Managing Your Digital Footprint: Ostriches v. Eagles

Julia Hengstler

> *You were qualified, they could afford you, and they needed you. So why didn't they hire you? They didn't want to tell you, but your boss-to-be rejected you because of the best kegger of your senior year. She saw the photo with the sorority girl with — is that a tattoo…straddling you as you spray Heineken all over her. – Douglas (2007, ¶1)*

> *Generally speaking, professors [and teachers] don't do as much boozing and carousing as students, so they may have fewer embarrassing photographs to post online. But … [they] do have plenty of colorful things to say about their students and colleagues, and social networks offer new ways for those catty comments to fall into the wrong hands. - Young (2009, When Professors Say too Much section)*

> *More than 95% of district administrators said that Web 2.0 will require a new type of teacher training… and 79% said that schools should take full responsibility for modeling… Yet only 44% reported taking full responsibility for the restructuring of schools to accommodate Web 2.0. - Lemke, Coughlin, Garcia, Reifsneider, & Baas (2009, p. 8)*

Learning Objectives

After completing this chapter, you should be able to:

- Describe the differences between 'ostriches' and 'eagles' as metaphors for approaches to managing digital footprints.
- Describe why educators should be 'eagles' rather than 'ostriches'.
- Explain the terms Web 2.0, social networking, and digital footprint.
- Explain the importance of digital footprints to educators.
- Explain the difference between the surface web & deep web.

- Explain the fundamental mechanics of how social networking functions.
- Describe Twitter and how it works.
- Explain some issues of professionalism and how they relate to digital footprints, Web 2.0 & social networking (e.g. blurring of personal and professional boundaries & professional responsibilities of educators).
- Describe the "creepy treehouse" & how to avoid it.
- Explain how ignorance of Web 2.0 and social networking can negatively impact your professional reputation.
- Cite cautionary examples of digital footprint issues and cyberbullying of students and educators.
- Explain the importance of guidelines to manage your digital footprint as well as use Web 2.0 & social networking technologies.
- Locate and cite some examples of some guidelines.
- Demonstrate understanding that blocking and/or banning of Web 2.0 and social networking technology is not an effective solution to risk management for educational professionals or students.
- Explain methods to monitor your digital footprint.
- Explain methods to create a positive digital footprint, and manage networks to protect your digital footprint and professional reputation.
- Explain a developmentally appropriate model to scaffold student use of Web 2.0 and social networking technologies and the educator's role.
- Explain how to defend your reputation and digital footprint when under attack.

Introduction

Over the last several years, with the rise of Web 2.0 and explosion in social networking (Facebook, Twitter, etc.), I have worked to heighten awareness about the potential of Web 2.0 and social networking technologies for education and the critical task of managing digital footprints—traces of a person's online activities. From a professional perspective the two must go hand in hand. As we are exposing more of ourselves online—and others are exposing us—powerful search engines like Google and identity aggregation services like CVgadget, Spokeo, and Pipl are developing intelligent tools that allow others to profile us. This convergence of content and aggregation capabilities affects educational opportunities, employment opportunities, relationships and more—some for the better and others for worse. In response, we are seeing the emergence of online reputation management as a business as evidenced by Trackur, ReputationDefender and Lookuppage. (I tried Trackur's free trial and was amazed at the amount of relevant data it was able to compile on me.)

As we expand our use of technology, reports of small and large faux pas affecting the lives of students, educators, and others increase. From my perspective, the generation gap in social networking use contributes significantly to the problem. Children, youth and young adults were among the early adopters of these technologies and learned how to use them from each other—compounding their limited wisdom. Technology community 'elders'—you, me, other adults with technical savvy and life experience—were doing little as a

community to provide scaffolding. We were not sharing the long range perspective –as only mature adults can—to help younger people understand the potential impact of sharing personal information with the world—often with little to no content filtering:

> [Many] students today have been using social networking sites since they were teens…It's been talked about, but there really hasn't been a concerted effort by churches, schools, social organizations to really teach people how to use these tools appropriately and inappropriately. (Dolan, 2009, What's going online section, ¶8)

As I immersed myself further in these technologies—especially Twitter—it became clear that a lack of knowledge regarding how the mechanics of social networking function, combined with a variety of unadvised or unwitting personal disclosures and an ignorance that the world was watching and finding people's content, caused similar issues to surface again and again—no matter the age of the person in question. During my research, I also discovered a surprising scarcity of data regarding cyber-bullying of adults—especially teachers, administrators, and post-secondary faculty when compared to the data on children and youth. Further, there are few examples of school or institutional policies that proactively manage and scaffold use of Web 2.0 and social networking technologies—beyond blocking and banning. K-12 schools, school districts, and school boards in North America and abroad are struggling with sound ways to incorporate these technologies in safe and responsible ways. The 2009 Consortium for School Networking US research study, "Leadership for Web 2.0 in Education: Promise and Reality Report" was one of the first attempts to benchmark Web 2.0 practice and policy (Lemke, C., Coughlin, E., Garcia, L., Reifsneider, D., & Baas, J., 2009). It provided a useful snapshot of the state of Web 2.0 use, attitudes and policies in American K-12 schools. Foundational elements of this process are policy, protocol and procedural development for students and faculty. Similar issues are emerging at the post-secondary level. People who are knowledgeable and use these technologies responsibly need to be in the forefront of these discussions.

Many individuals and educational groups are like ostriches—ignoring any educational applications of these technologies due to fear. By taking a passive role—especially with regard to their own reputations—these educators and groups put themselves at risk. Think about the ostrich with its head in the sand. Where is the bulk of the bird? Exposed to predators. On the other hand, some schools, districts and organizations are proactively working to manage the risks by providing resources, guidelines, structures, life-skills training and professional development to leverage the abilities of these tools to improve teaching and learning. These proactive groups are the "eagles". "Leadership for Web 2.0 in Education: Promise and Reality Report" (Lemke et al., 2009) indicated that many of these eagles are teachers—the early adopters pushing the boundaries of administration to keep pace. While many US superintendents and curriculum directors acknowledge the potential of Web 2.0 and social networking tools, they have limited to no experience with the tools, and little research to rely on for practice—let alone better or best practices (Lemke et al., 2009). Where progressive policies are in place, they provide support to educators for scaffolding students' responsible use of this technology in ways that contribute to community—be it classroom, school, town, nation or globe. They also scaffold educators' use of this technology to further allow them to contribute to their profession. Eagles also

see the public relations potential in these technologies. After all, Web 2.0 is what we, the users, make of it. All of us have something worth contributing—one of the underpinnings of 21st Century learning.

Educators are in positions of trust in our communities. As educators we can no longer be ostriches ignoring the implications of what we say about ourselves—or others—online. Further, we can't ignore what others say about us. We need to model sound practice in managing digital footprints. We need eagle eyes to survey our digital environments and respond to needs and threats. Regardless of whether educators decide to actively manage their own digital footprint, they have a moral responsibility to teach students how to manage their digital footprints to protect and hopefully expand the students' future opportunities. I strongly believe in the potential of Web 2.0 technologies—including social networking—to engage learners and educators in thoughtful, generative, collaborative, and horizon-stretching activities. To reach this potential, it is critical to support the development of personally, socially and morally responsible cybercitizens who can manage their own digital identities in ways that will create more opportunities for rather than less—irrespective of age. This chapter is not about instructional applications of these technologies, but how to personally and professionally manage our participation in them to minimize errors and maximize opportunities.

N. B.: The Web 2.0 and social networking policies referenced in this chapter were caught as snapshots in time. Policies continue to emerge and evolve. What was policy for a district or institution at the time of this writing, may be considerably different from existing policy.

Architecture of Participation

The internet and its use is in the midst of the shift from pushing content (information, software programs, etc.) out to users by experts and groups, to a participatory model where virtually any user can create and collaborate with others to develop content. This approach requires a modular design scheme where participants can add their pieces or create new ones that can integrate with pre-existing material—all while still leaving room for future contributions. O'Reilly (2005, p. 3) referred to this as "The Architecture of Participation." This modular design model encouraged networked participation: people collaborated in development; each person had the potential to contribute value through comment, feedback, or development. O'Reilly (2005, p. 3) went on to write, "One of the key lessons of the Web 2.0 era is this: Users add value."

Social networking sites and services were natural outgrowths of O'Reilly's "Architecture of Participation." In social networking, sites or services provide a vehicle for users to build a community of members interested in a common thing—whether that thing is their relationship to one another, a project, a certain movie/actor/author, interest in a school, a hobby, etc. Users may discover the site or service and become "members" or they may be invited by existing members—generally by someone known to them.

The "Architecture of Participation" is a powerful metaphor in that it encompasses both the contributions of people to development, as well as the underlying structural model making contributions possible. Rather organically, these two aspects facilitated the development of online human networks. Initially, the common Internet was more a 'consumer' model where content was consumed by users and controlled and produced by a few. As businesses

joined the web, companies would track user downloads, visits to their sites and resources as well as users' demographic or payment information. The major concerns during this time were: 1) "cookies"; 2) security of a person's demographic and payment data; 3) email issues like spam and phishing.

With the shift toward collaboration, creation and contribution on the web, people began to share online content in large numbers and in a variety of areas—software code, blogs, personal information, etc. Digital footprints expanded in depth and scope. As the PEW Internet & American Life Project report, "Digital Footprints" (Madden, Fox, Smith, & Vitak, 2007), pointed out, current users' digital footprints cover details of their personal lives that would have taken a private investigator months to compile just a few years ago—people blog about their lives including photos and videos; their social networking profiles detail their interests, hobbies, histories, friends, family connections and employment; images and videos on repositories like Flickr and YouTube are tagged with names, places, dates and more. As the report stated, "People are not just findable, they are knowable" (Madden et al., 2007, The Nature of Personal Information is Changing in the Age of Web 2.0 section). As I mentioned earlier, contribution is not enough to make people 'knowable' in terms of the PEW Internet & American Life Project report. "Knowability" requires tools to collect data about you.

The PEW Internet & American Life Project report (Madden et al., 2007) further defined 2 segments of a person's digital footprint: 1) an active footprint—referring to the data created by a person's voluntary contributions to the web like blogs, comments, Facebook pages, images on Flickr; and 2) a passive footprint—the data that is collected about a person like cookies or the browsing history on a computer. Passive information is data that other people or organizations collect about you (Madden et al., 2007). Since 2007 when the report was written, the explosion in use of social media and Web 2.0 platforms calls for a third type of digital footprint: one I've begun to call a 'second-hand' digital footprint. Second-hand digital footprints are comprised of data that others deliberately share about you. That shared data may be about your online or off-line behavior. Second-hand digital footprints may be consensual. For example, you might write an article in hard copy that a colleague asks to publish on her blog—and you agree. Second-hand digital footprints may be non-consensual like when students post videos of a teacher captured on an iPhone during class on YouTube without the teacher's permission. In the past, this body of information remained relatively disaggregated. It used to be difficult for a person or organization to assemble it to develop a detailed profile of an individual—to "know" you. Think of disaggregated information like living in a big city. While various people in the city might have small bits of information about you—your favourite dishes at a restaurant, where you bank, where your children go to school, etc.— a detective would have to interview them all to create a profile of you.

As Google reached maturity as a dynamic search engine and metadata (keywords and phrases that describe the content of online materials—data about data) became prevalent, Google became a powerful tool to aggregate information about people. "Googling yourself"—or searching variants of your name on Google to see what can be discovered about you—became a common practice. As Beal (2008) stated, "Google's not just a search engine, it's a reputation engine" (Build Your Google Reputation Now Not Later section).

Simpson (2008) writing for NEA Today pointed out:

> …thanks to advances in technology…post your racy photos, sexually graphic writings, or wild party stories on a personal Web blog. You'll be amazed by how quickly tech-savvy students can disseminate your postings to their friends and your employer. (¶3)

The Deep Web

While the practice of "Googling yourself" is becoming more common, Google only scratches the surface. It is estimated that the "deep" or "dark" web contains the bulk of information currently available and accessible online:

> Searching on the Internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth of information that is deep, and therefore, missed. The reason is simple: Most of the Web's information is buried far down on dynamically generated sites, and standard search engines never find it...The deep Web is qualitatively different from the surface Web. Deep Web sources store their content in searchable databases that only produce results dynamically in response to a direct request. But a direct query is a "one at a time" laborious way to search. (Bergman, 2001, ¶1-3)

Current data on the extent of the deep web is hard to find. Some statistics reported in a widely cited industry whitepaper made the following claims about the deep web:

- It contains 400 to 550 times more public information than surface web (that which we commonly call the "World Wide Web").
  - 7,500 terabytes of information versus 19 terabytes on the surface web.
  - Approximately 550 billion individual documents vs. 1 billion in surface Web.
  - 60 of the largest deep Web sites collectively contain about 750 terabytes of information — sufficient by themselves to exceed the size of the surface Web by 40 times.
- 95% of the deep web is publicly accessible information — not subject to fees or subscriptions.
  - Greater than 50% of content resides in topic specific databases.
- An estimated 200,000 deep Web sites exist.
  - Sites are narrower with deeper content.
  - Deep sites are more highly linked to than surface sites.
  - Deep sites receive about 50% greater monthly traffic than surface sites.
- It is the largest growing category of new information on the Internet. (Bergman, 2001)

When Bergman shared his data estimates for the deep web, they were questioned. As a result of the responses to his initial estimates, Bergman (2007) questioned the 2001 data himself saying "…while awareness of the qualitative nature of Web content has grown tremendously in the past near-decade, our quantitative understanding remains weak" (So What is the Quantitative Update section). That said, Bergman (2007) pointed out that while original numbers may have overestimated content at that time, data on the growth of the deep web in 2001-2004 indicates that the original estimates may more closely approximate the current numbers when combined with previously unindexed files and non-English content. Similarly, in 2007, Shestakov & Salakoski theorized that estimates of deep web content have been predominantly based on English language content and that the numbers did not consider the rising sector of non-English deep web content. Any way you slice it, the amount of publicly accessible information via the deep web is truly staggering and if your data is in a database somewhere, that information about you could be publicly available. The more that you do or contribute in the way of digital information via the web, the more likely it is that additional information about you will be publicly available if someone knows where and how to look for it. If you want to move beyond Googling yourself, it is worthwhile to take a look at tools like CVgadget, Spokeo, Pipl, Trackur, ReputationDefender and Lookuppage.

Social Networking

From its inception by military and scientific interests to its current state, the Internet is and always has been a network used by people and organizations to connect and exchange information. Although some features and functions of social networking emerged as early as the late 70's to early 80's with bulletin board systems (Nickson, 2009), it was the explosion of social networking from the mid 1990's to the early 2000's and the emerging power of internet search engines like Google that brought the issue of digital footprints to the forefront in popular culture. While the architecture and concept of contemporary social networking platforms first emerged in 1996 with Sixdegrees.com. The original site is now defunct though it was functional from 1997-2001 (Wikipedia, 2010). This service did not take-off until 2002-2003 with the appearance of sites like Friendster, MySpace, LinkedIn and Bebo (Wikipedia, 2011). Facebook, perhaps one of the most widely known social networking services, debuted in 2004 (Yadav, 2006). Social networking sites were set up to encourage the sharing of personal information either with defined networks or the world at large. It was not unexpected that these social networking services sought to create a profit model based on their membership. For the services, the value is in the user base, and the data it contains.

The Fundamental Mechanics of Social Networking

Many users had—and continue to have—a fundamental ignorance of how the content they contribute is distributed and replicated through many Web 2.0 services. This distribution model gives permanence to the contributed content even if a user deletes the original copy. It is this last aspect that can cause grief to many people. It is amazing that even very technologically savvy users seem blind to this fact. Twitter is a good example of the fundamental mechanics of social networking. It is critically important that you understand the fundamental mechanics as I outline them here. The reason it is so important is that this type of architecture underlies most social networking and Web 2.0 technologies to a greater

or lesser extent. If you understand the fundamental mechanics of social networking, it will go a long way to avoiding social media tragedies. In fact, when I do presentations, I often say, "If you take just one thing away from this today, it must be the understanding of the fundamental mechanics of social networking."

Twitter As An Example

Twitter is a micro-blogging platform where users can publish posts of up to 140 characters at a time. If your Twitter account is public, anyone can follow your content via a webpage generated by the service. For example, without a Twitter account you can still see what I post in Twitter simply by visiting a link generated by the site/service: http://www.twitter.com/jhengstler. This site will only show the posts I have made—not any of the content from people to whom I subscribe. Once you have a Twitter account, you can have two roles: you can passively receive others' posts by a type of subscription (this is called "following" and makes you someone's "follower"), or you can actively generate and publish your own posts to other interested users (here other users are "following" you, they are your "followers"). With a Twitter account, you only receive posts of the people you directly follow. For example, if you follow me, you'll see what I actively post but you won't see the content I receive from the users I follow—unless, of course, we follow the same users. I write something—post a tweet—it appears in my account and is then instantaneously replicated in the accounts of anyone following me.

Content posted by a user in Twitter falls into 4 general categories:

- tweets: original posts by a Twitter user of 140 characters or less that are seen by the user's followers and on the webpage version of any public accounts.
- retweets: republishing of another user's tweets with attribution to the original author on Twitter; a retweeted message is usually prefaced by "RT" to denote that it is a retweet followed by the contributor's Twitter account name; attribution may be multilayered to indicate the path the original tweet traveled to reach the reader; a RT is visible to followers and on the webpage version of any public accounts.
- replies: original post of 140 characters or less directed to a particular Twitter user; replies can help structure a conversation thread; you don't have to follow someone to reply to them; usually prefaced by "@" followed by the username of the person to whom its addressed i.e. "@jhengstler"; many Twitter clients allow users to monitor replies regardless of whether you are following the person who posted the reply; replies can be a way to contact people who are not following you; a reply is visible to followers and on the webpage version of any public accounts.
- direct messages: original posts by a Twitter user to another user that are considered "private" communication; a direct message is usually prefaced by "D" or "DM"; users may only direct message users who are following them; a DM is not visible to followers or on the webpage version of any public accounts unless the recipient violates the assumption of privacy and retweets the content or otherwise copies and shares it or the author retweets it; it is very important to understand that the privacy of such direct messages can only be assumed and never assured; privacy of direct messages hinges on an honour system between sender and receiver.

The replication and transmission of my tweet to you in my network of followers can be repeated in an exponential model of publication and transmission. I tweet and you receive it. Next, you retweet it to your followers. They, in turn, retweet it to their followers, and so on. This potential for exponential reproduction is critical in understanding the impact and scope a single tweet from a single user can have. This exponential power of a tweet is determined by the number and the extent of interrelated networks a tweet can travel. Imagine your single tweet as a person standing in a hall of mirrors with reflection upon reflection being created. The only difference between the hall of mirrors and Twitter is that in the real hall if you step out, the reflections of you cease. In Twitter, however, even if we remove the original tweet generating the reflections, the reflections themselves—and their potential for more duplication and transmission—remain in the networks still carrying them. This is why we must be conscious of what we tweet and how it can be perceived. As many social networking services and Web 2.0 technologies are fundamentally similar in their potential for exponential publication and transmission, ignorance of how they work through networks of networks is the cause of many social networking faux pas.

There Are No "Take Backs" in Social Networking

A while ago, I was at an educational technology conference. I was following a presenter on Twitter—someone I consider to be on the leading edge of educational technology use. At the time he had more than 1000 people who followed him. During the conference, the presenter tweeted a piece of information about an important educational technology person—also at the conference. The information was highly interesting. I thought the information would be of interest to my followers so, assuming that most of my followers were not following the presenter, I retweeted it. I had about 400 followers at that time. The retweet contained the attribution to the original author—the presenter—as it generally does. The time that elapsed between the original tweet from the presenter and my retweet was about 1 minute or less. (I could reflect on this timeframe because tweets are stamped with dates and times.) Within minutes of my retweet, I received a direct message from the presenter who wrote it. He asked me to delete it. I can only guess that the person referenced in the tweet contacted the presenter after discovering the message was circulating. Apparently, the content of that conversation had been considered part of a privileged communication. In requesting that I delete my tweet—just a retweet of the presenter's—it was clear to me that the presenter did not understand the basic mechanics of Twitter—and most social networking services. This is why a lack of understanding of the fundamental mechanics of social networking can cause problems for users.

The model of exponential publication and transmissions means that once tweeted—or otherwise published in a social network—there are no 'take-backs". I direct messaged the presenter that while I could delete my message, I was just one small part of the process. My deletion would not affect the duplicates of that message that had been sent out to my 400+ followers. They would retain their copies. In addition, I pointed out that the presenter had significantly more followers than I, and he—and his network—would likely have many more transmissions and replications to worry about. What my deletion would assure is that anyone who became part of my network after I deleted the original would not see the message—from me. This would not prevent people who had the message already from retweeting it at will. People who do not grasp these fundamental mechanics may continue to make these types of inadvertent errors that may damage relationships as well as careers.

Websites Mentioned in this Section

- Bebo: http://www.bebo.com
- CVgadget: http://www.cvgadget.com
- Facebook: http://www.facebook.com
- Flickr: http://www.flickr.com
- Friendster: http://www.friendster.com
- Google: http://www.google.com
- Jhengstler's Twitter: http://www.twitter.com/jhengstler
- LinkedIn: http://www.linkedin.com/
- Lookuppage: http://www.lookuppage.com
- MySpace: http://www.myspace.com
- PEW Internet & American Life Project: http://www.pewinternet.org
- Pipl: http://www.pipl.com
- ReputationDefender: http://www.reputationdefender.com
- Sixdegrees.com: original site/service now defunct though a new company is using the URL
- Spokeo: http://www.spokeo.com
- Trackur: http://www.trackur.com
- Twitter: http://www.twitter.com
- YouTube: http://www.youtube.com

Digital Footprint = Reputation

Professional Standards & Private Persona

As web technologies and social networking in particular have been on the rise, adoption of these in education as a whole has lagged behind that of business and government. One complication is that educators—like other employees in positions of public trust—are held to higher standards than the general population. In 1987, the British Columbia Court of Appeal (Canada) found that

> Teachers must maintain the confidence and respect of their superiors, their peers, and in particular, the students, and those who send their children to our public schools. Teachers must not only be competent but they are expected to lead by example. Any loss of confidence or respect will impair the system, and have an adverse effect upon those who maintain a standard of behaviour which most other citizens need not observe because they do not have such public responsibilities to fulfill. (Shewan v. Board School Trustees of School District #34 (Abbotsford), p. 7)

Similarly, "Facebook 101" (2007) from British Columbia's College of Teachers (British Columbia, Canada) reminded teachers that navigating the blurry lines separating personal and professional lives has always been a professional consideration resulting from the profession's position of public trust:

> An educator's responsibilities as a professional extend beyond the end of the day when his or her duties as an employee are over. Educators have always keenly understood that their responsibilities to ensure the well-being of children reach far beyond the classroom. (p. 13)

Another contributing factor is that our cultural sense of privacy is changing. This has been recognized by a number of authors:

- As the lines between public and private behavior continue to blur, we find ourselves living in a time of sublime cultural confusion. Consciously or unconsciously, we're playing out that struggle on the pages of Facebook. (Martin, M., 2008, ¶23)
- But the larger problem is that the norms of the virtual world are starting to bleed into the real world. The constant availability of 'private' information has reset the social-interaction bar at a much higher level: More personal data are required to feel a sense of normalcy…Does this mean that constructing authenticity in your professional relations now requires higher levels of social interaction and the proffering of more information? (Park, 2009, ¶6)

What Ostriches Do: Cautionary Tales

Educators Exposed as Ostriches

Combine the rising use of Web 2.0 and social networking, a lack of professional scaffolding for educators, shifting privacy norms, ubiquitous access to the technology with powerful search engines and you have a recipe for disaster. In my personal discussions with school administrators and professional organizations in British Columbia, Canada, it is evident that situations are occurring with regard to professional misuse of Web 2.0 and social networking. Unfortunately, these situations are being handled internally within a school or district, or quietly handled through professional organizations. As a result, they are being kept from the public eye. While it is appropriate to handle certain matters internally and protect people's privacy, lack of exposure can prevent others from determining the scope of the issues and the practices by which such issues can be handled. Such incidents could be stripped of identifying data and used to generate useful case studies. In my review of the available research, I have discovered that there is little organized data or analyses available to the public regarding professional faux pas/misuse of technology in education. Most of what the public can access is anecdotal reporting by media and certain professional organizations. I believe the underreporting of these incidents through more formal channels or mass media—especially in countries like Canada—masks the scope and severity of the mistakes being made by educators.

In my observation, there are generally four classes of Web 2.0 and social networking misuse:

- Not thinking it through: no reflection on content being posted or the implications; makes you ask "What were you thinking?"
- Plain bad choices: Posting content beyond questionable, where you might ask "Were you thinking when you did this or under the influence of something?"
- Leading a double life: posting content under an alias assuming it will never be tied to your professional identity.
- Multiple infractions: any combination of the above.

N.B.: This section takes a sensational approach to professional faux pas and misuse in an effort to shake educators and administrators out of their apathy regarding professional preparation, policy and practice for Web 2.0 and social networking. Too often we think, "Practicing professionals wouldn't do that" and yet they do. They then regret it, but as we know from the fundamental mechanics of social networking, there are no 'take-backs'. The best defense against these mistakes is professional preparation, policy, and practice, but often it takes serious situations to prompt these more formal interventions. My hope is that these cautionary tales might move us to a more proactive approach without the need for more 'serious situations' to occur.

Mistakes & Impacts

In 2007, WCNC reporter, Jeff Campbell in Charlotte (North Carolina) shone a light on a number of teachers' questionable Facebook postings. One teacher was suspended without pay. Another teacher who posted that she enjoyed drinking and "teaching chitlins in the ghetto of Charlotte" faced firing. Other instances involved female teachers posting images of themselves in "sexually suggestive poses" and a special education teacher posting, "I'm feeling p—ed because I hate my students!" (Helms, 2008). More American examples are shared in the National Education Association's, "The Whole World Wide Web is Watching" (2008). In Broward County, Florida in 2007, Band Director, Scott Davis created a MySpace profile, posted content regarding sex, drugs & depression. The school officials were alerted. In Ohio during the same year, reporters investigated Ohio teachers. They found a MySpace profile of a 25 year old teacher who publicly describes herself as "an aggressive freak in bed," "sexy," and "outstanding kisser". Another teacher's profile referred to getting drunk, taking drugs, and going skinny-dipping (National Education Association, 2008, ¶1).

Across the continent, one of the few high-profile Canadian cases involved Mark Classen, a principal at Harrison Hot Springs Elementary (British Columbia). Classen went on a trip to New Zealand in 2007. While there, his wife took a photo of him—nude—on the beach. The photo was posted to his personal website, a link got to a parent, and caused a local media circus. Classen went on paid leave, was disciplined, and eventually reinstated (CTV News, 2007).

In May 2009, a secondary teacher and head of the Language Department in Argyll and Bute, Scotland, was investigated when a parent complained about the nature and frequency of her tweets in Twitter. For example, one Tweet read, "Have three Asperger's boys in S1 class: never a dull moment! Always offer an interesting take on things" (Kemp, 2009, ¶3).

Investigations estimated that the teacher was tweeting 20 times a day, "on average once every 40 minutes" (Athow, 2009, ¶3).

Teaching level does not seem to be a barrier to poor filtering of content professionals post on Facebook. Perhaps one of the highest profile examples is the December 2008 postings of Professor Reiko Ohnuma, Dartmouth University, New Hampshire. Ohnuma created a Facebook profile and thought only her "friends" could see her content. In actuality, her content was public. A student found Ohnuma's Facebook page and found posts like:

- "Reiko is co-teaching this term with a black colleague…whose mind is no longer on the stupid class."
- "Reiko has nothing interesting to say about these damn papers, but better think of something quick."
- "someday when i am chair, we're all going to JOG IN PLACE throughout the meeting. This should knock out at least half of the faculty within 10 minutes (especially the blowhards) & then the meeting can be ended in a timely manner."
- "Reiko faked it with aplomb."
- "yeah, but i feel like such a fraud...do you think dartmouth parents would be upset about paying $40,000 a year for their children to go here if they knew that certain professors were looking up stuff on Wikipedia and asking for advice from their Facebook friends on the night before the lecture?" (Edgar, 2008)

After word of the content leaked, Ohnuma restricted access or closed the account; however, the screen captures were published in the school's blog, Dartlog. Ivy Gate, an online blog dedicated to doings in the American Ivy League Schools published the story under the heading, "Dartmouth Religion Professor Apparently Clueless About the Perils of Facebook" (Yu, 2008). R. Green, the acting Religion Department Chair at the time, defended Ohnuma stating,

> 'We understood the context of this…She's an excellent teacher—we know her to be an individual prone to humor and irony, and we're not surprised.' He went on to say, he 'considered his colleague brave to even venture into social networking,' calling her Facebook use 'an indication of Reiko's youth and vitality.' (Young, 2009, When Professors Say Too Much section, ¶3)

Communication technologies that pre-date social networking and Web 2.0 can also impact your digital footprint. Email has been around on the modern internet since 1971 and came into popular use in the mid 1970's (Peter, 2004). On the surface, email seems an innocuous platform. If you don't want the email—you simply "Delete" it. Yet, most of you are probably familiar with someone who pressed "Reply to All" instead of "Reply" sending a sensitive email message to places it shouldn't have gone. In my career as a student and as a high school teacher I was on the receiving end of two of these.

My first eye opening experience was while I was taking a graduate course. The course had a strong technology base, as did the instructors. While working online late one evening

with a fellow student, I received an email from one of my instructors. The email opened with a salutation to the dean of the faculty. When I read it, I was aghast to find that the instructor claimed I accused him of stealing an idea of mine. He then went on to claim I was evidencing 'disruptive' behavior in the face-to-face environment. The instructor had intended to send the email to the dean of the faculty in which I was taking the course—to what end I can only imagine. I shared this with my fellow student—as well as my stupefaction—because none of the content was true. As I sat instant messaging with my fellow student, I received a request for a message "recall." I had never heard of a recall even though I had been using email for several years. My fellow student explained to me that Outlook had the ability to recall a message the sender had already sent—as long as it hadn't been opened. Unfortunately for the instructor, I had already opened the email. I was able to forward my copy of the email on to the dean stating my concerns over this instructor's claims. The matter went up to the institution's highest administrative levels, but was eventually resolved to my satisfaction. That series of events opened my eyes about the permanence of email messages and the need to review to whom your emails are addressed before sending.

During my career I have often had respectful disagreements with colleagues over philosophical, pedagogical, or other approaches. Sometimes colleagues can be less than respectful in their disagreement. One school in which I worked had an internal email system. A discussion about a semi-controversial topic ensued on email, but during the exchanges, one of my colleagues sent me a rather scathing email. My first reaction was to move the email to a special folder and copy it. My next move was to send the teacher a polite email saying, "X, Are you sure that this is what you intended to say at the time you wrote it?" He quickly responded with a retraction. I never received another email like that again. Had I been less than professional, had I wanted to cause issues for this colleague, I could have sent this email on to others. I never did, but this ability brings me to a very crucial point about email or so called "private" messages like direct messaging in Twitter, internal messaging on Facebook, etc. Privacy of content is an assumption. It is a matter of understanding between the sender and the receiver. There is no assurance that the receiver will not copy and paste the material, broadcast it to his or her network at will—no matter what footer you may put on the bottom of a message stating that the content is confidential and only for the use of the recipient. If you think email issues are a thing of the past, as recently as October 2010, a dean at the University of Missouri in the United States accidentally broadcast an email with sensitive information about a student suffering from "mental distress" to the schools 6,000 graduate students by clicking "Reply All" (Carter, 2010).

Beyond email, just keeping personal data on a school or institutional computer can cause serious issues. For example, in July 2009, Crystal Defanti, a 5th grade teacher at Isabelle Jackson Elementary (Elk Grove, California) made one of the biggest mistakes of her career. Like many elementary teachers today, Defanti decided to make a "memories" video for her 5th grade students. Unfortunately, Defanti had stored personal videos on her computer. When Defanti made the class video she mistakenly bundled with it a clip of herself naked on a couch. The DVD was sent home to about 24 students. Once some parents and children played the video Defanti's error was discovered. A parent contacted her about the clip. Next, Defanti then called the other parents crying, apologizing, and asking them to get rid

of the DVDs. The local school district sent families a letter asking them to destroy DVDs. (Begnaud, 2009). The district took undisclosed disciplinary action but allowed Defanti to keep her job, though she's not currently listed on the staff directory (Isabelle Jackson Elementary School, 2009). "Understanding E-Safety and Managing the Risks" (Northern Grid for Learning, n.d.) cited a similar example from England of how personal use of school computers can raise serious issues for educators. A head teacher reported:

> 'There is porn on a member of staff's laptop—and it was downloaded by their partner at home' …[This] is representative of a number of scenarios occurring with increasing frequency as schools become more rigorous in the monitoring of their systems (p. 17).

Educators must remember that when they use the resources provided by the school, district or institution, that school district or institution has a right to review how, when, why, where, and by whom those resources are being used.

A more colourful American case is that of Stephen Murmer. Murmer was an art teacher at Monacan High School in Virginia. He developed an alter ego as an artist, Stan Murmur. Under this alias, Murmer created paintings via prints of his genitalia and bottom. In 2006, Murmer—as alter ego, Murmur, wearing a fake nose and towel turban—went on a television program to demonstrate his technique (American Civil Liberties Union, 2006). The video was later made available on YouTube (Fox News, 2006). Someone alerted the school district to the video and Murmer was put on paid leave. He was eventually fired in 2007 (Simpson, 2008). The American Civil Liberties Union became involved and Murmer settled a suit with the Chesterfield County School Board for $65,000 (American Civil Liberties Union, 2008).

Student Ostriches Exposed

Today's children, youth and young adults are tomorrow's adults, professionals and educators. Unlike those of us who came of age prior to the rise of social networking, many of these least stellar moments will be captured, shared and forever archived online—thereby affecting their opportunities and future. In fact, statistics indicate that our students' digital footprints are starting younger and going deeper than ever before. Indvik (2010) stated that 92% of toddlers in the US already had an online presence. Her article went on to state that globally, 81% of children 2 and under had an online presence (Indvik, 2010). She pointed out that an average North American adult's digital footprint is only likely to go back 10-15 years (Indvik, 2010). From my perspective, this is quite concerning. For an average adult, his or her digital footprint is likely to have started about the time that mature thought and behaviours were emerging. What will it mean when children's bad choices and mistakes are forever immortalized online? (For more on this thought, see my October 2010 blog post, "Fleas in a Bottle?: Will Social Networking Stymie Personal Development of Youth?")

One good example of youth's lack of long range perspective when posting to social networks is the Facebook postings from the Clemson University 'gangsta' party on Martin Luther King Day, January 2007. During the party, some Clemson students dressed in "blackface", padded their buttocks and drank malt liquor—drawing on offensive racial

stereotypes. The party caught national attention when images were discovered on Facebook. Clemson University President James Barker was forced to apologize for the students' behavior and investigations were launched by the university and the National Association for the Advancement of Colored People (NAACP). Evidence of similar events was discovered at Tarleton State University and the University of Connecticut School of Law (Schafer, 2007). The Associated Press reported, "Often such parties go unnoticed outside campuses until students post pictures on Facebook.com and other Web sites" (Associated Press, 2007).

In the summer of 2006, more than twelve United States colleges garnered national attention when hazing photos from sports teams were posted on image sharing sites (Teicher, 2006). Teicher (2006) reported that the content contained "scenes involving degrading costumes, excessive drinking, sexually suggestive poses with strippers and fellow athletes, and a blindfolded woman with her hands tied behind her back being led down a staircase." Read (2006) stated in the Chronicle of Higher Education, "College athletics departments are so worried about Facebook and MySpace that in some cases, they've spent the summer researching how their own students use [them]" (¶1). Some schools prohibited athletes from participating in photo-sharing sites and Facebook while others educated students in responsible use. In fact, the University of Michigan asked its athletes to pledge good conduct on social networking sites--behavior reflecting the "high standard of honor and dignity" of the institutions athletics program. The university stated that evidence of any behavior contravening school or team rules could result in the athletes' suspension from the team (Woo, 2006, ¶2).

The practice of posting questionable content on social networking sites is not restricted to athletes. In 2009, the Journal of the American Medical Association published an article titled "Online Posting of Unprofessional Content by Medical Students" (Chretien et al.). The research examined the online behavior of medical students across 78 medical schools in the United States and found:

- 60% of medical schools evidenced "incidents of students posting unprofessional content online;"
- 13% evidenced postings that violated patient confidentiality;
- 52% evidenced postings containing profanity;
- 48% evidenced postings containing discriminatory language;
- 39% evidenced depictions of intoxication; and
- 38% evidenced sexually suggestive material.

The researchers stated that their findings were nearly identical to a University of Florida College of Medicine study conducted a year earlier (Chretien et al., 2009). Clearly, Web 2.0 technologies and social networking sites in particular, present a new issue for candidates in professions with specific standards and/or codes of ethics and behaviours—education and medicine being two such cases. The question is, what provisions have training programs put into place to specifically deal with this type of situation?

Since 2008, our Faculty of Education at Vancouver Island University has been delivering a "Managing Digital Footprints" workshop to Year 3 students. I designed this workshop in response to a request for a technology workshop for Year 3 students who were pondering a future in education, but not yet committed. I thought long and hard about what I could teach these Year 3s—especially when they may never enter education. Managing their digital footprints on media such as Facebook seemed a natural and my work has expanded from there.

Cyberbullying

Cyberbullying is a specific type of unacceptable online behavior. The term "cyberbullying" refers to:

- Spreading lies and/or rumors about others.
- Insulting and/or targeting another's sexuality or physical appearance.
- Deceiving others into revealing personal information or images and publishing it, sending or forwarding it.
- Posting personally identifiable information or photos about another without consent.
- Threatening and/or intimidating others.
- Harassing or stalking others.
- Ostracizing, excluding, and/or causing peer rejection of others.
- Manipulating others.
- Stealing others' identities, making unauthorized access to accounts & impersonating them.

(Sources: National Crime Prevention Council, 2007; Northern Grid For Learning, n.d.)

Statistics on cyberbullying vary. The United States National Crime Prevention Council reported in 2007 that 43% of teens reported being victims of cyberbullying. In that same year, the Internet & American Life Project (Lenhart, 2007) report, "Cyberbullying," found only 32% of all teenagers reported some form of cyberbullying. The National School Boards Association research in 2007 found that just 7% of students "have experienced self-defined cyberbullying" (p. 6). In their findings, the National Crime Prevention Council reported that the highest incidence (50%) was found to be in females aged 15 to 16 years. In the majority of cases, the perpetrator was usually a friend or known to the victim (National Crime Prevention Council, 2007). The PEW Internet & American Life Project (Lenhart, 2007) found that the most common type of cyberbullying was the broadcasting or dissemination of private information. Some theorize that the arms' length distance provided by technology encourages bullying and intensifies it. Daniloff (2009) claimed "The disembodied aggressors are not only likely to be more severe, they are definitely harder to identify." However, in contrast to this expectation, most teenagers (67%) reported that they believe that more bullying happened offline than online (Lenhart, 2007).

On the post-secondary level, the University of New Hampshire surveyed 339 students in 2004 and found that:

- 10-15% of the students received repeated e-mail or Instant Messenger (I-M) messages that "threatened, insulted, or harassed."
- More than 50% received unwanted pornography.
- About 7% reported the harassment to authorities.
- Offensive messages originated from strangers, acquaintances, and significant others.
- Sexual minority students were more likely to be harassed by strangers. (Finn, 2004)

While many educators and parents cite safety concerns as their basis for blocking social networking sites in particular, the findings of the National School Boards Association research in 2007 seems to contradict these fears. The National School Boards Association (2007) found:

- 7% of students reported someone had asked them for their personal identity information on social networking sites; and 6% of parents agreed.
- 4% of students reported conversations with strangers on social networking sites that made them "uncomfortable"; and 3% of parents agreed.
- 3% of students reported repeated attempts by unwelcome strangers to contact them via a social networking site; and 3% of parents agreed.
- 2% of students say that a stranger they met online tried to meet them in person; and 2% of parents agree.
- 0.08% of students (or just 1 in 1,250) reported actually physically meeting a stranger they met online without their parents' permission.

It appears that the school-based messages of 'stranger danger' have transferred well to the online environment, but public perception is another thing. The National School Boards Association research (2007) highlighted the gap between the actual student data and school district perceptions regarding safety issues in social networking:

> School district leaders seem to believe that negative experiences with social networking are more common than students and parent report. For example more than half of the districts (52%) say that students providing personal information online has been a "significant problem" in their schools, yet only 3% of students say they've ever given out their e-mail addresses,[or] instant messaging screen names. (p. 6)

The greatest danger to students online and in social networking environments is not a strange adult predator as widely portrayed in mass media. Rather students' peers are the biggest threat along with other people known to the students. In 2007, the National Crime Prevention Council (United States) reported that 75% of cyberbullied teens were able to identify the cyberbully as "a friend, someone they know from school, or someone else they know." The research also determined that just 23% of teens were cyberbullied by a stranger generally via a chat room (National Crime Prevention Council, 2007).

One of the ways that we build relationships and trust with others is by sharing information about ourselves. Healthy adults with experience have developed skills to determine what content is safe to share and with whom. Adolescents may be particularly vulnerable to cyberbullying as they invest themselves in personal relationships by sharing confidences, images, etc. without this range of experience. Unfortunately, the stability of childhood or adolescent relationships can be variable and ephemeral. This becomes an issue when a friend with whom one has shared confidences or other data about oneself can turn rapidly into an enemy with ammunition to launch a very personal online attack.

Cyberbullying of Students

While the 2007 data from the National School Boards Association appears to downplay the threat from social networking from a percentage standpoint, there are several high profile cases where vulnerable students have suffered greatly. In some cases, data, information, or images were obtained and used by individuals without the victim's consent. In other cases, people in a position of trust in relationship with the victim used content shared in confidence as a weapon against the victim. In these latter cases, the victim may have voluntarily shared the information with an individual(s) who later made the content public. In some cases, victims voluntarily created content which they failed to appropriately safeguard. Just because you are not actively contributing digital content to the web, does not prevent others from contributing content about you. People can avoid—or mitigate—the impact of these second-hand digital footprints by monitoring their digital footprint even when they themselves do not actively post content. Once such information is identified, the victim can take steps to controlling that information either by contacting the sources involved in publishing it and/or contacting appropriate authorities.

"The Star Wars Kid" story speaks to our need to be aware of the lasting nature of any digital content we create. Ghyslain Raza, a Canadian teen from Quebec, is more widely known as the "Star Wars Kid". In 2002, at about 14 years old, Raza made a recording of himself with school video equipment using a golf ball retriever like a light saber. Raza did not erase the recording, and no one recorded over it. The video cassette sat unremarked on a shelf in the school for about a year. Students needing a blank cassette found it and watched it. They eventually edited it and circulated it by email. From email, the video was shared on Kaaza, and then posted on personal website. During a court case, Raza's lawyer stated "the video was so widely circulated that one Internet site solely dedicated to the two-minute clip recorded 76 million visits by October 2004" (Ha, 2006). Web100.com (2009) listed the "Star Wars Kid" video as the 12th most popular viral video of all time, while Molly Wood (2008) of CNET lists it as the 8th most popular web fad. Raza reported that hundreds of students in his "high school's common areas would jump on tables and chant, 'Star Wars Kid! Star Wars Kid!' There would be a commotion as they shouted and poked at him, trying to get a reaction" (Ha, 2006). Raza went on to say "It was total chaos... Any opportunity was good enough to shout 'Star Wars!' "(Ha, 2006). The experiences left Raza unable to attend class, drained of energy, and diagnosed with depression. Raza couldn't go to school or appear in public. Raza's family sued the families of three students involved and they settled out of court (Ha, 2006).

Another disturbing case is from England. In 2008, 13-year-old Sam Leeson joined Bebo (a social networking site). As a member, Leeson shared information about himself—pictures,

likes, interests. Because of his appearance and his preference in music, Leeson was bullied. The bullying spilled over to YouTube. After suffering the cyberbullying for a number of months, Leeson hung himself. His mother discovered Leeson was being bullied when she looked at his Bebo profile after his death (Daily Mail Reporter, 2008). Unlike, Raza, Leeson voluntarily contributed his information to the social network and placed it in a public domain. Yet like Raza, the digital content Leeson created was used to harm him.

Similarly, in 2006, Megan Meier, 13, of Missouri (United States) also committed suicide as a result of cyberbullying via social networking. Prior to her death, Meier was a member of MySpace. She also was suffering depression and was on medication. During 2006, Meier's friend, Ashley, Ashley's mother, Lori, and an 18-year-old employee of Lori's business created a fake identity under the name of "Josh Evans" on MySpace. The created this false persona to see if Meier was spreading rumors about Ashley. Ashley, the mother, and employee befriended Meier online as the supposed 16-year-old home schooled boy "Evans." Communications from "Evans" turned sour and the cyberbullying spilled over into electronic bulletins with messages like "Megan Meier is a slut." and "Megan Meier is fat." One day, Meier's mother found her hanging in the closet and Meier died the following day (ABC News, 2007). While Lori Drew was initially convicted, a federal judge nullified the verdict in July 2009. This Meier incident prompted the Missouri town to pass a law to prevent cyberbullying. Subsequently, Rep. Linda Sanchez (California) of the U.S. House of Representatives introduced the H.R. 1966 bill called the "Megan Meier Cyberbullying Prevention Act". The bill targeted repeated serious acts intending to harm the victim through a variety of electronic means. House subcommittee hearings were held in September 2009.

The case of Mike Carollo provides an example of cyberbullying at the university level. Carollo entered Boston University in 2008 as a freshman. A friend posted "Mike Carollo" and "any thoughts?" as joke on the now defunct site Juicycampus.com (Daniloff, 2009, The New Bathroom Wall section, ¶5). The post garnered 13 to 15 nasty responses. Carollo said, "There were a lot of things written about my sex life…'Slut' and 'whore' were the nice words. It was totally malicious" (Daniloff, 2009, The New Bathroom Wall section, ¶5). The site also falsely said he was "holding a gay parade & needed 'hot guy' volunteers" (English, 2008, p. 2). On the site, someone impersonated Carollo and posted his dorm and room number with the suggestion of a sexual encounter. Carollo reported "The intensity was kind of shocking… It was very unsettling" (Daniloff, 2008, The New Bathroom Wall section, ¶5). Carollo was only one of numerous university students squeezed dry by Juicycampus.com or sites like it. In another case a Boston College co-ed was described "the biggest slam pig of them all, a disgusting disease-infected whore," and in yet another, a Northeastern freshman was described in X-rated terms as "a ho" (English, 2008, p.1).

Cyberbullying of Educators

Educators are particularly vulnerable to cyberbullying both by disgruntled students, parents and colleagues—the legal ramifications of which are still being established in the North American context. In 2007, Katherine Evans was a 17-year-old student in Ft. Lauderdale, Florida (United States). Evans created a Facebook group called "Ms. Sarah Phelps is the worst teacher I've ever met!," featuring the teacher, and an invitation for other students to "express your feelings of hatred" (Kravets, 2008, ¶ 4). Phelps was Evans'

Advanced Placement English teacher. Three other students posted comments against the group and Evans removed it. The principal found out about Evans creating the group and suspended her for three days for "disruptive behavior" and for "Bullying / Cyberbullying Harassment towards a staff member" (Kravets, 2008, ¶ 5). Evans was also removed from the Advanced Placement course and placed in a less prestigious honours course. In 2008, the American Civil Liberties Union filed a lawsuit on Evan's behalf saying that the impact on her permanent school record is "unjustifiably straining her academic reputation and good standing" (Kravets, 2008, ¶ 6).

In a similar case, Justin Layshock was a 17-year-old student at Hickory High School, Hermitage, Pennsylvania (United States). In 2005, he created a mock MySpace page for his principal Eric Trosch with unflattering content. Layshock told his friends about the page and it quickly made the rounds at the school. His principal discovered the page. In addition to a 10-day, out-of-school suspension, the administration ordered him to finish high school in the Alternative Education Program and forbade him from attending his own graduation in the spring. The school eventually permitted Layshock to attend his regular classes, and he graduated in Spring 2006. On July 10, 2007, a federal judge ruled that the school's suspension had been unconstitutional and ordered a jury trial to determine whether Layshock is entitled to compensatory damages for the school district's violation of his First Amendment rights. The case is currently on appeal (American Civil Liberties Union, 2009).

What can educators do if they are defamed by students, parents, or others on the Internet? They can sue for libel—but it's not always that simple. While damages may be awarded, reputations are damaged, content may continue to circulate, and monies awarded may never be 'collectible' as the individual posting it may have no substantial assets. Yet, sometimes these cases are successful. In January 2006, eleven teachers in British Columbia won a court case against a parent, Susan Halstead. Halstead "made unfounded allegations of drug and alcohol abuse, incompetent teaching and serious behavior breaches, as well as creating a 'Least Wanted Educators' website" (Proudfoot, 2006). The teachers were awarded $676,000 in total damages. At the time of the cyberbullying, David Halme was president of a local teachers' association—and also named on the website. He approached Halstead who had confused his name with another teacher and asked her to correct her error. When Halstead refused to remove her posting about Halme, he organized the group of teachers under attach to launch the libel suit.

In "Cyberbullying Goes to College," Caleb Daniloff (2009) writes that a Boston University professor reported a colleague defaming him on RateMyProfessors.com. On the same site, Daniloff further states that a student accused a professor of showing up for class high and posted "veiled comments suggesting that he [the professor] might be sexually harassing students" (¶11). In another RateMyProfessors debacle, Ben Bierman, a College of Fine Arts lecturer at Brooklyn College (United States), caught one of his students plagiarizing and reported the incident. Subsequently, Bierman received belligerent emails from the student. The issue spilled over for two years on RateMyProfessors. Bierman stated, "I've stopped looking… It just caused so much stress. But one of the problems is that it's one of the first things that pops up on a Google search for me. I've worked hard my whole life in developing a positive public profile. There's no recourse, and it's extremely public" (Daniloff, 2009, ¶14). K-12 teachers may be familiar with RateMyProfessors' companion

site, RateMyTeachers.com. At the time of Bierman's case, this second-hand digital footprint was more prominent than his sanctioned one. This is one of the reasons that educators need to create and manage a digital footprint before someone creates one for them. It's more difficult to counteract a smear campaign if there is nothing positive online about you.

In a 2007 Facebook-related case, a Boston University music professor discovered a fake Facebook page posted in his name with his image and biography. The professor remarked, "…embedded in the document were really scurrilous things that were reputed to have been said by me, and they were quite unpleasant and ugly and immature." The professor had no idea how long the page had been up or who created it: "After many phone calls and sleepless nights, with the help of a friend's daughter who knew someone at Facebook, the professor persuaded site administrators to remove the page" (Daniloff, 2009, ¶3). Similarly, David Perlmutter (2009) reported how an older professor Googled his own name for the first time and was "horrified to find himself the focus of a nasty attack on a disgruntled student's blog" (Flood Google with Positives section, ¶2). The professor stated, "Forty years of scholarship and teaching …defamed by 'one guy who didn't get an A' (Perlmutter, 2009, Flood Google with Positives section, ¶2). Perlmutter (2009) stated that "Attempts to remove offensive items are rarely successful" (Flood Google with Positives section, ¶3).

At the University of Calgary in 2008, Keith & Steven Pridgen, 19-year-old brothers created the Facebook group "I no longer fear Hell, I took a course with Aruna Mitra" (CBC News, 2009; Yelland, 2011). In August 2008, Keith Pridgen posted on the "wall":

> [Instructor's name] IS NO LONGER TEACHING ANY COURSES AT THE U OF C!!!!! Remember when she told us she was a long-term prof? Well actually she was only sessional and picked up our class at the last moment because another prof wasn't able to do it…lucky us. Well anyways I think we should all congratulate ourselves for leaving a [instructor's name]-free legacy for future [law and society] students. (CBC News, 2009, ¶4)

The brothers were then censored by the university (Yelland, 2011). They were "found guilty of non-academic misconduct in November 2008 and placed on probation" (Yelland, 2011). Keith Pridgen claimed the treatment was unfair because Aruna was in a relationship with the program head involved in deliberations on the Pridgen case (Dormer, 2009, ¶5). After the incident, the University of Calgary Students' Union noted that the university policies had no direct reference to online misconduct and began working with the university "to find or to create policy and procedure, specifically for these social networking sites because it is pretty ambiguous" (Dormer, 2009, ¶). Meetings were scheduled between faculty and students to discuss Internet policies (CBC News, 2009, University's misconduct policies ambiguous section, ¶5). The brothers filed for a judicial review of the University of Calgary decision with the Alberta Court of Queen's Bench (Yelland, 2011). The argument hinged on whether the Charter of Rights and Freedoms was binding upon universities. The Charter of Rights and Freedoms is binding on the government and bodies acting in its stead. During the judicial review, Justice Strekaf ruled that the Charter of Rights and Freedoms applied to the University of Calgary because universities provide education and the government is responsible for education. Strekaf stated that that by punishing the Pridgen brothers,

the university was infringing on their right to free speech (Yelland, 2011). Yelland (2011) wrote, "The decision surprised the legal community, though it was not unprecedented." In general, the application of the Charter of Rights and Freedoms with regard to universities is hit and miss. In 2011, the University of Calgary filed an appeal against Strekaf's decision (Yelland, 2011).

The balance between free speech and the ability to protect one's personal and professional reputation is a perilous one. Currently the American Civil Liberties Union is bringing a variety of cases to court in the United States on behalf of students who have posted content parodying school employees, pretending to be them, criticizing them and inviting others to do so. Most of these cases are high school incidents that occurred outside of school and outside of school hours. Kravets (2008) pointed out that we are currently seeing an explosion of legal challenges to courts and school administrators who are wrestling "with campus civil order and free expression in an online world" (Kravets, 2008, ¶2). Kravets (2008) went on to quote Frank LoMonte of the Virginia-based Student Press Law Center, "We're in the very first generation of this and there's nothing ripe for the U.S. Supreme Court to hear" (Kravets, 2008, ¶3). From the Pridgen case, it's clear that similar issues seem to be surfacing in the post secondary environment as well. Daniloff (2009) quoted Theirry Guedj, Associate Director of Boston University's Faculty & Staff Assistance Office, that "over the past five years, online harassment cases have been spiking, in particular through Rate My Professors" (¶12).

In looking to balance free speech with appropriate school conduct, a review of the current cases seem to reveal two major issues: 1) determining the school or institution's authority to discipline the students involved; and 2) the appropriateness of the discipline meted out. In the United States, student can be disciplined for off-campus behaviour if it constitutes a "substantial disruption" to school culture/environment. Canadian educators have had less legal experience with these matters. Wendy Harris, a British Columbia lawyer who frequently acts for school districts reported to the British Columbia Teachers' Federation that "Very few cases …have ended up in the courts in Canada…The US, with its more litigious traditions, has had a number of cases that frame the rights of the student and of the school authorities and have some relevance, even if they do not apply directly" (Kuehn, 2008, ¶8). Harris went on to state that as of November 2008, there had been "no reported decisions challenging a school's authority to discipline students for content of websites… yet" (Kuehn, 2008, ¶11).

That said, the Canadian British Columbia Teachers' Federation provides a series of questions to help educators assess student misconduct online and whether a school is in a position to discipline the misconduct:

- Is there a nexus to the school (e.g., did the student's conduct occur at school or away from school)?
- What is the content of the speech (e.g., is it political, lewd, offensive; does it promote violence; is it a school activity)?
- Does the content impact on the school environment or reputation of staff (e.g., what is the impact on the other students or staff)?
- What is the level of disruption to the school (e.g., is it substantial or trifling)?

- Has the school tolerated similar types of speech (e.g., are there other websites containing similar comments)? (Kuehn, 2008, Regulating Student Expression on the Internet section).

Sexting: A Special Form of Cyberbullying

Sexting is a specific type of cyberbullying where the victim sends a nude or partially nude picture of him or herself to a specific person. The recipient then circulates the image leading to harassment, defamation and a number of other negative outcomes including driving people to suicide. In Ohio (United States), in 2009, a high school student, Jesse Logan sent a nude image of herself to her boyfriend. After the two broke up, the boyfriend shared the picture with other girls at their school. The girls further circulated the images (Celizic, 2009). Logan then reported the incident to school personnel who referred her to a police officer, Paul Payne. In a previous sexting incident involving a minor at the school, Payne had opened a criminal investigation and spoken with the parents of the students distributing the image. Since Logan was 18, however, Payne told her he could only ask students to delete the image but could do nothing beyond this. Payne encouraged Jessica to consent to an interview with a local television reporter doing a story on "sexting." Jessica appeared on the program anonymously to talk about the harassment she faced as a result of the picture. Her face was blurred and her voice altered, but students knew it was her (Zetter, 2009a).

When the girls found out Logan had spoken to the police, the harassment escalated. Logan was called "slut", "whore" and "skank" as well as having things thrown at her (Zetter, 2009a, ¶10). She received harassing calls and texts. Logan became depressed and afraid to go to school. She eventual graduated but at the ceremony and following party, students pelted her with objects. Later, students "continued to harass her by phone and online" (Zetter, 2009a, ¶13). After attending the funeral of a friend who committed suicide, Logan herself committed suicide (Zetter, 2009a).

If you think sexting victims are limited to vulnerable young women, think again. In January 2010, 21-year-old Greg Oden, a professional basketball player for the Portland Trailblazers and number 1 draft pick in 2007 had a nude picture of himself surface on the internet. Oden had taken pictures of himself with his cellphone and sent them to his girlfriend about a year and a half prior. Once he was famous, the pictures found their way online. As a professional basketball player, representing the Trailblazers, Oden apologized for the incident and called it "very embarrassing" (Associated Press, 2010, ¶3).

Even administrators can find themselves in very tricky situations when trying to deal with sexting cases. One illustrative example is the case of Ting-Yi Oei, a 60-year-old assistant principal in South Riding, Virginia (United States). In March 2008, Oei heard rumours of students sexting images at his high school. Oei was asked by his principal to investigate the incident and told to capture evidence of the image. Oei recovered evidence but was not very technologically savvy. Since he did not know how to capture the image himself, Oei asked the student with the evidence to text the message to his school email address. Oei and the school's safety/security specialist met with the student who reported the incident. Later the boy who reported the sexting incident got in trouble over another matter. The school administration suspended the boy. Next, the boy's mother contacted Oei asking

him to revoke the suspension. Oei refused and the parent contacted the police to report that Oei had the sexting image on his computer. The mother's report led to investigations, accusations, arrest, large legal fees, personal grief and loss of reputation—especially when Oei's principal did not come forward on his behalf. Though the charges were eventually dropped and court fees paid by the school board, Oei and his image have suffered substantial setbacks (Zetter, 2009b). Clearly, when recovering digital evidence—especially in suspected sexting incidents, clearer policies and protocols must be in place at schools.

An egregious case of peer as cyber predator is the case of Anthony Stancel from Wisconsin (United States). Stancel, 18 at the time, was described as a "high achiever who was particularly alive in political science classes. He had an attention-loving side…and while not the most popular boy…he was not a loner." He was a boy from a 'nice' family in 'middle America.' This 'nice' boy created false Facebook profiles pretending to be girl. He then solicited male schoolmates to sext nude photos of themselves promising that "she" would reciprocate. Once Stancel had the photos, he threatened to release the nude photos to friends and the entire school unless the boys performed sex acts on Stancel. It wasn't until February 2009 that Stancel was caught when the police confiscated his computer based on a totally unrelated incident: Stancel had emailed a bomb threat to his school. Prior to the email, Stancel had had no run-ins with authority. Once police examined Stancel's computer they discovered 39 files under individual names. 31 classmates were victims with youngest boy being 15. Police found 300 nude pictures and some videos. Stancel faced numerous charges (Saulny, S. 2009).

The Creepy Treehouse

The 'creepy treehouse' is a term coined to describe the feeling of discomfort cited by students when professors and educators seek to join students' social networks. As Young (2008) said, "…some students greet an invitation to join professors' personal networks with horror" (¶1). Jared Stein (2008), Director of Instruction Design Services at Utah Valley University says,

> Though such systems may be seen as innovative or problem-solving to the institution, they may repulse some users who see them as [an] infringement on the sanctity of their peer groups, or as having the potential for institutional violations of their privacy, liberty, ownership, or creativity. Some users may simply object to the influence of the institution. (¶19)

What would a case of "creepy treehouse" look like? Saeyoung Park (2009) in "I Don't Want to Be Your BFF, Either," recounted the case of a female graduate student at Yale University. The woman's graduate advisor sent her a friend request on Facebook. (A friend request is how a person asks to join your network on Facebook.) The student said, "I was a bit surprised. I didn't really know what to do. Then he started writing on my wall, and my departmental friends felt uncomfortable, and I had to unfriend him. It was awkward for a week" (Park, 2009, ¶4). In their research regarding the use of social networking by institutions, Madge, Meek, Wellens & Hooley (2009) found that 43% of university students on Facebook said that Facebook should not be used for formal academic work so as to preserve its 'social' nature. The researchers also asked the students "whether they

considered it appropriate for staff from the university to contact them via Facebook in the future for teaching, marketing, pastoral or administrative purposes. In all cases, the majority of students were opposed to the idea" (Madge et al., 2009, p. 151). The message seems to be that students do not want educators in their Facebook networks.

Websites Mentioned in this Section

- Bebo: http://www.bebo.com/
- CNET: http://www.cnet.com
- Dartlog: http://dartreview.blogspot.com/
- Facebook: http://www.facebook.com
- "Fleas in a Bottle?: Will Social Networking Stymie Personal Development of Youth?": http://jhengstler.wordpress.com/2010/10/28/fleas-in-a-bottle-will-social-networking-stymie-personal-development-of-youth/
- Ivy Gate: http://www.ivygateblog.com/
- Juicycampus: now defunct
- Kazaa: http://www.kazaa.com/
- MySpace: http://www.myspace.com
- PEW Internet & American Life Project: http://www.pewinternet.org
- RateMyProfessors: http://www.ratemyprofessors.com
- RateMyTeachers: http://www.ratemyteachers.com/
- Twitter: http://www.twitter.com
- Web100.com: http://www.web100.com
- YouTube: http://www.youtube.com

Policies, Guidelines, & Permissions

Electronic communications can cause uncomfortable situations for people who feel passionately about something, because their very immediacy makes it a quick way to vent. However, technology—and social networking in particular—is not therapy or a place to vent. What you say online in a moment of anger or ignorance could cost you your job, make you a target of abuse or prevent your advancement. If you want to be perceived as a professional, you must reflect on your communication before you comment on it in a digital format. When you Google social networking etiquette or tips, many sites refer to the mom-boss standard: if you determine that your content would be considered offensive by your mother (or insert your family's moral compass here—father, grandfather, grandmother, etc.) or your boss, you should not post it.

As educators, however, you are held to higher standards. In many countries, teachers have professional codes of ethics. For example, where I work in British Columbia, Canada, the British Columbia Teachers' Federation has a professional code of ethics and the British Columbia College of Teacher has a set of professional standards governing professional behavior. As a measure of your online interactions for educators, I suggest you include a check with your code of ethics/professional standards in addition to the mom-boss

rule: Ask yourself, "Would the content pass muster with my mother, my boss, and my professional standards/ethics?" If you find the content to be questionable by any one of these measures, rethink sending that message or posting that content.

A few years ago, when I first began looking for examples of educational policies or guidelines that supported the potential use of Web 2.0 technologies while managing the risks, there were few examples. This situation remains relatively unchanged—especially in North America. The Lemke et al. (2009) report, ""Leadership for Web 2.0 in Education: Promise and Reality Report" indicated that though more than 77% of administrators in US school districts believed in the potential of Web 2.0 and social networking tools to support teaching and learning, a large percentage of them were in the dark about promising practices and tools. Blocking and banning are the policies of choice with regard to social networking and Web 2.0, as evidenced by the National School Boards Association's 2007 research, and the more recent 2009 study "Leadership for Web 2.0 in Education: Promise and Reality Report" conducted by Lemke, Coughlin, Garcia, Reifsneider, & Baas. The 2009 study stated that approximately 70% of US school districts continue to ban social networking sites. One of the main findings of the 2009 study contended: "While there was broad agreement that Web 2.0 applications hold educational value, the use of these tools in American classrooms remains the province of individual pioneering classrooms" (Lemke et al., p. 11). More than 60% of the administrators surveyed, believed that students should be restricted to approved educational websites (Lemke et al., 2009).

Research by the National School Boards Association in 2007 found that while the majority of schools had websites (69%) and almost half (49%) collaborated with other schools online, approximately 80% of districts forbade online chat & instant messaging; and approximately 60% forbade blogging, bulletin boards, as well as sending and receiving email. Although 52% of schools specifically forbade the use of social networking sites while in school, 27% of districts reported that their schools participated in a structured teacher/principal online community and 69% reported that at least half of staff used social networking for professional learning communities (37% said at least 90% of staff are using it for this purpose). Though almost half of the schools surveyed (46%) participated in online pen pal programs or international programs, only 35% of schools or students blogged for instructional purposes and just 22% of classes created/maintained educational wikis (National School Boards Association, 2007). In summary, Lemke et al. (2009) stated, "For most school districts, policies and practices regarding Web 2.0 are only now evolving. While district administrators recognize the promises of Web 2.0 for learning, they are extremely wary of the potential pitfalls" (p. 19). One of the main contributing factors to this prevailing attitude may be that these educational leaders:

> …are more passive than active users in the Web 2.0 space…Most of the current use of Web 2.0 applications by district administrators (superintendents, technology directors, and curriculum directors) is restricted to accessing and viewing of content using a few of the more common applications such as Wiki's and blogs. (Lemke et al., 2009, p. 12)

While Lemke et al. (2009) stated "…the velocity of innovation and change in society, as represented by Web 2.0, is outpacing K-12 education's current capacity for innovation", it's not outpacing business. Rather than blocking and banning, some technological businesses took a different approach to Web 2.0 and social networking use. In 2005, IBM created a wiki to guide employees' use of blogs: "These guidelines aimed to provide helpful, practical advice—and also to protect both IBM bloggers and IBM itself, as the company sought to embrace the blogosphere" (IBM, n.d., ¶1). The "IBM Social Computing Guidelines" (IBM, n.d.) provide a thoughtful and forward thinking set of policies that schools, districts and institutions can use for formulating their own. Another set of exemplary business guidelines worth reading is "Intel Social Media Guidelines". The 2009 Deloitte LLP Ethics & Workplace Survey, "Social Networking and Reputational Risk in the Workplace" reports "60 percent of business executives say they have the 'right to know' how employees portray themselves and their organizations online" (2010, ¶4).

Approaches in the education sector can be far less comprehensive. For example, in 2008 Michael Simpson reported that the Ohio Education Association urged all its members to remove any personal profiles they posted on MySpace or Facebook. The association warned members that such profiles could "be used as evidence in disciplinary proceedings," which could "affect not only a teacher's current job but his/her teaching license" (Simpson, 2008, ¶12). In 2009, Martha's Vineyard (Massachusetts) school staff ethics guidelines were updated to read, "…your out-of-school conduct can affect your job security. The line between our public and private lives is less clear, so what you post on a blog, on your MySpace page, on Facebook, can be accessed by students" ("Internet conduct can trip up some employees", 2009, p. 2). A program policy from School District 69 (Nanaimo, British Columbia) stated, "While not specifically prohibited, the use of social networking sites must take a secondary place to academic applications" (Collaborative Education Alternative Program Code of Conduct, n.d., Acceptable Conduct section ¶5). Citadel Middle School Code of Conduct (2009) stated, "At no time are photographs or video clips taken at school or during school associated events (examples: field trips, sports games, class video project) to be posted on any website or social networking sites." The policy went on to say that if students bring their own computers into school "forms of online communication and social networking sites (examples: Facebook, MSN Messenger, Twitter) are not allowed" (Citadel Middle Electronic Devices Protocol, ¶3).

Another policy example is the Employee Use of Social Networking, SD Policy GBEBD (Sept. 2/09) from the Raymond School District (SAU 33), Raymond, New Hampshire:

> The School Board strongly discourages school district staff from socializing with students outside of school on social networking websites, including but not limited to MySpace, Facebook, Twitter…websites.
>
> All school district employees, faculty and staff who participate in social networking websites shall not post any school district data, documents, photographs or other district owned or created information on any website. Further, the posting of any private or confidential school district data is strictly prohibited… Nothing in this policy prohibits employees, faculty, staff or students from the use of approved educational

> websites if such sites are used solely for educational purposes. Access of social networking websites for individual use during school hours is prohibited. (J. Gillespie, personal communication, October 19, 2009)

More progressive and effective scaffolding of behavior via guidelines and policy is necessary if education is to harness the educational power of Web 2.0 and social networking. One of the best examples of progressive school guidelines with regard to technology use comes from Kent County Council's (United Kingdom) "Safer Practice with Technology for Adults Working in Schools" (2009). I urge any teacher, school, district or institution looking to develop their own materials to download this document as a guideline example that could be adapted to their needs. Questions addressed in this handbook include:

- Should I use my mobile phone to take photographs of students?
- Should I continue to use my Social Networking site?
- Should I have my pupils as friends on Instant Messaging services?
- What is my responsibility for the use of my school laptop at home?
- What is inappropriate material?
- How should I store personal data safely?
- How can I use ICT appropriately to communicate with young people?
- As a technician, how can I safely monitor school network use?
- Can my school limit private online publishing?
- How do I ensure safer online activity in the primary classroom? (Kent County Council, 2009)

For teachers working with students under the age of majority, a useful practice is the creation of Web 2.0 and social networking permission slips for parents to sign. One example is Neill A. Rochelle's Middle/HS Permission Slip for Google, Ning, Wikis, and Delicious. This slip can also be adapted for social networking software. (Rochelle is the Superintendent for Iroquois Central School District in Elma, New York.) Another is the Permission Slip from Erin Wyatt for wikis. Suffern Middle School in New York posts several Web 2.0 permission slips. Here you will find the Saywire Permission Slip and the ePals Permission Slip. One more example is the Parent Permission Slip [for] Shelfari by C. Mitton at East Vincent Elementary School in Spring City, Pennsylvania. (If you know of similar permission slips or policies, and would like to contribute them to a public repository, please post them with any necessary permissions in my public Google Docs folder called "tech_policies" found here: https://docs.google.com/leaf?id=0B_x_FsTFLhdHNGFkODJkOWEtNTI0ZC00YjBkLWJhM2EtNTExYjBiMTVhYTdl&hl=en)

Business practice has set the standard for managing employee behavior in the Web 2.0 era. The Virginia Bar Association and the National School Boards Association indicate that banning and blocking Web 2.0 and social networking technologies is not a sound strategy. As Gouckenour (2010) wrote for the Virginia Bar Association in "Social Networking and the Workforce: Blurring the Line Between Public and Private Spheres":

> Despite the need for reasonable restraint by users, absolute bans by employers on employees' use of social networking sites, both in and out of the office, would be unreasonable. Instead, to avoid unnecessary confusion over social networking in the workplace and appropriate content of personal social networking sites, companies and employers can clearly define social media rules. Social networking sites are useful marketing and employee networking tools and their use should not be discontinued solely because information posted by personal users may end up far from intended targets. As long as those using social networking sites do so with the knowledge that posted information is never truly private, users will not have to wonder whether posts are safe or questionable. (p. 10)

The National School Boards Association report "Creating & Connecting: Research and Guidelines on Online Social—and Educational—Networking" in 2007 concluded that while

> …the vast majority of school districts have stringent rules against nearly all forms of social networking during the school day…school districts may want to consider reexamining their policies and practices and explore ways in which they could use social networking for educational purposes. (p. 1)

As time and the rest of the world marches on with regard to Web 2.0 and social networking use, educators will be drawn into further participation. Educational professions will only benefit if they become leaders in responsible use of these technologies. To do so, educators must manage their digital footprints.

Managing Image & Reputation

Reputations—and images—are fragile things that are easily maimed and difficult to restore. The fragility of image and reputation, combined with the ability to replicate and transmit messages—both good and ill—along networks, as well as the rise of powerful search engines and identity aggregators, means that Web 2.0 and social networking can have substantial impacts on the survival of businesses, organizations and individuals. No wonder then, that as use of Web 2.0 and social networking technologies rose, the business sector—especially technology savvy businesses—moved to develop policies and guidelines to manage employee use of these technologies. Furthermore, businesses began leveraging these types of technologies to evaluate their current and potential employees. Tim Ferguson (2007) wrote:

> Employers are increasingly checking out online personal information about candidates when making recruitment decisions. Net reputations …can have a significant effect when applying for a job…one in five employers finds information about candidates on the Internet, and 59 percent of those said it influences recruitment decisions. (¶1-3)

The Charlotte-Mecklenburg Schools (North Carolina) take a similar approach with existing students and employees. The school district "has an investigator who specializes in online issues, including reports of inappropriate material posted by students about teachers" (Helms, 2008). It also searches for inappropriate content posted by faculty. The school district conducts searches in response to complaints rather than using random sampling. As a result of these investigations, "several employees a year are disciplined for inappropriate posts" (Helms, 2008). Helms (2008) went on to write that Charlotte-Mecklenburg and other districts generally review web pages, MySpace and Facebook sites before hiring.

What Eagles Do: Tips & Guidelines for Managing Your Digital Footprints

About An Eagle

In the course of your professional career, you will generate an active and passive digital footprint—and others will create a second-hand footprint for you. Expectations are increasing that educators do something productive online whether that is providing a classroom portal, posting homework assignments or creating a blog. You need to regularly monitor what you are posting about yourself, as well as what is being said or shared about you. Your first step should be to determine what content is available about you. You can do this by using Google to search variants of your name, as well as one of the deep search engines like Trackur, ReputationDefender and Lookuppage. Sometimes you might discover another person with the same name but of a very different character. In this case, you need to determine how to differentiate yourself. Once you determine what content might exist, you can actively monitor any new content by using variants of your professional name to create alerts with Google; Twitter Alerts with TweetBeep; and Backtype alerts (searches blogs, comments).

With today's technology, you need to consider yourself a "brand." When you create accounts on Web 2.0 and social networking services that you will make public, pick your "username" with a mind to the professional identity you wish to create. Once you establish a name, use the same professional username for all your professional accounts. For example, the web address for your Twitter page and Delicious page are generated based on your username. When you use a consistent username across a number of services, it helps people locate you more easily. For example, my Twitter page is http://www.twitter.com/jhengstler. It is an account where I tweet educational technology links and information. The public page for my Delicious account where I share educational technology bookmarks is http://www.delicious.com/jhengstler. Linking these accounts with identifiable usernames can help raise your professional profile. The opposite process is useful if you are attempting to separate your accounts into the "personal" and the "professional." Personal accounts should have distinctly different usernames or identifiers, different content and different networks. No matter what you post online, assume that everyone will see it someday and link the various accounts—this will help prevent the posting of questionable content.

You should also create a visual identity for your professional persona. This picture will be associated with you and your content. To do this, you will need an image to go with your online identity. Paying for a good headshot can be a worthwhile investment. Determine the image you want to project. Do you want to be seen as a confident professional or a casual person? Once you obtain a good headshot or find a quality photo you can use, be

sure to create an icon-size version of the image—about 100 x 100 pixels in size or smaller. Use this icon image consistently where your Web 2.0 and social networking sites provide a placeholder. Protect your digital image as you do your reputation. Ash (2009) suggested,

> [You] Ask close friends and colleagues to be respectful. If you're out somewhere and you don't want your photo taken, just be very explicit, telling whoever you're with that you're having a good time but you don't want it to be public, either the photo published or your name mentioned. (¶25)

This advice can be particularly useful in social situations like staff or faculty parties when your behavior may be more casual than professional.

Eagles Know Their Audience

Some people are uncomfortable making their persona public. In my case, I've committed to making my online identity my professional identity with the exception of my Facebook account. My Facebook account I keep as my one personal online space. If you want to create a professional persona, it should include content like your full name, and your employment history. The only accounts, identities, content and networks linked to this professional account should be work-related. In contrast, when building a 'personal' profile, do not link it to your school or work information or networks. For example, your personal accounts should not link to your work email. If professional contacts attempt to communicate with you via your personal accounts, direct them to your professional accounts and vice versa. The safest course—as evidenced by the Stephen Murmer case—is to always act like your personas will eventually be linked or your personal data will be leaked.

Increasingly Web 2.0 and social networking services are allowing users to define groups of friends and give them different permissions—limiting what they can or cannot see. Linder (2009) asked readers to think about how much instructors want their students to know about them: Do you want them to be able to see pictures, messages from your personal friends, or your family status? Conversely, how much do you want to know about your students? Remember that on sites like Facebook, when you "friend" students they can get access to your personal information—and you can get access to theirs. Linder (2009) also asked readers to think about how pictures of students or commentaries by them might influence how instructors might treat them in class, evaluate them, and write recommendations for them.

If you are creating personal accounts, be sure that you are aware of all the privacy settings for the site or service you are using and that you set them at the most restrictive levels possible. If you are a Facebook user, you might want to try the third-party application Privacy Mirror to see what the general public can see about you. That said, third party applications that you "add in" to your account on services like Facebook generally require that you provide the application –and the company who made it—access to your account information. Be clear about what you are sharing and with whom before accepting these third party applications—and what information is shared with your network. For example, do you want your colleagues' noses out of joint because you selected one of them over the other as the 'smartest person you know'?

Eagles' Content

Think back to the case of Crystal Defanti, the 5th grade teacher with the video clip of herself bundled with her school content. Defanti's situation demonstrates why, if possible, you should keep your personal data on a personal computer or external hard drive and your work related content on a school computer. This isn't always possible, so if you do have personal data on your school computer, make sure that it's nothing incriminating or embarrassing. Also, remember as you write your emails: the privacy of so-called 'private' communications hinges solely on an honour system—content can be copied and pasted to anywhere. In addition, instant messaging, texting, chat, blogging, and commenting on websites all create permanent records: your content should withstand scrutiny. You are entitled to personal opinions, but assume that if you post them online, everyone will see them. Avoid writing derogatory comments about colleagues, higher-ups or others. All your content should pass the mom—boss—professional standards/ethics rule.

While it might seem common sense, the Global Online Recruitment Resource (2007) stated that when posting content online, you should avoid:

- References to drug abuse [To which I add, "any use"];
- Extremist or intolerant views, including racism and sexism;
- Criminal activity;
- Evidence of excessive alcohol consumption [To which I add: "any alcohol consumption by minors"];
- Inappropriate pictures, including nudity;
- Foul language;
- Links to unsuitable websites;
- Lewd jokes;
- Silly email addresses; and
- Membership of pointless or silly groups. (Top Ten Turn-offs for Employers on Social Networking Websites section)

(As a side note, if you don't want your house robbed in your absence, don't post information about when you and your family will be taking trips.)

Perlmutter (2009) also warned that posted content "may end up scrutinized as a reflection of the quality of your research, teaching, and service" (Proofread Your Prose section, ¶2). With that in mind, you need to make sure your postings are free of misspellings and grammar errors (Perlmutter, 2009). You also need to make sure that that you do not intentionally or unintentionally plagiarize the work of others. Make sure you have copyright or permission for any "borrowed" materials you post. You can always use materials licensed in the Creative Commons, and if there is something you would like to reuse from another author, contact the author directly to see if s/he will allow you to use it. You need to keep any correspondence (e.g. email) from authors granting you permission in case someone questions your use of the material at some future date.

Also, if your advancement is tied to your publishing content, Perlmutter (2009) suggested that posting your insights online, and making experimental data freely available "might cost you promotion-advancing publications when a journal or book editor asks whether the material has appeared 'in print or online' before" (Weigh the Difference Between Facebooking and Publishing section, ¶2). Perlmutter (2009) went on to advise, "…self-publish only summaries and observations rather than complete treatises. Restrict full posts of articles for co-editing and commenting to password-protected venues like Google Docs" (Weigh the Difference Between Facebooking and Publishing section, ¶2). Of course, blogs, wikis and other online publication venues can also raise your professional profile and can be evidenced in electronic portfolios, during performance reviews, or when you seek to change jobs.

Eagles Know When To Be Un'friend'ly

Your image is defined in a large part by your network. You need to actively manage your network and be prepared to prune individuals posting questionable content that would reflect poorly on you. When I first started with Twitter, I followed one user who shared a great deal of valuable information that I often retweeted to my followers. One day this user posted a promotional message for an adult toy provider. This was totally unexpected and initially caught me off-guard. I looked and found that this user had a public Twitter account and the user's image was visible in the list of people I followed. Clicking on the image of the user in the list—or cloud— of people I followed would take you to the user's public page. Even if I didn't actively retweet this questionable content, others could click on him in the list of people I follow and might read the adult toy store content in his public page. How would this look to my students, or to the dean of my faculty? I quickly sent a direct message to the user that while I had appreciated his content in the past, I needed to "unfollow" him due to the adult toy message.

The practice of cutting someone from your network has various terms, "unfriend" in Facebook or "unfollow" in Twitter. When you build networks, make sure you know how to sever connections. If a colleague, professional, or other person with whom you are networked posts materials that you would consider problematic, privately let the other person know that while you value his/her contributions, some recent content does not adhere to your professional standards. You might state that ties to this type of content could jeopardize your job or professional standards. If a colleague, professional or other person expresses concern over content/actions from a person in your network, be sure to actively address the concern. If the person who expressed concern is important to you or your career—and in these days of social networking, that could be just about anyone—follow-up with the individual to share what steps you took to address the concerns.

Eagles Maintain Personal/Professional Boundaries

Educators—whether at the kindergarten level or the post-secondary level—are always in a position of trust with regard to their students. In addition, there will always be a power dynamic which makes any relationship between educators and students an uneven one—where educators by virtue of their position have authority and students do not. We are still in an uneven relationship with parents/guardians as we hold the authority over their vested interested—their child. This makes it unadvisable to include students in personal networks and can make inclusion of parents in personal networks too tricky to contemplate—

particularly challenging to avoid in small, rural communities. Adding older students or alumni to a personal network can also be problematic, especially if their younger siblings are still matriculating through your school. This does not mean these people cannot be part of a professional network. Your first task should be to separate your personal and professional content and networks. If the majority of your accounts are personal in nature, create accounts for professional use. Restrict access to your personal network. Creating different user names or account identities can help—as can using different representative images or icons. That said, always prepare for the moment your personal and professional content could be linked.

Social networking and other Web 2.0 tools can be used for educational benefit when selected wisely, and when risks are managed appropriately—risks associated with the developmental level of the students, as well as risks to an educator's digital reputation. When incorporating these tools, a teacher or instructor needs to align the planned activities with any existing school or institutional policies. If you find these restrictive, rather than contravening them, advocate for change or ask permission for pilot projects from your administrators.

Discuss your project ideas with your administrators. To do this, you should outline your project concept; why the Web 2.0 or social networking use is essential (i.e. what educational benefit is unique to these technologies); which sites or services students will be using; where, when, how, and with whom the students will be accessing the sites or services; as well as how long they will be used. Be sure to acknowledge the risks and how you will manage them—just as you might do in a fieldtrip form where students are taken off-site.

In general, work with your school or institution to:

- define responsible online behavior;
- define cyberbullying;
- establish clear reporting mechanisms;
- create documentation that defines the chain of reporting issues and incidents;
- including roles and responsibilities;
- including when and how to contact parents/guardians, authorities, affected students, etc.; and
- define consequences for poor behavior.

As educators, you should be working to scaffold students into autonomous cyber-citizenship. At the earliest levels—approximately kindergarten to fourth/fifth grade—the teacher should have a professional account (separate from any personal content) on either a public site or closed school/district based network. Young students would post through the teacher and the teacher's account and it would be through this teacher's account that the class would interact with others. In such a case, the content posted needs to be manageable for the teacher. For example, two classes on opposite sides of the globe may exchange Tweets on what they ate for breakfast and lunch as a step to understanding cultural differences. They could post some pictures of actual dishes via Twitpic (a service that works with Twitter to allow you to share images in a tweet) and send links to recipes. Here, the students and

teacher collaborate on the content to be posted, with the teacher making sure that student identities and personal images will remain anonymous. Think of taking students online, much like you would think of taking them on a field trip—teachers should prepare an overview of the project to share with parents/guardians as well as an appropriate permission slip that follows school guidelines. In these types of activities, the educator models responsible online behavior and talks students through behaviours and choices.

As students mature, approximately grade four/five to early high school, they should be developing the capacity to manage their own accounts on closed educational social networks via software managed by an educator, school or district. This software should be located on an official class, school or district server. This is the most secure option. Another option might be a secure online site with restricted access to the participants in a class or school. In this type of scenario, student activity and content posted is monitored by school personnel—guiding students' responsible behavior. Some closed educational networking software is fee based like Saywire (offers a free trial) or Ning. Establishing separate class, school, district or institutional social networks can help educators avoid the creepy treehouse effect. Educause Learning Initiative (2008) said this about Ning:

> For today's students who spend countless hours on Facebook and MySpace, faculty participation on those networks is often seen as an intrusion into a private domain. Ning provides an avenue for instructors to take advantage of social networks in a neutral setting, offering functionality and an experience that are familiar and comfortable to students. (What are the Implications for Teaching and Learning section, ¶1)

Some password protected learning management software like Moodle or Blackboard can also be used to create closed networks. Mahara, an opensource software initially designed for developing and delivering eportfolios, now has pwowerful Web 2.0 features and tools built-in. It, too, would work well on a local server and can be linked by a software bridge to Moodle. The younger the student, the more restrictive the environment should be.

You should also use an appropriate permission slip that defines the tools used, the activities anticipated, and the anticipated risks. It is important to remember, in various countries like Canada, there is increasing concern regarding where users' data is stored. In 2001, the US Patriot Act was signed into law. At that time Canadian medical records housed on American servers on American soil were subject to American searches. As a result, Canadian educators developed a heightened concern regarding the vulnerability of student data. In fact, in 2004 the BC government amended its provincial Freedom of Information and Privacy Act "to prohibit public bodies in BC from contracting with companies that store personal information outside of Canada, or allow access to that information from outside of Canada" (Tso, n.d.). It is incumbent upon educators to determine where student data will be housed—and the associated risks—and include that information on any permission slips or project descriptions. When students are posting content, you must always have a set of guidelines defining responsible online behavior as well as what constitutes unacceptable behaviour like cyber-bullying. These guidelines should be approved by your administration, reviewed at the beginning of each course, revisited periodically and shared with parents and guardians.

Managing online relationships with older high school and post-secondary students can be particularly challenging. Even at this level, continuing the separation of your personal and professional networks is wise. Linder (2009) advised faculty at the post-secondary level to develop their social networking policies with regard to students before classes begin. If students find you on a network and ask to friend or follow you, what will you do? If you accept one student as a member of your network, what happens to students who don't use social networking? Will there be social pressure on other students to join your network? If you view embarrassing personal information on students' profiles will it change how you see them or mark them? Linder (2009) also pointed out that students may not anticipate these complications from networking with you. The safest route is to keep your personal information separate and private—that goes for your students as well. You want to avoid the "creepy treehouse" effect. You can still leverage the power of Web 2.0 and social networking by creating networks specifically for your course or classes. For high school and older students, Ning as well as password protected learning management systems like Mahara, Moodle or Blackboard are still good choices to combat the "creepy treehouse" effect. Though currently targeted at business users, Yammer is another Web 2.0 software platform that has applications for building closed educational networks. Have a server? You might want to take a look at Kootali, a Facebook-like application you can install on your server to create closed networks. All these tools would allow you to establish an academic network separate from students' social networks. While you would not need social networking permission slips for university students—as they are adults—if you are working with high school students, it would still be advisable to review your project with your administration to ensure it falls within the school or district guidelines and policies, and use a Web 2.0 or social networking permission slip with a cover letter describing your project/activity. Further, when working with university students, they should be made aware of the risks and benefits of using the particular service in question-including where the data is housed. Provide them with a project overview, similar to what you might provide an administrator to brief her on the project.

Eagles Defend Their Reputations

Daniloff (2009) stated, "While research into cyber abuse among young teens has exploded, authoritative studies of adult online malfeasance are hard to find" (¶6). There are some adult cyberbullying statistics available. Working to Halt Online Abuse (as cited in Daniloff, 2009) reported an average of more than 100 requests for help from people 18 years old and older each week. Greater than 60% of the victims are white females between the ages of 16 and 30. Of those cases of cyberbullying, 36% started on email and 11% on instant messaging. The UK Dignity at Work Partnership (as cited in Daniloff, 2009) found 20% of workers were cyber bullied by email, 6.2% by text message. Daniloff (2009) reported that "The disembodied aggressors are not only likely to be more severe, they are definitely harder to identify" (Daniloff, 2009,¶10). What should schools and institutions do about the cyberbullying of faculty? "The most important step… is to make cyberbullying an audible part of the campus conversation" (Daniloff, 2009, The Rule Book Please section, ¶1).

When seeking to deal with cyberbullying of faculty by students, we must remember the two major issues that are emerging from the legal cases: 1) determining the school or institution's authority to discipline the students involved; and 2) the appropriateness of the discipline meted out. As Alleyne (2009) wrote,

> …[Schools] should understand and develop policies about social networking sites before they take action against students. If they can't be clear about what qualifies as misconduct, how can students expect to know?…It's pretty ridiculous to just throw social networking under the ambiguous "but not limited to" umbrella. (¶5)

If you discover student content that is defamatory, and the student can be identified, it is useful to apply the series of 5 questions supplied by the British Columbia Teachers' Federation (discussed earlier) as a means to assess student misconduct. Should you find objectionable content about yourself posted by someone else, Douglas (2007) suggested that you send the person a private email asking him or her to 'temporarily' remove the content rather than posting your displeasure on a site. Unfortunately, he stated that "…if the material ends up on a journalistic (or even pseudo-journalistic) site, the chances [of the content being removed] …are small. Journalists generally consider it unethical to clean up a subject's image" (Douglas, 2007, Control the Pages You Don't Control section, ¶1).

J. Bernstein (2009) took more of a risk assessment approach. He counseled readers to first think before responding. He asked readers to determine if the situation was an isolated incident to provoke or whether it was gaining momentum with others joining in. "If it's an isolated incident, and no one has replied, you might consider letting sleeping dogs lie" (Bernstein, 2009, Step 2: Repair Your Online Reputation section, ¶1). If it's a matter of factual information in a blog that is wrong, he suggested contacting the author and asking him to revise the content. Most reasonable authors will revise their content. However, if the criticism is true, Bernstein (2009) advised readers to "apologize using the same medium as the message" (Step 2: Repair Your Online Reputation section, ¶2). He stated that demonstrating willingness to engage regarding the criticism "is likely to win over the skeptics. It also reflects well on [you]" (Bernstein, 2009, Step 2: Repair Your Online Reputation section, ¶2).

If, upon reflection the situation looks like a calculated campaign, such as a blog post plus content on Twitter, Bernstein (2009) suggested taking action. If you're being attacked professionally, you should contact the stakeholders in the situation, including your boss, the media relations person, and the legal department. Next, Bernstein (2009) recommended attempting to contact the detractor informally offline. If the person won't remove content, your next stop is to go public with a post where the original comment exists:

> Be open, constructive, conciliatory, and willing to engage. Try something along these lines: Jim, I've already spoken to you about this, and as you know, what you are saying about me is inaccurate. I would like you to remove it. Meanwhile, if anyone out there reading this has any questions, this is how to reach me. (Step 2: Repair Your Online Reputation section, ¶5)

If the issue continues and is defamatory, Bernstein (2009) suggested contacting a lawyer. This was necessary in the Halstead case described by Proudfoot (2006) in British Columbia, Canada.

Schools and institutions need to develop protocols and procedures for faculty to report cyberbullying. In an interview with Daniloff (2009), Thierry Guedj, Counselor & Assistant Director, Faculty and Staff Assistance Office, Boston University, stated that campuses need to develop an "institutional response with a formal investigative structure" (No Place to Hide section). In the same article, Urs Gasser, Executive Director of the Berkman Center for Internet & Society, said

> Universities should create a climate where, if teachers or workers are affected, they can speak up and know that 'it's not only me,' but a general problem of our time…There should be a person within the organization they can call and say, 'What can I do, and how can we work together to resolve this issue?' And not to further victimize the person by isolating them. (Daniloff, 2009, The Rule Book section, ¶)

Guedj and Gasser's (Daniloff, 2009) commented hold not only for universities, but schools and districts across the world. Kent County Council (n.d.) in the UK had a great poster outlining a working example of how an institution might react: "Response to an incident of concern".

Websites Mentioned in this Section

- Backtype Alerts: http://www.backtype.com
- Blackboard: http://www.blackboard.com
- British Columbia College of Teachers Standards: http://www.bcct.ca/Standards/StandardsDevelopment.aspx
- British Columbia Teachers' Federation Code of Ethics: http://bctf.ca/ProfessionalResponsibility.aspx?id=4292
- Delicious: http://www.delicious.com
- Educause: http://www.educause.edu
- ePals Permission Slip: http://sc.ramapocentral.org/education/components/docmgr/default.php?sectiondetailid=8724&fileitem=14693&catfilter=2348&PHPSESSID=4c2f084e74a5ad28cb39e47644d9eb34
- Facebook: http://www.facebook.com
- Google Alerts: http://www.google.com/alerts
- Google: http://www.google.com
- IBM Social Computing Guidelines: http://www.ibm.com/blogs/zz/en/guidelines.html
- Intel Social Media Guidelines: http://www.intel.com/sites/sitewide/en_US/social-media.htm
- Jhengstler's Delicious page: http://www.delicious.com/jhengstler
- Jhengstler'sTwitter page: http://www.twitter.com/jhengstler
- Kootali: http://www.kootali.com
- Lookuppage: http://www.lookuppage.com

- Mahara: http://mahara.org/
- Moodle: http://www.moodle.org
- MSN Messenger (now Windows Live Messenger): http://download.live.com/messenger
- MySpace: http://www.myspace.com
- Neill A. Rochelle's Middle/HS Permission Slip: http://api.ning.com/files/iC1yGHkE2tAtaJnjBONc-qpYH98lBO4QrNhx9hmPJnUJbwfd2*DGwu4jOfBeXsyEcjpnBNR--I0AJ-GOy0FaqPuxIDKX9WHN/grade612permissionslipforWeb2.0andsocialnetworkingsites.doc
- Ning: http://www.ning.com
- Parent Permission Slip [for] Shelfari: http://www.slideshare.net/cmitton/parent-permission-slip-shelfari-presentation
- Permission Slip from Erin Wyatt: http://education.ning.com/group/middleschool/forum/attachment/download?id=1027485:UploadedFi58:22929
- Privacy Mirror: http://apps.facebook.com/privacy_mirror
- ReputationDefender: http://www.reputationdefender.com
- Response to an Incident of Concern (Kent County Council): http://www.kenttrustweb.org.uk/UserFiles/CW/File/Advisory_Service_ICT/E-Safety/ResponsetoIncident_A4Poster.pdf
- Saywire Permission Slip: http://sc.ramapocentral.org/education/components/docmgr/default.php?sectiondetailid=8724&fileitem=14694&catfilter=2348&PHPSESSID=4c2f084e74a5ad28cb39e47644d9eb34
- Saywire: https://saywire.com
- Suffern Middle School Web 2.0 Permission Slip Site: http://sc.ramapocentral.org/education/components/docmgr/default.php?sectiondetailid=8724&catfilter=2348&PHPSESSID=4c2f084e74a5ad28cb39e47644d9eb34#showDoc
- Technology Policies (Julia Hengstler's Public Google Docs Folder): https://docs.google.com/leaf?id=0B_x_FsTFLhdHNGFkODJkOWEtNTI0ZC00YjBkLWJhM2EtNTExYjBiMTVhYTdl&hl=en
- Trackur: http://www.trackur.com
- TweetBeep: http://www.tweetbeep.com
- Twitpic: http://www.twitpic.com
- Twitter: http://www.twitter.com
- UK Dignity at Work Partnership: http://www.dignityatwork.org
- Working to Halt Online Abuse: http://www.haltabuse.org
- Yammer: http://www.yammer.com

Summary

Ultimately, being online—much like stepping outside your door each morning—is rife with risk. Your knowledge, skill, and good judgment are what allow you to manage those risks to the best of your ability. It is only when you leave the safety of your house and venture outside that you can connect with the world, expand your horizons and enrich yourself and others. Web 2.0 and social networking technologies have much to offer education—teachers and learners—but only if educators and students develop the knowledge, skill and good judgment to manage the risks involved. A major component of your risk management is managing your digital footprint—traces of your electronic activities that others can discover and aggregate.

With the convergence of Web 2.0, social networking technologies, powerful search engines and information aggregation services, managing the content of digital footprints has become a critical professional skill for protecting professional reputations. Without professional development or training, many educators blur their personal and professional content and networks—sometimes with disastrous effects. Many educators are unaware of their second-hand footprints—what is intentionally said or shared about them by others—or avoid monitoring them. These issues combined with a lack of understanding about the fundamental mechanics of how social networks function, has made educators vulnerable—ostriches with their heads in the sand.

Being aware of the mechanics of Web 2.0 and social networking, the issues, as well as emerging strategies and policy guidelines can transform ostriches into eagles. As "Understanding E-Safety and Managing the Risks" states,

> It is not possible to create a 100% safe environment and it is the school's [and teacher's] responsibility to demonstrate that they have managed the risks and to have done everything that could be reasonably expected of them to protect the users and the school. The school [and teacher] that is seen to have managed the risks will have policies, practices and infrastructure developed and regularly reviewed to ensure they meet the needs of their specific learning community. (The Northern Grid for Learning, n.d., p. 4)

Eagles are people who can leverage the educational and professional benefits of today's technologies while actively, responsibly, and professionally managing their digital footprints—and the inherent risks. I hope that this chapter has helped you become more like an eagle. Remember, it is the eagle that soars while the ostrich watches from below.

Glossary

Cookies. A small file placed on your computer by a second or third party to track your online activity—generally in regard to your activity on a specific site.

Cyberbullying. Bullying, intimidating, harassing, etc. individuals via electronic means.

Dark web. See "Deep web".

Deep web. Also "dark web"; information contained on the Internet in databases not indexed by major search engines although most of it is publically accessible via specialty searches; data in the deep web is generated dynamically in response to database queries; though there are no definitive estimates of the amount of data in the deep web, the general consensus is that it is much greater than the "surface web".

Delicious. Online service that allows users to share their bookmarks or favourites; commonly referred to as a 'social bookmarking' site due to the ability of users to network and subscribe to others' accounts, keywords of interest, etc.

Digital footprint. Traces or records of a person's online activities; may be active—content voluntarily contributed by a person, or passive—data collected about a person by a second or third party.

Direct message. Original post by a Twitter user to another user that are considered "private" communication; usually prefaced by "D" or "DM"; users may only direct message those who are following them; a DM is not visible to followers or on the webpage version of any public accounts; it is very important to understand that the privacy of such direct messages can only be assumed and never assured.

Facebook. Social networking site created in 2004; users create profiles and link with other users to form a network; users may also invite non-users to join Facebook and their network.

Facebook wall. Area in a Facebook user's site that acts like a public bulletin board; linked members (also known as "friends") may post to each others' 'walls'; content on the walls is viewable by those with access

Follower. Person or group subscribing to content from a particular user or group on a Web 2.0 or social networking service; specifically a term used in Twitter.

Following. Act of subscribing to content from a particular user or group on a Web 2.0 or social networking service; specifically a term used in Twitter.

Friend request. Internal message sent by a social network site—more specifically in the social networking site Facebook—on behalf of a person or group who wants to network with the recipient of the message.

Friending. Adding another person or group to your network—more specifically in the social networking site Facebook.

Googling yourself. Searching variants of your name on Google to see what can be discovered about yourself.

Identity aggregator. Service—generally fee based—that scours the surface web and deep web to collect information on a given person in order to develop a detailed profile of the individual.

Instant messaging. Synchronous communication between two or more people on an instant messaging service like Windows Live Messenger.

Learning management system. Software—generally internet based—used to develop, deliver and administrate learning activities, courses, or programs.

Metadata. Keywords or terms that are included to describe the data contained in electronic media; metadata is required for effective indexing and searching.

Phishing. Fraudulent emails sent to elicit sensitive information from the recipient via trickery in order to conduct some type of criminal activity.

Post. Content that a user puts online to share with others.

Posting. When a user puts content online to share with others.

Profile. Information about a user of a service or software; data may be supplied by the user or collected about the user through use of the service or software.

Recall. Function on an email program that allows a sender to retrieve an unread email message from the recipient's inbound email.

Reply. On Twitter, an original post of 140 characters or less directed to a particular Twitter user; replies can help structure a conversation thread; usually prefaced by "@" followed by the username of the person to whom its addressed; many Twitter clients allow users to monitor replies regardless of whether you are following the person who posted the reply; replies can be a way to contact people who are not following you; a reply is visible to followers and on the webpage version of any public accounts; also refers to a function in email that allows you to reply to the sender of a specific email.

Retweet. Republished tweet from another Twitter user with attribution regarding where the information came from; a retweet is usually prefaced by "RT" followed by the contributor's Twitter account name; attribution may be multilayered to indicate the path the original tweet traveled to reach the user retweeting it at the time; a RT is visible to followers and on the webpage version of any public accounts.

Sexting. Practice of sending nude or partially nude pictures of yourself to others; often used to later cyberbully individuals.

Social networking. Activity or technology whereby individuals or groups build online communities based on a common interest or activity and where they network to share content, ideas, etc.

Spam. Unsolicited junk mail delivered to your email account.

Surface web. What is generally considered the "world wide web"; small percentage of information of what is publically accessible on the entire Internet; the entire internet is much like an iceberg with the majority of content in the "deep web" or "dark web".

Tweet. A posting of 140 characters or less via Twitter that are sent to a member's network or 'followers'.

Twitter. A micro blogging and social networking platform where users create tweets or postings of 140 characters or less that are sent to their network or 'followers'.

Twitter client. A software program that allows you to use the Twitter service; e.g. Tweetdeck, Hootsuite, etc.

Unfollow. Process of removing someone from your social network—more specifically in the social networking site Twitter; procedure may have social ramifications.

Unfriend. Process of removing someone from your social network—more specifically in the social networking site Facebook; procedure may have social ramifications.

Web 1.0. Initial stage of the Internet where a defined set of developers pushed content such as software, documentation, and resources out to users; model was consumeristic.

Web 2.0. Developmental stage of the Internet defined by user participation, collaboration and contribution; required implementation of modular developmental designs to facilitate user collaboration and contributions; modularity of design gave rise to human networks of contributors and users.

References

ABC News. (2007). *Parents: Cyberbullying led to teen's suicide*. Retrieved from http://abcnews.go.com/GMA/story?id=3882520&page=1

Alleyne, B. (2009). *Student on Probation for Expressing a Negative Opinion About an Instructor on Facebook*. Retrieved from http://www.njnnetwork.com/njn/?p=6231

American Civil Liberties Union (ACLU). (2006). *ACLU Says Virginia Schoolteacher Has Right to Artistic Expression*. Retrieved from http://www.aclu.org/free-speech/aclu-says-virginia-schoolteacher-has-right-artistic-expression

(2008). *Fired Art Teacher Wins $65,000 Settlement from Chesterfield County School Board*. Retrieved from http://www.buttprintart.com/aclu_7mar08_release.html

(2009). *Layshock v. Hermitage School District*. Retrieved from http://www.aclupa.org/legal/legaldocket/studentsuspendedforinterne.htm

Ash, A. (2009). Social networking 101: Facebook and your digital reputation. *National Post*. Retrieved from http://www.nationalpost.com/life/story.html?id=1993356

Associated Press. (2007). *Scholars weigh in on college parties that mock black stereotypes*. Retrieved from http://diverseeducation.com/article/6950/1.php

(2010) *Blazers C Greg Oden apologizes for nude photos*. Retrieved from http://ca.sports.yahoo.com/nba/news?slug=ap-trailblazersoden&prov=ap&type=lgns

Athow, D. (2009). *Scottish teacher faces sack over inappropriate Twitter use*. Retrieved from http://www.itproportal.com/portal/news/article/2009/5/22/scottish-teacher-probed-over-twitter-posts-about-pupils/

Beal, A. (2008). Ten tactics that could save your online reputation. *Mashable: The Social Media Guide*. Retrieved from http://mashable.com/2008/03/11/online-reputation/

Begnaud, D. (2009). *Teacher gives sex tape to 5th graders on DVD*. Retrieved from http://cbs13.com/local/teacher.porn.dvd.2.1068250.html

Bergman, M. (2001). White paper: The deep web: Surfacing hidden value. *The Journal of Electronic Publishing, 7*(1). doi: http://dx.doi.org/10.3998/3336451.0007.104

Bergman, M. (2007). *The murky depths of the 'deep web'.AI3 (Adaptive Information Adaptive Innovation Adaptive Infrastructure)*. Retrieved from http://www.mkbergman.com/343/the-murky-depths-of-the-deep-web/

Bernstein, J. (2009). *October 2009, How to Save Your Online Reputation*. Retrieved from http://www.bnet.com/2403-13068_23-349621.html

Carter, D. (2010). University dean accidentally hits the 'reply all' button. In *eCampus News*. Retrieved from http://www.ecampusnews.com/technologies/university-dean-accidentally-hits-the-reply-all-button/

CBS News. (2009). *University student reprimanded for Facebook comment*. Retrieved from http://www.cbc.ca/technology/story/2009/03/10/cgy-facebook-uofc-comments.html

Celizic, M. (2009). *Her teen committed suicide over 'sexting'*. Retrieved from http://today.msnbc.msn.com/id/29546030/

Chretien, K., Greysen S., Chretien, J. & Kind, T. (2009). Online posting of unprofessional content by medical students. [Abstract*]. Journal of the American Medical Association, 02*(12):1309-1315. Retrieved from http://jama.ama-assn.org/cgi/content/abstract/302/12/1309

"Citadel Middle School Code of Conduct". (2009). Retrieved from http://public.sd43.bc.ca/middle/citadel/Code%20of%20Conduct%2020092010/Code%20of%20Conduct%20Citadel%202009-2010%20version%206%20-%20Final.pdf

"Collaborative Education Alternative Program Code of Conduct ". (n.d.). Retrieved from http://www.sd69.bc.ca/school/CEAP/SiteCollectionDocuments/CEAP%20Code%20of%20Conduct.pdf

CTV News. (2007). *B.C. principal reinstated after nude photo scandal*. Retrieved from http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20070615/naked_principal_070615/20070615?hub=TopStories

Daily Mail Reporter. (2008). Boy, 13, 'hanged himself after he was bullied on Bebo for being a fan of Emo music'. *Mail Online*. Retrieved from http://www.dailymail.co.uk/news/article-1025654/Boy-13-hanged-bullied-Bebo-fan-Emo-music.html

Daniloff, C. (2009). Cyberbullying goes to college. *Bostonia*. Retrieved from http://www.bu.edu/bostonia/spring09/bully/

Deloitte Development LLC (2010). Social networking and reputational risk in the workplace. *Ethics & Workplace Survey*. Retrieved from http://www.deloitte.com/view/en_US/us/About/Ethics-Independence/article/8aa3cb51ed812210VgnVCM100000ba42f00aRCRD.htm

Dolan, P. (2009). Social media behavior could threaten your reputation, job prospects. *American Medical News*. Retrieved from http://www.ama-assn.org/amednews/2009/10/12/bil21012.htm

Dormer, D. (2009) Student on probation for Facebook comments. *Calgary Sun*. Retrieved from http://cnews.canoe.ca/CNEWS/Canada/2009/03/10/8690941-sun.html

Douglas, N. (2007). *How to look good when your recruiter Googles you*. Retrieved from http://valleywag.gawker.com/tech/silicon-valley-users-guide/how-to-look-good-when-your-recruiter-googles-you-247854.php

Edgar, M. (2008). *Reiko Ohnuma, Part 2*. Retrieved from http://dartreview.blogspot.com/2008/12/reiko-ohnuma-part-2.php

Educause Learning Initiative. (2008). *7 Things You Should Know About Ning*. Retrieved from http://net.educause.edu/ir/library/pdf/ELI7036.pdf

English, B. (2008). *Dorm Rumors*. Retrieved from http://www.boston.com/news/education/higher/articles/2008/12/29/dorm_rumors/?page=2

ePals Permission Slip. (n.d.) Retrieved from http://sc.ramapocentral.org/education/sctemp/12345/1265347662/tm_parentalconsent.pdf

Facebook 101. (2007). *Teacher Magazine, Winter 2007*, pp. 13-15. Retrieved from http://www.bcct.ca/documents/TC/2007/TCMagazine_Winter_2007.pdf

Ferguson, T (2007). *Want a job? Clean up your web act*. Retrieved from http://news.cnet.com/2100-1025_3-6171187.html

Finn, J. (2004). A survey of online harassment at a university campus. [Abstract]. *Journal of Interpersonal Violence, 19*(4), 468-483. Retrieved from http://jiv.sagepub.com/cgi/content/abstract/19/4/468

Fox News. (2006). *Virginia teacher suspended for painting with butt*. Retrieved from http://www.foxnews.com/story/0,2933,236201,00.html

Global Online Recruitment Resource. (2007). *Employers use Facebook for further background checks*. Retrieved from http://www.onrec.com/newsstories/17612.asp

Gouckenour, E. (2010). Social Networking and the Workforce: Blurring the Line Between Public and Private Spheres. *VBA News Journal, 36*(4), 8-10. Retrieved from http://www.vba.org/vnjWinter10.pdf

Ha, T. (2006). 'Star Wars Kid' cuts a deal with his tormentors, *Globe & Mail*. Retrieved from http://www.thefreeradical.ca/Cyber_bully_lawsuit_settled.htm

Helms, A. (2008). Teachers disciplined for Facebook postings. *Charlotte Observer*. Retrieved from http://www.charlotteobserver.com/597/story/319902.html

IBM. (n.d.). *IBM Social Computing Guidelines*. Retrieved from http://www.ibm.com/blogs/zz/en/guidelines.html

Indvik, L. (2010). *92% of U.S. toddlers have online presence* [study]. Retrieved from http://mashable.com/2010/10/07/toddlers-online-presence/

Intel. (2009). *Intel Social Media Guidelines*. Retrieved from http://www.intel.com/sites/sitewide/en_US/social-media.htm

"Internet conduct can trip up some employees". (2009). *Martha Vineyard Times Online*. Retrieved from http://www.mvtimes.com/marthas-vineyard/news/2009/03/19/internet-conduct.php?page=1

Isabelle Jackson Elementary School. (2009). Staff. Retrieved from http://www.egusd.net/jackson/staff.html

Kemp, J. (2009). *Teachers banned from Twitter after indiscreet tweet* . Retrieved from http://www.guardian.co.uk/education/2009/jun/10/teacher-banned-twitter

Kent County Council. (2009). *Safer Practice with Technology for Adults Working in Schools*. Retrieved from http://www.kenttrustweb.org.uk/UserFiles/CW/File/Advisory_Service_ICT/E-Safety/SaferPracticeWithTechnology-260509.pdf

(n.d.) . *Response to an incident of concern*. Retrieved from http://www.kenttrustweb.org.uk/UserFiles/CW/File/Advisory_Service_ICT/E-Safety/ResponsetoIncident_A4Poster.pdf

Kravets, D. (2008). *Student who created Facebook group critical of teacher sues high school over suspension*. Wired. Retrieved from http://www.wired.com/threatlevel/2008/12/us-student-inte/

Kuehn, L. (2008). Renegotiating school boundaries in the age of social networking. *Teacher Magazine, 21*(3). Retrieved from http://bctf.ca/publications/NewsmagArticle.aspx?id=17112

Lemke, C., Coughlin, E., Garcia, L., Reifsneider, D., & Baas, J. (2009). *Leadership for Web 2.0 in Education: Promise and Reality*. Culver City, CA: Metiri Group. Commissioned by CoSN through support from the John D. and Catherine T. MacArthur Foundation.

Lenhart, A. (2007). Cyberbullying. *PEW Internet & American Life Project*. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf

Linder, K. (2009). *Students and social networking: Should you 'friend' your students?* Retrieved from http://www.facultyfocus.com/articles/trends-in-higher-education/students-and-social-networking-should-you-friend-your-students/

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). Digital Footprints. *PEW Internet & American Life Project*. Retrieved from http://www.pewinternet.org/Reports/2007/Digital-Footprints.aspx

Madge, C., Meek, J., Wellens, J. & Hooley,T. (2009). Facebook, social integration and informal learning at university: 'It is more for socialising and talking to friends about work than for actually doing work'. *Learning, Media and Technology, 34*(2), 141-155. Retrieved from http://pdfserve.informaworld.com/640982_770885140_912648077.pdf

Martin, M. (2008). Old people Facebook disasters. *Salon.com*. Retrieved from http://www.salon.com/life/feature/2008/09/29/old_people/index.html

Mitton, C. (n.d.) *Parent Permission Slip Shelfari.* Retrieved from http://www.slideshare.net/cmitton/parent-permission-slip-shelfari-presentation

National Crime Prevention Council. (2007). *Teens & cyberbullying*. Retrieved from http://surfsafety.net/Cyberbullying-Exec%20Summary-FINAL.htm

National Education Association. (2008). *The whole world wide web is watching*. Retrieved from http://www.nea.org/home/12784.htm

National School Boards Association. (2007). *Creating & Connecting: Research and Guidelines on Online Social—and Educational—Networking*. Retrieved from http://www.nsba.org/SecondaryMenu/TLN/CreatingandConnecting.aspx

Nickson, C. (2009). The history of social networking. *Digital Trends*. Retrieved from http://www.digitaltrends.com/features/the-history-of-social-networking/

Northern Grid for Learning. (n.d.). *Understanding e safety and managing the risks*. Retrieved from http://www.northerngrid.org/attachments/206_ng_understanding_esafety_and_managing_the_risks.pdf)

O'Reilly, T. (2005). *What is Web 2.0*. O'Reilly. Retrieved from http://oreilly.com/web2/archive/what-is-web-20.html

Park, S. (2009). I don't want to be your BFF, either. *Chronicle of Higher Education, 55*(39), B22. Retrieved from http://ezproxy.mala.bc.ca:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie&db=aph&AN=42531463&site=ehost-live

Perlmutter, D. (2009). Facebooking for the tenure track. *Chronicle of Higher Education, 56*(2) Retrieved from http://web.ebscohost.com/ehost/detail?vid=5&hid=112&sid=2926f0a8-1e31-45c8-8d11-b360cf0637f9%40sessionmgr110&bdata=JkF1dGhUeXBlPWlwLGNvb2tpZSZzaXRlPWVob3N0LWxpdmU%3d#db=aph&AN=44294876

Peter, I. (2004). *The history of email*. Retrieved from http://www.nethistory.info/History%20of%20the%20Internet/email.html

Proudfoot, S. (2006, March 18). Angry bloggers learn web isn't licence to libel. *The Ottawa Citizen*.

Read, B. (2006). Social networks under suspicion. *Chronicle of Higher Education*. Retrieved from http://chronicle.com/blogPost/Social-Networks-Under-Suspi/2483/

Rochelle, N.(n.d.) *Neill A. Rochelle's middle/hs permission slip*. Retrieved from http://api.ning.com/files/iC1yGHkE2tAtaJnjBONc-qpYH98lBO4QrNhx9hmPJnUJbwfd2*DGwu4jOfBeXsyEcjpnBNR--I0AJ-GOy0FaqPuxIDKX9WHN/grade612permissionslipforWeb2.0andsocialnetworkingsites.doc

Saulny, S. (2009). Sex predator accusations shake Wisconsin town. *New York Times*. Retrieved from http://www.nytimes.com/2009/02/11/us/11wisconsin.html?_r=3

Saywire Permission Slip. (n.d.) Retrieved from http://sc.ramapocentral.org/education/components/docmgr/default.php?sectiondetailid=8724&fileitem=14694&catfilter=2348&PHPSESSID=4c2f084e74a5ad28cb39e47644d9eb34

Schafer, S. (2007).Clemson University investigates party, students' racial mocking upsets public. *The Daily Texan*. Retrieved from http://www.dailytexanonline.com/university/clemson-university-investigates-party-students-racial-mocking-upsets-public-1.961776

Shestakov, D. & Salakoski, T. (2007). *On estimating the scale of the national deep web. In Database and Expert Systems Applications* (pp. 780-789). Retrieved from http://springerlink.metapress.com/content/mj04774149679615/?p=419b75b410a14bd594c1d94e893b798b&pi=0 doi: 10.1007/978-3-540-74469-6_76

Shewan v. Board of Trustees of School District #34 (Abbotsford). (1987). CanLII 159 (BC C.A.). Retrieved from http://www.canlii.org/en/bc/bcca/doc/1987/1987canlii159/1987canlii159.html

Simpson, M. (2008). The whole world (wide web) is watching. *NEA Today*. Retrieved from http://findarticles.com/p/articles/mi_qa3617/is_200804/ai_n25502223/

Social Network Service. (2010). In *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Social_network_service#History

Stein, J. (2008). *Defining creepy treehouse*. Retrieved from http://flexknowlogy.learningfield.org/2008/04/09/defining-creepy-tree-house/

Tso, W. (n.d.). The US Patriot Act and its effect on Canadians. *Centre for Constitutional Studies*. Retrieved from http://www.law.ualberta.ca/centres/ccs/issues/theuspatriotactanditseffectoncanadians.php

Teicher, S. (2006). Online photos put hazing in the spotlight again. *The Christian Science Monitor*. Retrieved from http://www.csmonitor.com/2006/0614/p16s01-legn.html

Web 2.0. (2009). In *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Web_2.0

Web100.com. (2010). *Viral Video: Top 100*. Retrieved from http://www.web100.com/viral-video-100

Wikipedia. (2010). Sixdegrees.com. Retrieved from http://en.wikipedia.org/wiki/Sixdegrees.com

(2011). Social network service. Retrieved from http://en.wikipedia.org/wiki/Social_network_service

Woo, S. (2006). U. of Michigan asks athletes to pledge good conduct on social-networking sites. *Chronicle of Higher Education*. Retrieved from http://web.ebscohost.com/ehost/detail?vid=7&hid=5&sid=90dc403b-9dc0-4d51-88dd-271d9d2444ba%40sessionmgr10&bdata=JkF1dGhUeXBlPWlwLGNvb2tpZSZzaXRlPWVob3N0LWxpdmU%3d#db=aph&AN=22552685

Wood, M. (2008). *Top ten web fads*. Retrieved from http://www.cnet.com/1990-11136_1-6268155-1.html?tag=cnetfd.l

Wyatt, E. (n.d.). Permission Slip from Erin Wyatt. Retrieved from http://education.ning.com/group/middleschool/forum/attachment/download?id=1027485:UploadedFi58:22929

Yadav, S. (2006). Facebook—The complete biography. *Mashable: The Social Media Guide*. Retrieved from http://mashable.com/2006/08/25/facebook-profile/

Yelland, T. (2011, January 6). U of C appeals Facebook ruling. *The carillon*. Retrieved from http://www.carillonregina.com/?p=2023

Young, J. (2008). When professors create social networks for classes, some students see a 'creepy treehouse'. *Chronicle of Higher Education*. Retrieved from http://chronicle.com/blogPost/When-Professors-Create-Social/4176

(2009). How not to lose face on Facebook, for professors. *Chronicle of Higher Education, 55*(22), A1-A3. Retrieved from http://web.ebscohost.com/ehost/detail?vid=2&hid=107&sid=d05a2dde-6ec2-4265-8c1c-9e3d6253d5b3%40sessionmgr112&bdata=JkF1dGhUeXBlPWlwLGNvb2tpZSZzaXRlPWVob3N0LWxpdmU%3d#db=aph&AN=36546614

Yu, J. (2008). Dartmouth religion professor apparently clueless about the perils of Facebook. *Ivy Gate*. Retrieved from http://www.ivygateblog.com/2008/12/dartmouth-religion-professor-apparently-clueless-about-the-perils-of-facebook/

Zetter, K. (2009a). Parents of dead teen sue school over sexting images. *Wired*. Retrieved from http://www.wired.com/threatlevel/2009/12/sexting-suit/ (2009b). 'Sexting' hysteria falsely brands educator as child pornographer. Retrieved from http://www.wired.com/threatlevel/2009/04/sexting-hysteri/