collaborative work, peer-to-peer instruction, and the provision of virtual training scenarios (role-playing) not available or practical in the non-virtual world. However, the business models of many SNSs as essentially advertising platforms and as a means of tracking online behaviors which can be monetized (with non-transparent policies of data collection and retention) raise some key concerns for educators.

KEYWORDS

Social networks–education, e-learning, Social Network Site (SNS)

INTRODUCTION

The growing popularity of Social Networking Sites (SNSs) for use in business, advertizing, and recreation–and now for educational purposes–has become an international phenomenon. Facebook, for example, surpassed 1 billion active monthly users in October 2012 [1]. President Barack Obama has been a frequent user of SNS sites for both of his election campaigns and U.S. governmental use of SNSs will undoubtedly expand despite some security and defense issues (data-mining and compromise of military secrets by enemy cyber attackers using phishing, worms or Trojans). Military social network use has been partially solved, however, by the development of a secure private network called NIPRNET. Second Life, Facebook, Google+, MySpace, Twitter, LinkedIn and other social networking sites are a set of web
technologies designed to facilitate content creation, sharing, communication and interaction among users. They often revolve around user-generated content such as photos, videos and blog text, and copyright and data ownership issues have been the subject of serious debates, especially with Google’s YouTube service. SNS users typically create a profile with uploaded pictures, text, or videos and links to other sites and then begin interacting with “friends” or other users or members both on and offsite who are invited to connect to the user’s profile. Other connected users, variously called ‘friends,’ ‘contacts’ or ‘followers’ can be anyone who is allowed to connect with the user’s profile (view and share information), and friends can include anyone ranging from intimate family members to complete strangers. Most sites provide some form of blocking, reporting mechanisms, and privacy settings, allowing the user some control over who has access to specific information, although data remains available and in many cases legally belongs to the site owners. As discussed below, there is a fundamentally antagonistic relationship on sites such as Facebook between individual users, who generally desire greater control over private and personal information, and the site owners whose revenue streams depend on maximizing the amount of personal information (friendship relationships or friends, email contact lists, online browsing habits, “likes,” product purchases, etc.) that the site collects to sell to advertisers. Each SNS site caters to different demographics: LinkedIn appeals to business professionals, Facebook has a wide spectrum of users, Myspace has a younger subscriber base primarily interested in music (music star Justin Timberlake is part owner), and Edmodo has been specifically designed for educational uses.

Situated within the U.S. context (the largest social media sites are incorporated in the United States), this paper examines the current uses and potential as well as the serious ethical and practical barriers to social networking site use in education. Awareness of internet law and internet practice in the United States is critical for international educators to assess security, privacy, and trust in SNSs for educational use, since Google, Facebook, and Twitter, for example, store data primarily on U.S. servers which are subject to U.S. laws. Although these sites subscribe to the US-EU Safe Harbor framework, which allows U.S. companies to comply with the stricter privacy protections of the European Union Directive 95/46/EC, both Facebook and Google have been the subject of EU data regulator investigations regarding lack of privacy protections.

Social networking will inevitably become more and more attractive as a medium of instruction for educational institutions on restricted budgets. In fact, some form of social media is used by the majority of Internet users every day: according to the Pew Internet & American Life Project, 63% of online adults reported having one profile on an SNS in 2010, and 86% of 18–29 year olds said that they use an SNS every day [2].

SNS usage is particularly high among high school and undergraduate university students (73% of online teens and 72% of online adults in 2009 used social media), but the recent blurring of academic and social life raises questions
about what exactly students are doing on their computers since the laptop computer has become one of the most important productivity tools for students (for accessing libraries and e-resources, writing term papers, checking databases, etc.). At the same time, wireless-enabled computers now fulfill many entertainment and recreational needs (surfing the internet, watching online videos, online gaming, chatting with or emailing friends, etc.). Anecdotally, students around the world are reporting difficulty in separating these two worlds. At the author’s own institution—an American medical college in the Middle East—students have confronted the issue of interruption of study time by social network use by such strategies as changing Facebook passwords on each other’s accounts and locking each other out from social media sites until final exams have been completed. Madden reported in 2010 a sharp drop in blogging activity from 28% of 12-29 years olds in 2006 to only 14-15% in 2009 [3]. This finding is somewhat troubling since writing has been a central mechanism for learning and discovery throughout the history of education. Writing promotes active learning, in contrast to some online learning activities such as passively reading online text or listening to or viewing lectures (podcasts or streaming videos). Research studies on SNSs are now stratifying and delineating the specific nature of online educational activities, since passivity or activity of the specific educational task seems to be an important factor when correlated with academic achievement. Even if SNSs are not used in formal learning experiences, do they promote other kinds of learning such as social skills development, general communication, and psychosocial development? There is persuasive evidence that learning outcomes in general are not dependent on the teaching medium used, i.e. traditional, face-to-face instruction versus electronic, or mixed-mode blended approaches, but more on factors such as curriculum design and student motivation, preparation hours, etc. [4]. There is a general consensus among e-learning specialists that technology is not an educational panacea, and that many early adoption programs were disastrous: expensive computer hardware and networks were dumped into the classroom without clear learning objectives or specific activities and learning goals. As social networking specialist Karen Kear points out: “by using online networking tools such as discussion forums, social network sites, wikis, blogs and instant messaging, learners can carry out activities together. They can be members of online learning communities….however, simply giving learners communication tools will not automatically create a learning community. It requires a teacher with skill, knowledge and imagination” [5]. The fact that SNSs offer so many new and easily accessible choices for interactivity merits further study. Griffiths et al. have even argued that SNSs represent the future of health care in their potential for health education, health monitoring, and health information networking [6].

I. BENEFITS AND POTENTIAL OF SOCIAL NETWORKING IN EDUCATION

The interfaces for most social networking sites—led by Google’s revolutionary uncluttered search engine box in the 1990s, and Facebook’s
equally simple early graphic layout in 2004–have been developed for ease of use and even neophyte users report few problems with the basic functionality of these sites. Adding material (uploading files) and navigating is relatively simple. This reduces teaching and training time in educational settings. Also, free web-based hosted services obviously save enormous institutional costs and ITC maintenance time when compared to proprietary Learning Management Systems, such as Blackboard and Moodle (an open source LMS, but which requires ITC experience for installation and maintenance). However, LMSs have been specifically designed for educational purposes, thus they have theoretically more robust security as they are installed on in-house servers and offer greater secured functionality such as gradebooks, quiz banks, and third party educational plugins.

The social nature of SNSs promotes the formation of communities that were formerly limited by geographical boundaries: now virtual communities using the same natural language can transcend many practical limits and barriers (time, place, and social class, for example) and communities can now be organized by belief, practices, or goals or purposes instead of geospatial accident.

The ease in which multimedia can be linked, shared and consumed also provides an entertainment aspect to social media use which has been capitalized upon by edutainment developers. Some educators claim this entertainment value promotes student engagement and motivation, while others view it as a distraction from serious learning endeavors. An excellent case study illustrating educational use of SNSs, and specifically avatar-based virtual worlds, is the Second Health project built on Linden Labs Second Life virtual world platform in 2007. The project, which consists of a virtual hospital for clinical skills simulation training is a joint venture between the UK’s National Health Service (NHS) and the Department of Biosurgery and Surgical Technology at Imperial College London. Users can create avatars which communicate with other avatars, navigate the virtual world and obtain and manage objects. Imperial College has developed clinical scenarios which allow participants to practice safety training in a simulated clinical environment without endangering real patients or trained standardized patients. In the pilot test of Second Health’s clinical scenarios conducted for nurses who had never used Second Life before, 82% of participants recommended the Medical Device Clinical Scenario to other nursing students and colleagues [7]. Role playing is an essential feature of clinical skills medical education: various patient and physician-in-training encounters (taking a history, examining a patient, ethics consult with family members, etc.) using avatars in virtual social worlds have great potential for expanding the possible varieties of role playing scenarios, again all without endangering live patients or standardized patients (specially trained actors), who are extremely costly to train and employ. The website Edmodo.com may be the best example of a safe and secure social network specifically designed by educational support staff for educational purposes. Facebook and other SNSs in their business plans do not seem to have targeted education-specific applications.
II. BARRIERS TO SNS USE IN EDUCATION

1 EDUCATIONAL OUTCOMES

According to the work of Yaros, which is grounded in social learning theory, it is reasonable to hypothesize that social media will facilitate knowledge transfer since learning is fundamentally a social experience impacted by social and environmental contexts [9]. Some recent studies have attempted to correlate SNS use with educational achievement. Theoretically, one could hypothesize that excessive SNS use takes time away from learning activities and potentially interrupts concentration and study while multi-tasking on computers (undergraduate and graduate student study and research are now heavily conducted on computers, for example reading e-texts and searching electronic databases). One could hypothesize as well that SNS use has positive effects such as refining knowledge-seeking behavior, and developing general social, networking, and negotiation skills. Although there is a large body of research on the education outcomes / media nexus (television / movies) as well as the education outcomes / e-learning relationship, these research findings must be used carefully in attempting to elucidate SNS educational usage or to create analogies for hypothesis building. One specific caveat should suffice: television, although encompassing both visual, dramatic (narrative), and natural language elements just like social networking, is essentially a passive medium, while social networking’s core functionality revolves around interactivity. Kirschner and Karpinski argued in 2010 that Facebook use took time away from...
study and resulted in lower GPA. Their research results indicated that Facebook users reported lower GPAs and spent fewer hours per week studying than non-users [10]. This approach is generally known as the time displacement theory and studies to test it have had variable results. Also this pilot research was exploratory in nature, used a small sample size (219), and employed a self-reported GPA. However, Pasek, More, and Hargittai, found no such correlation between Facebook use and educational achievement in a nationally representative sample in 2009, reacting to an earlier study by Karpinski which had caused a media stir [11].

According to Junco’s large-sample study (n=1839), “time spent on Facebook and checking Facebook were negatively related to overall GPA, while time spent on Facebook is slightly negatively related to time spent studying” [12]. Some activities on Facebook were positively correlated with GPA and some negatively, indicating that more studies are needed to determine specific usage of the site as it relates to overall academic performance. Paul et al. [13] also found a correlation between decreased GPA with higher usage of social networks and determined that those students with a higher attention span spent less time on social networks. In their 2009 survey of college students, Valenzuela et al. discovered a positive relationship between Facebook use and outcomes such as life satisfaction, social trust, civic engagement, and political participation, which naturally would result in a better prepared and more rounded student primed for learning [14]. Unfortunately at the current time, the amount of available evidence does not allow us to do a satisfactory meta-analysis of the seemingly contradictory research outcomes about SNS use and academic achievement.

Due to its ubiquity and ease of use, social networking certainly merits further study for educational use, but educators will need to take the lead in developing social networking for educational purposes and not rely on the business sector to realize the potential educational uses of their online services and products. Although ‘digital natives’ may be adept at using communication technologies, they may not be capable of adapting them for learning purposes and may not be aware of online learning resources. Older adults often mistake younger users’ apparent facility with using the interfaces of technology (sending an SMS, setting up a profile) for a deeper understanding of how technology and networks actually work. Many of the tasks that students perform online simply involve clicking on buttons and following prompts. Except for a very small percentage of self-actualized and self-motivated students, most learners cannot be expected to integrate any technology, let alone SNSs, into their learning goals. Ng argues, “it is the task of educators to raise awareness of the range of educational technologies that the digital natives could use for learning. They need to be taught about these technologies, just like people born into a community need to be taught how to speak the language or use tools and equipment that are available to the community. Unlike the learning about and use of social networking and other entertainment tools which are largely peer-driven and learnt through ‘tinkering’, it is unlikely that digital natives would seek out, explore and use educational technologies unless they are introduced to them and/or there is a need
to use them for a useful purpose” [15]. Ng points to another potential problem with educational uses of social media: education has traditionally involved the transfer of knowledge from expert to novice; unless the expert is being paid for her time or is conducting a formalized learning activity (for which again, she would expected to be remunerated), the novice expecting expert knowledge, advice and consultation can only rely on the altruistic behavior of the expert. This is not to say that valuable peer-to-peer knowledge cannot be gained from social networking, but peer (technically meaning equal) in the sense of knowledge exchange means someone with the same knowledge base. There is some concern that social networks, both online and traditional, can reinforce social boundaries and actually exacerbate exclusion [16]. The interactive web in its early days was idealistically envisioned as a flattening experience that could potentially reduce power differentials and promote democracy and the dismantling of social castes. But do social networks in reality encourage the kind of self-growth and learning that results from respectfully engaging difference and entertaining other points of view? The word for ‘like congregating with like’ on the Internet is ‘homphily,’ literally love of the same. The persistence of flaming and hate-speech in unmoderated forums and chat rooms indicates the continuing human need to segregate and differentiate alongside the desire to connect, empathize and recognize similarities. The dangers of continually reproduced sameness that SNSs can promote by the creation of circles of like-minded ‘friends’ strike at the heart of the critical and analytical thinking skills central to western education, confronting and understanding otherness: “when we make our conversations into a kind of echo chamber…we lose the kind of critical opposition which allows us to question our beliefs, either to reform incorrect views or to understand more clearly why we believe what we believe, through the experience of talking it through with people we disagree with” [17].

2 MALWARE AND SNS APPS

Educational applications (apps) that run on mobile computing platforms hold great promise as smart phone usage increases: applications running on servers can process large amounts of data providing data-intensive processing for small hand-held devices. For example, natural language processing, image processing, and GPS geolocation are traditionally highly CPU intensive, but this processing can now be done by hosted service cloud architecture and then transmitted to the mobile device via wireless Internet. However, the proliferation of apps for hand held devices means a new breed of malware, especially if there is inadequate policing of app makers. Malicious applications have been discovered by security researchers both on the Apple App Store and Google Android. Many SNSs do not sufficiently review and vet potential malicious application developers who create apps for their platforms in order to harvest personally identifiable information (PII) for both targeted advertising and possibly even identity theft in a small number of cases. When a user installs an app, they may be inadvertently granting that app unrestricted access to all personal data, including that which has been designated
private by the user with privacy settings. As Egele et al. explain: “unless the application requires solely public profile data, the user has to either grant an application full access rights to all her profile information, or she cannot use the application at all. These are the only options available to the user, and they do not vary with the data needs of an application. This behavior is in direct contradiction with the ‘principle of least privilege’…which states that every actor should only get the minimal set of access privileges that allow it to fulfill its task. The privacy problem in the current system exists because there are no means for a user to restrict or learn what information is accessed by a given application” [18]. The scenario above, in conjunction with SNSs’ often repeated statements that they take user privacy seriously, creates an illusory sense of privacy and personal data control for the SNS user. Privacy and security are closely related issues since private data obtained by malicious persons can be used to exploit system, account, and individual personal computer vulnerabilities. The practice of apps harvesting data is probably much more widespread than reported. The Location Protection Privacy Act of 2012 sponsored by U.S. Senator Al Franken (D-Minnesota) would crack down on so-called “stalking apps” by requiring companies to obtain customer permission to collect location data (cell phone GPS coordinates, for example) and permission to share this information with third parties.

The vast amount of personal information on social networks opens up the user to spear phishing, or personalized targeted attacks to glean PII that hackers can use for identity theft, fraud, and other illegal commercialization. Researchers Moyer and Hamiel demonstrated one simple and successful spear phishing experiment called “Satan is on My Friend List.” The researchers “detailed how they had (with permission) impersonated a well-known IT security professional on LinkedIn. Social networks are full of members who judge their self-worth by the number of ‘friends’ they have. Some even boast of their promiscuity, labeling themselves ‘open networkers’. Moyer and Nathan found plenty of them with a simple Google search. In 12 hours, their fake persona had attracted 42 connections, giving it sufficient credibility to attract connection requests from a member of the person’s family, other professionals and a magazine editor. At no time did anyone question the veracity of the profile” [19].

Weir et al., however, see no specialized threats from social networking. They conclude that the medium of social networks simply provides a low-cost easily accessible platform for e-crime, and that if SNSs did not exist, the exact same crimes would be committed but by other means: the “networking context serves simply as an enabler in the perpetration of the offence. In the absence of this context, wrong doers would have to find alternative ways to achieve their nefarious ends and, in so doing, would commit the very same criminal acts by different means” [20].

3 VIRTUAL VIOLENCE: ONLINE BULLYING / CYBER-STALKING

A youth survey from the U.S. reports that 72% of adolescents or teenagers have been victimized by online harassment. Name-calling and personal insults were the most common forms of harassment [21]. The faceless nature of
some online threats such as trolling render them particularly traumatic (fear of the unknown). Nancy Willard defines cyberbullying as online behavior that is “defamatory, constitutes bullying, harassment, or discrimination, discloses personal information, or contains offensive, vulgar or derogatory comments” [22]. Spreading rumors, malicious gossip, spamming, and using online photos abusively can also be construed as abuse. Obviously these concerns are endemic to the Internet itself, but each can be exacerbated and facilitated by SNS use due to the interconnectedness of information and informants.

Kwan and Skoric’s study of Facebook bullying of 13-17 year olds (n=1636) in Singapore argued that cyberbullying is simply an extension of everyday bullying: “parents and schools should focus on the root of the problem, which very frequently manifests itself in everyday school bullying. It is also necessary to question the continued efforts in differentiating cyberbullying from school bullying. While the medium/environments certainly differs, it seems that fundamental causes and motivations are quite similar” [23]. Another cyber threat, unwanted or illegal online sexual solicitation or sexually harassing behavior, is more common in open chat rooms than on SNSs, probably because the majority of users are now using privacy settings to restrict viewing of their profile information to friends only [24].

4 LACK OF PRIVACY PROTECTION

To understand the privacy and security issues surrounding social networking site use, one must look carefully at their business models – they are essentially advertisers. Both Google and Facebook derive most of their revenue from advertising services based on tracking user behavior and aggregating user data across accounts, a practice which has spurred an ongoing privacy dispute with European data regulators. Google’s thirst for tracking data is so strong that it subverted Apple’s Safari browser privacy settings (do not track) to enable user tracking, and was fined $22.5 million by the Federal Trade Commission in 2012 for this offence. Social networking sites normally set default privacy settings at the lowest possible (most open) level to record user behavior and glean personal data in order to serve targeted advertisements back to the users. They also may sell information about users to other parties, although specific details about these practices are not publicly available. Bonneau and Priebusch after their review of social networking privacy policies in 2009 noted that although most sites promote themselves as privacy friendly and pro-privacy, policies are often written in confusing legalese, and “privacy in social networks is dysfunctional in that there is significant variation in sites’ privacy controls, data collection requirements, and legal privacy policies, but this is not effectively conveyed to users” [25]. This is because the open sharing concept (low privacy level) of SNSs is in fact financially beneficial to them. Internal research from Facebook indicated that in 2009 fewer than 20% of users actually modified their default privacy settings, which seemingly contradicts other self-reported data by users themselves that they were actively restricting access to their profiles and believed that they were enhancing their degree of privacy: this
contradiction possibly indicates that users are misusing or misunderstanding Facebook’s privacy settings, or are being deliberately misled into a false and unwarranted sense of privacy. Whatever the ultimate cause of this discrepancy, “it is likely that more individuals will experience unexpected privacy violation and intrusion by parents, employers, and unknown others” [26].

Conflict has arisen recently between Google, Inc.—a U.S. company which has ventured into social media and uses similar practices as other SNSs and maintains almost identical policies to many popular SNS sites—and European Internet regulators in that Google’s new privacy policy does not conform to European data protection laws [27]. Many U.S. online corporations generate considerable income from advertising based on behavioral profiles generated by the user’s site and Internet usage, as well as other collocated and aggregated data. Due to its dominance of the search engine and online media markets (YouTube), as well as popular services such as Gmail, Google has more personally identifiable data about users than any other entity, including the U.S. government. Online companies can obtain revenue from selling profile information to government and law enforcement agencies. The recently released *Yahoo! Compliance Guide for Law Enforcement* states that Yahoo profile account information will be supplied at a cost of 30-40 USD per account (with required subpoena) [28].

Although users generally believe that through deletion, privacy settings and the option to request a full file of their personal data (personal history) stored with Facebook, that they are in control of their private data, this is not the case. Facebook stores more data than it will release to an individual upon request. A group called Europe vs. Facebook using the European privacy law Section 4 DPA + Art. 12 Directive 95/46/EG obtained a 500 MB PDF file of data which the group thought had been deleted by themselves. This was in contrast to a 150 MB PDF file of the same requested information that Facebook had earlier released to the group via its web request form. Thus, according to Miller, “‘removed’ content is not really deleted by facebook and it is often unclear what facebook exactly does with our data. Users have to deal with vague and contradictory privacy policies and cannot fully estimate the consequences of using facebook” [29]. The implications of Facebook’s data retention policies are clear: youthful indiscretions of students recorded by Facebook could haunt the users later on in adult life. Sharing health information and student records or grades “privately” with family or friends on Facebook or other SNSs creates sensitive PII that can be viewed internally by site administrators. In other contexts, this data would be protected by FERPA, HIPAA, and HITECH laws in the U.S. Currently technology is moving much faster than internet law to address data privacy concerns on SNSs and the official enforcement agency the Federal Trade Commission (FTC) does not vigorously pursue infractions except in the case of health data breaches [30].

The list below represents the current challenges that the U.S. government is facing in using social media for connecting to the public. These are the identical concerns with respect to privacy, security, trust, reliability, permanence, and inclusion that educational institutions and students
must face. Each point has obvious and serious implications for education. The authors who compiled this list in 2010–Bertot et al.–point out that these issues are only “partially addressed or not addressed at all by current [U.S. government] policy”:

• Ensuring information disseminated through social media is consistently available;
• Making information available through social media available in other formats for those who lack equal access due to infrastructure, ability, language, or literacy;
• Maintaining consistency of access for government agencies and for members of the public;
• Archiving information disseminated through social media for permanent access and retrieval;
• Preventing release of sensitive or secret information;
• Fostering transparency and accountability, through which government is open and transparent regarding its operations to build trust and foster accountability;
• Ensuring the security of personally identifiable information;
• Maintaining security of user information;
• Providing a continuously updated data.gov registry, with an historical index that shows current and past data availability;
• Ensuring that third-party social media technology providers (e.g., Twitter, Facebook, YouTube, Second Life) adhere to government privacy, security, and accuracy policies and requirements;
• Ensuring that individual-government transactions that transpire through social media technologies are confidential, private, and/or secure as required by federal laws and policies;
• Ensuring continuity of service, especially when technologies sunset. For example, Yahoo announced the discontinuation of its delicious tagging service;
• Ensuring that mashups and other forms of data integration—an increasing activity due to data availability via data.gov—do not lead to user profile development that invades privacy or otherwise compromises individuals, national security, or agency data security;
• Monitoring the storage of government information when held off-site through cloud computing services. Allowing private companies to maintain potentially sensitive government data raises enormous questions of data retrieval, accuracy, and permanence, as well as opens up significant opportunities for misuse of data by providers or attempts by other governments to access the data based on the geographic location of the server farms where the data are maintained; and
• Ensuring that social media technologies are not the only means of getting a response from an agency” [31].

Due to these concerns, a new category of privacy-conscious applications has arisen, exemplified by Glassboard.com which delivers private social networks for both smart phones and on the web. Glassboard’s homepage lists all of the primary concerns that educators, consumers, and businesses encounter in attempting to use social networking in a safe and secure manner (see Table 1 below):
Table 1. Features of Glassboard.com Addressing Users’ Privacy and Security Concerns When Using Mainstream SNSs

<table>
<thead>
<tr>
<th>Glassboard Homepage Claim</th>
<th>Concern Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Glassboard has no privacy settings — because everything is private.”</td>
<td>Overcomplicated and potentially deceptive privacy settings-defaults set to maximum data sharing.</td>
</tr>
<tr>
<td>“you never have to worry about the rules changing.”</td>
<td>Change in terms of service, such as implementation of Facebook’s Beacon, without prior warning to users.</td>
</tr>
<tr>
<td>“get things done knowing your messages are confidential”</td>
<td>Lack of confidentiality, lack of protection against internal data abuse and data mining.</td>
</tr>
<tr>
<td>“Unlike Google, Facebook, and Twitter, we don’t mine your data to sell advertising. We don’t do ads.”</td>
<td>Poorly regulated and non-transparent use of consumer data for profit. Unknown third party usages of consumer data.</td>
</tr>
</tbody>
</table>

5 SURVEILLANCE AND SPYING

Facebook and Google are two of the most extensive and wide-ranging surveillance tools ever developed, with the largest databases of personally identifiable data ever compiled. They are routinely monitored by local police forces, private detectives, the Department of Homeland Security, the CIA, human resource directors (to screen job applicants), and university and high school administrators to police student and faculty behavior. Although SNSs claim that they collect user data anonymously, it is now a trivial exercise to link a device ID, IP address, or photograph (using the facial recognition software that tags Facebook photos) with a few simple and publically obtainable pieces of information such as gender, date of birth, and zip code to identify a specific user [32]. As Doyle and Fraser point out “the virtual ritual of narcissistic self-display on social networks like Facebook has become so compulsive that many are dangerously unaware that they are dressed in an open kimono in a world of ubiquitous visibility where new forms of surveillance and control are emerging” [33]. Those who are more sanguine about a potentially emerging Big Brother state argue that similar tools such as Wikileaks can be directed against the powerful institutions who are engaged in surveillance to create greater state transparency and equilibrium between citizen and state.

6 MISCELLANEOUS CONCERNS

The social network Facebook now manages and possibly entirely owns a large dataset of over 1 billion users. This data represents a unique resource for sociological, business, behavioral and epidemiological research. Most importantly, educational outcomes in SNSs can be tested and assessed on a large scale for the benefit of students and educational theory. Due to the mixture of anonymized information and PII, concerns related to research on human subjects naturally arise. Until recently SNS site owners were cavalier about protecting this data from data breaches, and normally when conducting their own research or licensing information for research by others did not seek informed consent from the users who generated the data on the sites. In February 2012, Twitter announced that it would sell a two-year archive of tweets to data analytics companies, a development that sparked protests from a variety of quarters. There was no opt-in or opt-out option provided to users. According to Grimes et al., “many researchers see virtual worlds as a harmless sandbox, in which all research
is fair game, since any harm done is virtual and without lasting impact” [34]. This viewpoint fosters an attitude that any form of online data is up for grabs without any ethical restrictions attached to it. However, online harm that could translate to real world harms from improperly collected, handled, and disclosed research data on human subjects could include libel, slander, defamation, damage to reputation, and disclosure of health status. Learning objects or business ideas that are posted to SNSs may become the property of the site. Formerly, Facebook claimed in perpetuity rights to all data (specifically IP or intellectual property) on its servers posted by users, but currently the terms of service read: “you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it” [35]. The shared content loophole appears to grant Facebook irrevocable rights to most user data on the site. When Instagram, an online photo sharing application purchased by Facebook in 2012, recently announced in its new terms of service that it had the right to sell user-posted photographs to third parties without prior notification, the backlash from users forced the company to backpedal. This behavior again is not in the least surprising since revenue streams in Facebook's current business model rely on creative commercial uses of user-posted data and metadata. Inclusion and access are also two serious concerns with the use of SNSs, specifically the digital divide. A large proportion of students internationally do not have affordable access to broadband Internet, with enough bandwidth for streaming video, limiting their learning experiences online. There are also sizable and not accurately measured student populations in Muslim countries whose parents forbid social media use, both for cultural reasons to prevent uncontrolled relationships and their parents’ refusal or inability to purchase the hardware to access the sites [36].

7 CONCLUSION

Social networking sites have great potential for educational use and are already in use for these purposes, such as educational apps for smart phones, Second Life avatar-based classrooms and Edmodo, an SNS specifically designed for educational purposes. These technologies may pose significant challenges to traditional Learning Management and Course Management tools. Privacy and security of student and instructor data are key concerns, however, for educators. There are, however, a variety of both user-controlled and potential technological solutions to protecting students and educators in SNS educational settings. Codes of SNS classroom conduct could be prepared by educational institutions and students could be specifically trained in privacy and security best practices through e-learning modules and online tutorials. Instruction in use of SNS privacy settings is critical, as sites often set defaults to the highest information sharing level. Educational institutions may even wish to employ encryption, block tracking and flash cookies (if possible), or employ Virtual Private Networks (VPNs) to obscure user IP addresses on SNSs. The
ubiquitousness of Google’s highly interconnected advertising network based on AdWords and AdSense on the Internet may render some of these attempted privacy protections as illusory, however. Recently two mechanisms relying on obfuscation to increase privacy and security in SNSs have been proposed: Hessler et al.’s scheme for obfuscating messages by encrypting corresponding coefficients instead of the data itself, and Parris et al.’s proposal for obfuscating personal information on Friendlists used for improving opportunistic network performance [37]. Also peer-to-peer technology which would decentralize data storage (distributed framework) would protect individual SNS user data from exploitation [38]. However, due to the pervasive and ‘back door’ methods that data aggregators and third party apps can use to scrape and crawl personal data from social network sites, technological solutions may need to be augmented by legislation. For example, the crowning argument of Internet lawyer Lori Andrews’s recent book on privacy and social networks is that a “Social Network Constitution” is now desperately needed given the strong analogy between “Facebook Nation” (the users of Facebook) and the traditional political nation state [39]. Elements of Andrews’s proposed constitution include: “the right to privacy of place and information,” “the right to privacy of thoughts, emotions and sentiments,” and “the right to control one’s image.” SNSs’ educational potential has been demonstrated in the recent Arab Spring revolts in Egypt, Libya, and Tunisia. SNSs such as Twitter, Facebook, and YouTube probably played a major role in the 2011 uprisings in North Africa by educating young Arabs about the actual political and social conditions in their own countries; and through discussions in forums and chat rooms, the crowdsourcing of expert and peer opinion on the historical circumstances of current government policies deeply guided public opinion. These tools were also used to rapidly organize concerted action. As Ghannam has pointed out: “to peruse the Arab social media sites, blogs, online videos, and other digital platforms is to witness what is arguably the most dramatic and unprecedented improvement in freedom of expression, association, and access to information in contemporary Arab history” [40].

REFERENCES


