the jaltcalljournal

ISSN 1832-4215
Vol. 11, No.2 Pages 165–176

Social media ethics in English language teaching

Andrew Blyth
University of Canberra
ablyth@uni.canberra.edu.au

Many teachers are increasingly using Social Networking Services (SNS) in their classrooms, which allows for the first time the outside world to peer into students' private learning spaces (Blyth, 2011). However, the adoption of social media has mostly been done without careful consideration of possible ramifications students may suffer. Consequently, this article considers issues of information management, identity, reputation, privacy, and potential consequences on classroom dynamics. Finally, there is a discussion of the privacy strategies that teachers could adopt.

Keywords: Social media, SNS, privacy, ethics, information management

Introduction

This article continues the discussion of social media ethics began by Blyth (2011) who stated some of the issues and potential problems of classroom SNS use and made a call to discuss this topic within ELT. This article will refer to publications in sociology and computer ethics, since there have been so few articles published within ELT and CALL. The focus will mainly be on aspects of protecting digital identity especially concerning real-world identity and reputation. Ferrari (2013) highlighted four points for safety for students developing digital competency, including protecting devices, protecting data and digital identity, protecting health, and protecting the environment. This includes, "active protection of personal data, understanding other people privacy

[sic], to protect self from online fraud and threats and cyber bullying" (Ferrari; 2013, p. 29), which are underlying themes of this article.

For different groups of people, social media and related ethics mean different things. Many new parents have stated concern about the privacy of their children (Geddes, 2014), and some teachers have their own reasons for considering the importance of social media ethics. Firstly, some teachers are aware of repercussions that may or have already occurred from uncensored publicity of personal information on social media, but they are uncertain as to how to proceed. Secondly, teachers respond to the intentionally provocative word choice, "ethics." "Ethics" is a rather potent academic concept, because of the powerful human rights connotations attached to it.

We are entering an age of communication that has never been experienced before, and our cultural history with the internet is short, so we have not yet learnt how to avoid all of the pitfalls. This is evidenced by the fact that we have not settled on a canonical term to describe the medium of Internet communication we are referring to. Consequently, the terms social media, social websites, blogging, micro-blogging, internet forums, newsgroups, websites with a public or even a limited display of user created content, and including Facebook, Google+, Instagram, Joomlas, Line, Mixi, Padlet, PHPBBs, Snapchat, Whisper, and others are for this article synonymously "Social Networking Services" (SNS).

All SNSs offer a range of security and privacy options with varying outcomes depending on what and how personal information is treated by the SNS provider. For the purposes of this article, the term "information" refers to data about a person including profile content and bio-data, images, likes and plusses; also reportable ideas, thoughts, events or actions people have or could do. Wagstaff (2010, cited in Blyth, 2011, p. 470) described a kind of data dichotomy of cookies and breadcrumbs, of which this article focuses mainly on the latter. Cookies are the bits of data websites leave on your computer. Conversely, breadcrumbs are the bits of data we leave on websites, which can include profile information like our name, avatar, address, photos, as well as comments, Facebook likes or Google+ pluses, and so forth. Additionally, there seems to be a continuum of profile types that SNS services require: maximal to minimal. Maximal profiles require real names, multiple email addresses, date of birth, phone number, and more; in essence, a wide range of information such as that expected on dating sites like Match.com and Eharmony as well as Facebook. Conversely, a minimal profile type might require only a username, like Whisper. Most SNSs fall somewhere in between.

Our breadcrumbs can be aggregated and compiled on third party websites. For instance, pressing the like button for your favourite movie on a review website can appear in your Facebook page. Geotagging services like FourSquare automatically post a message to Twitter each time you pass near certain locations like your favourite bar or café. Furthermore, photographs can have embedded GPS metadata, and Google+ and Twitter posts can also be geographically tagged. Websites like Spokeo.com use these breadcrumbs to allow anyone to look up people, and can even geographically locate them, providing a partial address, and even show a satellite view of their house or neighbourhood. Palis (2012) reported on a list of "creepy apps" that were (and some are still) available. One such app, Girls Around Me (GAM), aggregates women's breadcrumbs and displays them on a Google-like map with pins that indicated current approximate locations of women with their Facebook profile photo. Additionally, Maden and Smith (2010) say that facial recognition software and apps can be used to inhibit political participation. Facial recognition software can allow you to discover the name of someone you see (and photograph) in a bus or at a pub

(see http://www.ibtimes.com/facial-recognition-apps-nametag-could-lead-situation-war-terror-1553180 for more details). These functions already exist in Facebook (currently only in the US; Geddes, 2014) and Google+, allowing people to automatically "tag" "friends" in photos.

Despite the potential for objectionable uses of breadcrumbs, I support SNS use in education. Even if there are no pedagogically effective ways to implement SNS in education now, there will probably come a time when student learning will occur more efficiently with SNS than without. Consequently, the benefits should outweigh the risks, but finding a way to ensure this happens is the intention of this discussion. Therefore, teachers cannot heedlessly impose upon students a requirement to display class activities on SNS, especially as there may be repercussions either now or in the future for them leaving their EFL breadcrumbs on the web. Central to this is the need to promote student digital competencies and protect their reputations whilst they are within our duty-of-care.

Ideally, the ELT community would agree on a set of best practices; however, there is still a dearth of knowledge of social media ethics. Therefore, this paper will only introduce the most central concepts; in particular, information management, privacy, how these may affect classroom dynamics, and then end with examples of options on how we can reduce the chances of serious negative events. Unfortunately, the options given may be inadequate, as demonstrated in the privacy strategies section far below.

Information management and identity

Information management, in particular, digital privacy and real-world reputation are intertwined. Nippert-Eng describes the impression management we do, where we "… organise what we do and do not [allow] others [to] know about us" (2010, p. 24), which includes real world events and attaching them to our digital identities, which creates an online record that is for all intents permanent. Some of these events we might like to revel in, whilst others we would rather forget. Some SNS posts may stigmatise us later in life; we have yet to see the outcome of a political campaign of a netizen with a substantial breadcrumb history. Consequently, some parents' take extraordinary actions in protecting their children's future reputations, where they vehemently oppose any photos of their new-borns from being posted online, and even adopt online pseudonyms to refer to their children (Geddes, 2014).

Despite our best efforts, events or incidents that happen to us may be out of our personal control, which may have consequences. Therefore, we do everything possible to keep these life events from damaging our reputations and relationships with others; simultaneously, we selectively share this sensitive information with an intimate few to further deepen friendships. Examples of things we keep private in order to maintain a good reputation can include divorce, sexual orientations, health status (like AIDS or similar), mental illness, failed job interviews, personal opinions of certain other people, among others. An uncontrolled public disclosure of sensitive information can inhibit normal social interactions (Nippert-Eng, 2010). Google has abandoned their real-name required policy for Google+. However, Facebook continued to enforce theirs for quite some time[1] despite many people needing to use pseudonyms for various reasons. A technology journalist, Violet Blue, reported that Facebook was "insidiously outing a disproportionate number of gay, trans and adult performers," which placed them at high risk of discrimination, harassment, and violence (cited in Kayyali & York, 2014). Furthermore, this policy also allowed

for reprisals against political journalists in Syria and Vietnam (Violet Blue, 2014, cited in Kayyali & York, 2014).

Consequently, we have to be mindful of what we ask our students to share about themselves on social media. Blyth (2011) stated that there is a dichotomy in education: there is the inside classroom space, and the outside; terms that are intentionally transparent. Inside the classroom is traditionally a private place where students can experiment with not just language, but also thoughts, ideas, and beliefs, especially in the senior high school and university levels. Such students typically have not cemented many of their beliefs, which may change during their adult lives, anyway.

In an example of where the outside world was brought into a private space was when the then British Prime Minister Gordon Brown's remarks about a right-wing woman who had just confronted him during an election campaign stop were reported in the media. Though his unflattering remarks were made in the privacy of his car, he still had a live wireless microphone attached to his lapel, and the remarks were recorded by journalists outside, which were then reported and resulted in him being lambasted (Aide, 2010, cited in Blyth, 2011, p. 471).

Blyth (2011) suggests that SNS may similarly play a detrimental role in our students' futures, where ramifications can be nearly immediate or delayed. What if a student posted comments that could later be interpreted as being misinformed, stereotyping, or ignorant? Though our students are young, many of them are in fact future leaders of society, where some of them will attempt to become bank managers, politicians, schoolteachers, and other trusted professionals. There are already reports of lost job opportunities as a consequence of students' less-than salubrious SNS postings (Lewis, Kaufman, & Christakis, 2008). It does not help that writing is a form of communication through time, where unknown persons at various points in history and geography are able to read our messages and potentially misinterpret them, or worse, re-interpret them. Written communication has many issues, for instance, the full context and background of the written message may be assumed by the writer but not conveyed (Hyland, 2009). This means the reader will interpret the written message using only the knowledge that he or she has, especially as the written message is disembodied from the writer and the original context (Hyland, 2009). What if the student changes his or her views on a topic? Unhelpfully, the recent and contested EU ruling on the Right to be Forgotten still has an uncertain future. Despite this uncertainty, "College students … provide personal information … that can be viewed by large numbers of unknown people and potentially used in harmful ways" (Lewis, Kaufman, & Christakis; 2008, p. 79).

Information management, reputation, and consequences

The issue of information management is on the minds of many internet users who consider how their online presence may affect their offline reputations. As a consequence, North American internet users occasionally monitor their and other people's web presence (Maden & Smith, 2010, p. 1):

- 57% of adults use search engines to check on themselves
- 46% of online adults have an SNS profile
- 46% of adults search for people from their past
- 31% of employed internet users have searched for information about colleagues
- 34% go online to check up on their dates

Additionally, Maden and Smith (2010) report:

- 12% of employed adults are required to promote themselves via SNS
- 48% of adults agree that it is now easier to meet new people
- 40% of internet users say that through the internet they have been contacted by someone from their past
- 33% of internet users worry about the amount of information available about them being online (down from 40% in 2006).

Interestingly, the numbers above reveal a privacy paradox. In order for us to engage in an online social environment, especially within the paradigm designed by Facebook, users are required to reveal themselves (Leigh Young & Quan-Haase, 2013). Nippert-Eng (2010), described how we use personal secrets as a kind of currency in friendships. The more secrets we share with our friends, the tighter the friendship bonds become. Similarly, this online privacy paradox forces people to publicly share otherwise personal information, as though it was a currency. The more privacy relinquished and personal information that is spent on SNS, the more engagement within the online community one is allowed. Effectively, Facebook is a trading house for people's personal information. According to Nippert-Eng (2010), intrinsically tied in with having secrets is the management of these, which is usually used as a system of keeping others close or distant, and to do so the control of secrets is paramount. Nippert-Eng (2010) suggests that there is a secrets etiquette, where decisions are made as to either disclose or not disclose certain information to certain people, which also entails considerations of information ownership. Ownership of information involves whether a person has the right to disclose other people's information or not and the power it can give to the secret holder. Consequently, disclosing other people's information removes their ability to manage their identities and relationships, as seen with the Gordon Brown example above.

It can be assumed that young university students worldwide have limited experience of the world, so they would have a certain level of naivety. However, disconcertingly for teachers who typically have more life experience, Maden and Smith (2010, p. 1) say that people aged 18-29 are more likely to implement privacy strategies, as listed below:.

- 44% say they take steps to limit the amount of personal information about them online, compared to 33% of 30–49 year olds,
- 71% say they change privacy settings, compared to 55% of 50–64 year olds,
- 47% say they delete unwanted comments, compared to 29% of 30–49 year olds.
- 41% say they remove their name from photos, compared to 24% of 30–49 year olds.

Lewis, Kaufman, and Christakis (2008) were more specific when they surveyed how their North American university students use SNS and privacy settings. Firstly, university students are more likely to be involved on an SNS if their friends are. Secondly, their SNS behaviour typically mirrors their friends'. They also found that students usually display a lot of themselves, but, and thirdly, only turn on privacy settings as a consequence of a negative event, say a crashed party, a lost job opportunity, a sexual assault, among other reasons. The figure below is an adaptation of their explanation. It shows that their privacy behaviour is typically consequential to a negative experience. Where first a negative event occurs, behaviour in terms of privacy settings and what is posted changes; awareness is raised within the victim's circle of friends; then this awareness spreads. The negative event may occur soon after certain postings, or be delayed for quite some time.

Figure 1. A model of the adoption of privacy settings based on Lewis, Kaufman, and Christakis (2008).

The potential irony is that, if we do not have this social media ethics discussion now, a serious negative event may occur in the ELT community, where for instance, a student's class SNS participation may result in real world consequences. Therefore, our behaviour may also become consequential, and may cause an unpragmatic extreme swing of the pendulum to near complete avoidance of SNS in the classroom. Students relinquish a lot of their personal autonomy when they enter our classrooms, so as classroom leaders, we have an onus not to increase the chances of consequences of studying with us. Consequently, it is proposed that we should adopt the model below in Figure 2. The model first proposes that we problematise a situation (the status quo): the current use of SNS in the classroom. Secondly, consider the possible consequences (as raised by Blyth, 2011; and above). Thirdly, the step now is to create and analyse the plausibility of potential solutions (see below). So that, fourthly, we can prevent or minimise incidences of negative events.

Figure 2. Getting four steps ahead: a proposed model of preventing or reducing the incidents of negative events involving SNS in education.

Who's accountable?

Before we can draw up a set of best-practices guidelines, there is still the question of placement of responsibility. There are concerns of what if (or when) sensitive information is exposed and when there is damage to a (former) student's reputation, and whose responsibility it is. What degree of responsibility should be placed on the teacher if Facebook, Google+, or Whisper was the SNS used? Perhaps initially the SNS provider is responsible for having a particular interaction paradigm that encouraged, elicited, or leaked the sensitive information. However, some may claim the teacher is responsible if he or she chose that particular service; and even if students voted to use a particular service, a vote is still a compromise between the available options the teacher presented under his or her purview. Is it the teacher's fault for choosing to do a particular activity on a particular medium (SNS instead of on paper)? Or, is it the teacher's fault for choosing a type of activity that elicited the information? Finally, is it the education institution's fault for not properly equipping and training the teacher and or the students? Consequently, since data breaches and lapses of security are almost inevitable (see Blyth, 2011), strategies or tactics must be used to protect student privacy and reputation for classroom SNS use. But the question remains, whose responsibility is it for teaching students (and staff) about digital privacy?

Classroom dynamics

A practical issue that relates directly to ELT is the effect of poor SNS privacy management on classroom dynamics. As stated, our students sacrifice some of their autonomy and dignity when practicing and using their English interlanguage in our classrooms. However, to do so requires a level of trust where others will keep in-class interactions and events private, and not post them onto the SNS record for the outside world to see, that is, unless there is little risk of repercussions. Already, for good classroom dynamics, teachers foster and encourage an environment of trust, but now we also need to instil a respect for other-people-privacy on SNSs. Roessler and Mokrosinska (2013, p. 771) say that "…privacy is an integral element of the dynamics of all social relationships."Additionally, "[w]hen individual privacy is threatened, this endangers not only individual freedom but also social relationships and practices…" (Roessler & Mokrosinska, 2013, p. 772), which can be assumed to be applicable to the classroom as well. Hadfield, a leading ELT teacher and author, wrote of one of her own classes, "… my own most miserable teaching experiences have been due to … a negative atmosphere that … built up in the group" (1992, p. 9).

Another practical aspect to consider is the students' internet literacy. SNS-based classroom activities typically require all students to use the same SNS, regardless of their levels of familiarity with the particular service. Lockely (2011) and Murray and Blyth (2011) reported on Japanese students' computer and internet literacy levels. In general, Japanese university students, in their first week of first year university classes report having very low levels of computer and internet literacy. Some students even claim to have never used a computer before. Instead, students seem to rely on the software that is available on their smartphones. Considering students' low internet fluency, some students will be able to start an activity and get it done relatively quickly, whilst many are still struggling with the SNS website. That is, before they can begin to plan the language they need to use for the task, and then consider strategies on how to complete it. Such students will be immediately behind the eight ball, which will likely affect the classroom dynamics.

Social media privacy strategies for classroom use

This section explores some examples of strategic use of SNS in the classroom that attempt to avoid negative events. Many readers will of course know other ideas, but only four can be considered, which are using pseudonyms, privacy settings, a teacher or institution created SNS, and education-oriented services. Additionally, to ensure that students (and some teachers) use privacy strategies, any such solutions to be offered to the teaching community must meet these criteria of privacy infallibility:

- be easily understood,
- easily implementable,
- realistic (people are likely to do with minimal coercion),
- ethical, and that
- personal information is safe and secure.

1. Pseudonyms

Teachers might suggest that students create a new account for foreign language learning with a pseudonym. It would seem obvious and uncontroversial, but not without practical

and competency concerns, aside from some SNS's pseudonym outing policies. Pseudonyms are fine for students who have easy computer access, or when smartphone apps like Twitter on iPhone or InstaPic (for Instragram) on Windows 8 allow for multiple accounts and easy switching between them. However, most smartphone apps only allow for one account at a time to be logged in; otherwise, the user would need to sign out, and then enter their other username and password (like Skype or Google+ on iPhone, and like the Twitter app on Windows 8). Having two accounts adds a new hurdle in that some people never remember their passwords. Even if a student makes a new Google+ account with a pseudonym, they are most likely to use the account that comes easiest to them, perhaps their Line account, or not bother signing out of their personal account and continue to use that for EFL classes anyway. Furthermore, in cases where some students do not have computers at home or a smartphone, access to the SNS is greatly reduced, effectively creating inequality among classmates.

Finally, most Japanese students only use their real names for SNS accounts. A brief survey of some of my own classes in 2014 revealed that almost all of my students used and preferred Line, a new Japanese SNS that has already replaced Mixi, and they almost always used their real names. Prior to our first class in the 2014 academic year, my first-year students were already using Line to find and interact with each other. Notably, in one of my classes, a girl had taken it upon herself to photograph the weekly homework list I wrote on the board, and she shared this photo with the rest of the class on Line (as seen below). This posting and sharing of homework was done by their own nous. Since my students were already interacting on Line, how could I ask them to create a new pseudonym account and use that instead? Inevitably, there will be a potential for outings with references to both real and pseudonym-accounts. Furthermore, using pseudonyms may be confusing when attempting to maintain real-world relations.

2. Privacy settings and behaviours

Using privacy settings relies on people bending to a company's interaction and privacy paradigms, and students being strategic on what and how information is treated; however, these can still fail. For instance, on Facebook, users are structurally bound to interact with other users on each other's walls or timelines in particular ways engineered by the company. In contrast, Google+ is like a social blog roll that allows for fine-grained control of privacy by posting to specific groups or users. In further contrast, Whisper allows for only short messages to be posted network wide, but are virtually anonymous. Consequently, within the rigid design of the SNS environment, users implement their own strategies for sharing information (or not).

There are strategies that our students can employ to mitigate privacy risks. Leigh Young & Quan-Haase (2013, p. 487–478) surveyed their Canadian university students to determine what privacy strategies they employ on Facebook, which our students could also implement. Firstly, it was found that 71% of users change the default privacy settings to "Friends Only" or "Some networks and all friends." Additionally,

- 79% regulated access to tagged photos
- 77% restricted access to their wall
- 71% limited access to their news feed
- 62% ignored unknown friends requests
- Some censor what photos are added

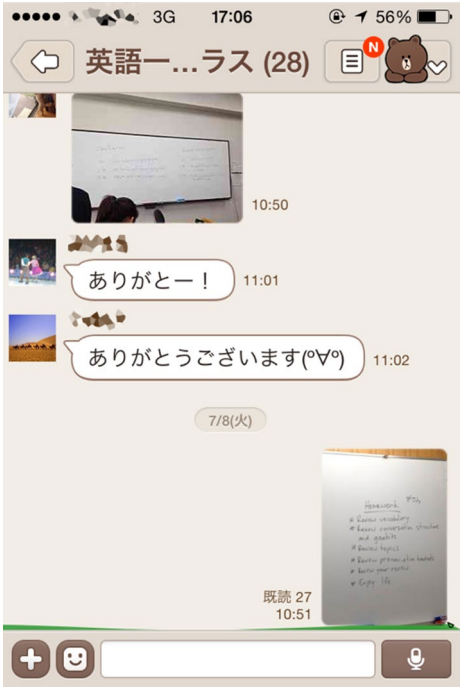

Figure 3. A screenshot of the Line group page for their class, where the photo of the homework is posted and discussions of my class are done. This shot was kindly provided by a student. Names in the image were pixelated.

- Some untag their names from certain photos
- Social privacy concerns affect friending practices, thus unknown people are not friended.

However, despite the final point, Lemieux (2012) claims a 72% success rate of university students on his North American campus who accepted an invented profile (a non-existent person) as a "Friend." In his study, he created a profile that was gender-ambiguous with the name of Jamie (which could be either male or female), and with a profile photo that appeared to be a romantic couple of both genders. He asked his class to all friend this fake profile, and begged them to keep it a secret that Jamie is non-existent, and asked them to allow "Jamie" to *friend* their friends. Consequently, 72% of friending requests of Jamie were accepted. This demonstrates that privacy strategies can fail, and that determined people of whatever motives can still gain access to personal networks and information.

3. Using a teacher or institution created SNS

There is SNS software that can be obtained and installed on the teacher's or institution's own website. These include Coppermine, Dolphin, Joomla, Moodle, PeoplePods, PHPBB forums, Sharetronix, Wiki, among many others. Since these software packages are probably completely unfamiliar to our students, implementing any one of these puts most students on a near-equal footing, in that they all have to familiarise themselves with the software first before they can begin to properly engage in language learning tasks. The advantage of using any one of these software packages is that virtually none of the outside community can access these educator-administered sites. Also, a teacher's or institution's own website can include a "do not list" instruction for the Google search engine indexing bot, effectively creating a dark-net. However, unlike Facebook, students' accounts can be accessed by website administrators who could actually know the students in real life. It must be remembered that many universities have harassment policies and committees because there is a history of teachers' misuse of privilege in many institutions. For instance, with PHPBB, administrators can access each person's account and profile and can change passwords, email addresses, read private messages, add or change posts, and so forth. Such administrator access is intended to assist regular members who had forgotten how to access their accounts, and for those with low internet literacy. This kind of access is ordinarily necessary; however, the administrators are usually geographically distant to the member, which greatly reduces the risk of the inappropriate access, though this will not be true in education.

For students, using such an in-house SNS is inauthentic. The community was created by the teacher or administration, and so the only users who access it are other students. Essentially, these are gated communities, as only certain people are granted, or bother to access it. Such gated communities lack a certain richness and variety that Facebook, Google+, Twitter, and others offer. Also, these gated communities are not permanent. Once the semester is over or a student's enrolment expires, so too their interactions and accounts. Additionally, the webhosting and domain may expire because the teacher fails to pay. Additionally, the teacher may lack the technical skill to adequately maintain the website software, or to maintain a minimum standard of security of databases like MySQL. Whatever the case may be, a Twitter feed will always appear more authentic and have more face value than an educator-created community.

4. Education-oriented websites

Though not widely known, companies like Educreations, Go Soapbox, Padlet, and Socrative (reported by Tolosa, 2014) offer a better fit for pedagogical needs and some privacy. The interaction paradigm does not encourage a sharing or over-sharing of personal information, but instead is a display of task output. Padlet will be discussed as an example of education oriented websites.

On Padlet, a group of students can be asked to collaborate to make a page of content on a theme, such as a cake recipe with pictorial directions, or a wall of information about a graded reader used in a series of classes. With Padlet, only generic computer literacy skills are required, so work can easily be done in groups, and there is a diffusion of responsibility and accountability (especially good for overcoming any anxiety in displaying interlanguage). Additionally, there is a democratic agreement of content to be displayed (reducing

the teacher's accountability) on Padlet. In contrast, Facebook, Moodle, and PHPBB encourage a solitary online task engagement. Whereas, pedagogical advantages of Padlet include a Vygotskian type of collaborative learning, social construction of knowledge, and developing workplace related communicative competencies because of the group-work nature of tasks. Additionally, Cooperative Learning theory suggests students gain more academically and productively from collaboration (Kagan & Kagan, 2009, cited in Sakurai, 2015), and promotes improved social relations and social skills in classes (Sakurai, 2015). Furthermore, Padlet allows for a variety of levels of privacy from most private to very public. In terms of risks posed to students, Padlet profile information is very minimal, requiring only a username, name, and email address, all of which teachers do not have access to. The choice of pedagogical task is, of course, burdened on the teacher, but the students through democratic agreement take responsibility for the content. The tasks in this interaction paradigm can appear to be more related to the display of information within a vocational setting, improving the face value of it over a teacher-created SNS. However, for data protection, little is known about Padlet's security, and many companies do not report security breaches anyway (Privacy Rights Clearinghouse, 2011). Admittedly, this option does not address developing SNS privacy skills or learning about other-people privacy that Ferrari (2013) says students need, thus deferring immediate risk from teachers.

For further discussion

As previously explained, there are some important aspects regarding the ethical use of SNS in the EFL classroom. These include information management, identity, privacy, and classroom dynamics. To manage these and other issues, strategies for safeguarding students' current and future reputations are needed. Though four examples of privacy strategies were offered, these failed the five simple criteria of privacy infallibility. Consequently, we are still at step three in the model of reducing negative events (see Figure 2). Therefore, it would be inappropriate to end this article with a conclusion; instead, a question is required. What other SNS privacy strategies can we offer our colleagues and students?

Notes

1. Prior to initial submission of this article, Facebook had a policy of using real names only; however, this policy has since been revoked.

Acknowledgements

Sincere gratitude and appreciation is extended to the editor and the reviewers, whose tireless efforts have contributed immensely to make this paper the best it could be.

References

Blyth, A. (2011). Cookies and breadcrumbs: Ethical issues in CALL. *ELT Journal*, *65*(4), 470–472.

Ferrari, A. (2013). *DIGCOMP: A framework for developing and understanding digital competence in Europe*. Seville, Spain: European Commission.

Geddes, L. (2014, September 21). Does sharing photos of your children on Facebook put them at risk? *The Guardian*. Retrieved from www.theguardian.com/technology/2014/sep/21/children-privacy-online-facebook-photos

Hadfield, J. (1992). *Classroom dynamics*. Oxford, UK: Oxford University Press.

Hyland, K. (2009). *Teaching and researching writing*. Harlow, UK: Pearson Education Limited.

Kayyali, N., & York, J. (2014). Facebook's 'real name' policy can cause real-world harm for the LGBTQ community. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2014/09/facebooks-real-name-policy-can-cause-real-world-harm-lgbtq-community

Leigh Young, A., and Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The internet privacy paradox revisited. *Information, Communication, and Society*, *16*(4), 479–500.

Lemieux, R. (2012). Fictional privacy among Facebook users. *Psychological Reports: Relations and Communication*, *111*(1), 289–292.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, *14*(1), 79–100.

Lockley, T. (2011). Japanese students' experience of ICT and other technology prior to university: A survey. *The JALT CALL Journal*, *7*(1), 93–102.

Maden, M., & Smith, A. (2010). Reputation management and social media: How people monitor their identity and search for others online. *Pew Research Internet Project*. Retrieved from http://pewinternet.org/Reports/2010/Reputation-Management.aspx

Murray, A., & Blyth, A. (2011). A survey of Japanese university students' computer literacy levels. *The JALT CALL Journal*, *7*(3), 307–318.

Nippert-Eng, C. (2010). *Islands of privacy*. Chicago: University of Chicago Press.

Palis, C. (2012, April 6). 7 Creepy apps that will make you paranoid about your privacy. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2012/04/06/creepy-apps_n_1403268.html

Privacy Rights Clearinghouse (2011). *Data breaches: A year in review*. Retrieved from https://www.privacyrights.org/top-data-breach-list-2011

Roessler, B., & Mokrosinska, D. (2013) Privacy and social interaction. *Philosophy and Social Criticism*, *39*(8), 771–791.

Sakurai, Y. (2015). Implementing cooperative learning in EFL reading classes at a Japanese university. *Language and Culture: Bulletin of the Institute for Language Education*, *32*, 59–73.

Tolosa, C. (2014). Mobile technology tasks in initial language teacher education. *One World Many Languages*. Paper presented at AILA World Congress 2014, Brisbane Australia, 10–15th August.

Author biodata

Andrew Blyth is a doctoral student with the University of Canberra, Australia, where he studies applying psycholinguistic listening theories to ELT, and has an interest in social media ethics. He also teaches EFL and TEFL at various universities in Nagoya, Japan.