Australian Journal of Teacher Education

Volume 34 | Issue 2 Article 1

2009

Reading in the Hyperconnected Information Era: Lessons from the Beijing Ticket Scam

Alison Ruth
Griffith University

Reading in the Hyperconnected Information Era: Lessons from the Beijing Ticket Scam

Alison Ruth
Griffith University
a.ruth@griffith.edu.au

Abstract: In this paper I argue that the kinds of literacy needed for making sense of information on websites is more nuanced and embedded in our everyday context that we are currently providing for learners. The kinds of analysis of websites which allow the processing of information in context are presented. This is demonstrated by an analysis of a scam site, which sold non-existent tickets to the Beijing Olympics and a description of a phishing attempt at Twitter. The skills required to understand information presented on the web have evolved far quicker than the parallel shifts in road safety skills, and people are now required to read web sites contextually if they are to be able to make informed decisions about information available on the World Wide Web. It is proposed that this is achieved through education rather than filtering out undesirable information.

Introduction

The simple task of reading, that is decoding words on a page, becomes a more complex task in a media rich environment, that is, containing more than just text. The colourful images available in magazines and web pages add context and layers of meaning to text on the page or the screen. Further meaning can be derived from layout and structure of 'pages' both online and off. The case being made here is that it is the totality of the presentation of web pages that adds complexity to the task of making sense of information presented in web pages. This includes text, images, style of presentation, and background colour as well as a host of other features as discussed below.

This is further complicated by the sociocultural positioning of the individual doing the reading and our interpretation of the act of reading. Gee (2000) discusses how "dichotomies between cognition and context, skills and meaning, formal structures and communicational functions, and the individual and the social" are converging. It is within the context of converging processes that reading, in this paper, is placed. Billett (2009, p42) elaborates that the "construal of experiences will differ across those engaging in the same physical and social environment due to distinct premediate experiences leading to particular ways of experiencing the observed and felt world". Like Billett, I attempt to go beyond a simple account to explain what constitutes situated reading (sense-making) on the World Wide Web while also recognising that it is distinct for each individual.

In a parallel fashion, learning to negotiate roads, crossing safely, estimating the distance and speed of cars in the environment, is a cultural and geographically bounded activity. Visiting a country where the traffic travels on the 'wrong' side of the road than one is accustomed, emphasises the process of reading in new contexts. It has taken many decades and slow innovation for us to accept and rely upon the network of roads

in towns and cities, yet in less than two decades, many web users have become accustomed to many features that appear strange or are not important to those people still adjusting to the 'new frontier'. As people become more familiar with the scope and limitations of mediated contexts (Ruth, 2008), the skills described herein become more important and more contextually bound.

The development of skills for 'reading', that is, making sense of information in media rich web sites and assessing the validity of that information is a seemingly neglected part of learning, in many Western educational systems, and an imperative in the era of an Internet-enabled world. While many students are exposed to processes of critical reading, these skills are by no means universal (see for instance Turner, 2007). Turner (2007, p112) highlights that the 'cultural dimension of literacy' (specifically critical literacy) has been lost particularly as it relates to an individual's everyday life. Furthermore, there are many conceptualisations of how reading and literacy has shifted online causing potentially 'rapid transformations in the nature of literacy' (Leu, Jr., Kinzer, Coiro, & Cammack, 2004), with the coining of terms such as e-literacy (Schleppegrell, 2007, Symons, Langille, & Hemming, 2002, Lewis, 2002), hyper-literacy (Bawden, 2001), information literacy (Bawden, 2001, Bundy, 2004), cyberliteracy (Livingstone, 2008), digital literacy (Bawden, 2001), web literacy (Sutherland-Smith, 2002), media literacy (Livingstone, 2004) and techno-literacy (Donnison, 2007). Each of these terms signals some part of the transformations that have occurred with what may be thought of as a core competence of shifting technologically mediated social interactions – initially the ability to read, then to write but moving toward deeper and more diverse forms of literacy. These diverse levels of literacy include the skills of reading texts literally, looking for connections between texts, and applying this understanding to new situations (Verezub, Grossi, Howard, & Watkins, 2008) as well as making sense of the contextual information contained in the page. Such sense-making has implications for much of what we do in the 21st century, including discriminating the increasing spam load in email (Lewis, 2002).

Reading online – being hyperconnected – is the form of literacy associated with Internet enabled digital technologies, and is an important skill for all people who seek to engage in technologically mediated discourse. Many people come to the Internet with 'some' to 'broad' skills in reading, which do not necessarily map directly onto all the skills needed to read online such as "extending thinking skills beyond the hierarchical, linear sequential model" (Sutherland-Smith, 2002, p 665). However, there is a debate about whether reading online is a new form of literacy, or that our standard and requirements of literacy have changed as Snyder (2008, p 219) states the definition of literacy has become multiple, adding weight to the conceptualisation of 'literacies' (p11). Generally, the term 'literacy' is thought to include the ability to 'read, write and communicate', which is embodied in UNESCO's definition of literacy as "an active process of learning involving social awareness and critical reflection, which can empower individuals and groups to promote social change" (UNESCO, 2005, p22). UNESCO's definition provides the basis for the increasing standard of literacy required to survive in a networked world, as a hyperconnected reader. UNESCO's focus is on the pre-digital and pre-networked literacies but provides a conceptualisation that may be expanded to digital environments.

UNESCO's goal of empowering users through the ability to critically reflect on information presented is an essential part of education and may be expanded to include web-based (and other) documents for Web users in the 21st century. Navigating the changing face of the information landscape requires some training beyond what has been traditionally considered sufficient for 'functional literacy', that is, the ability to

function within society. UNESCO (2005) points to the 1978 definition adopted by their General Conference, specifically:

> 'A person is functionally literate who can engage in all those activities in which literacy is required for *effective functioning of his [sic] group and community* and also for enabling him to continue to use reading, writing and calculation for his own and the community's development.' [1] (p 22, italics added)

Following from this, to be functionally literate, in the networked society, includes not only our traditional notions of literacy but also determining validity of information in online environments, and to be able to read hyperconnectedly with specific attention to all features of a page – visual and textual. This is increasingly complex given that the objective of most Web pages, and indeed advertising in general, is to attract your attention. This is complicated by search engine optimisation practices, which help businesses achieve high rankings and early appearance in search engine results pages, based on, among other things, keywords that match potential search terms. Search engine optimisation is a profitable business practice, which many companies validly use to good effect. However, these same techniques can be used to achieve high search engine rankings based on non-relevant or overly broad search terms and subsequently con unsuspecting Web users into spending money on non-existent items as in the example detailed herein and elsewhere (Furnell, 2005). A recent example of phishing includes that documented by Twitter, a microblogging website (see http://blog.twitter.com/2009/01/gone-phishing.html). Phishing is the "the practice of directing users to fraudulent web sites" (Dhamija Tygar Hearst, 2006, p581). Other forms of affiliate and fraudulent marketing may also result in link-spamming most noticeable in un-moderated forums, (Niu, Wang, Chen, Ma, and Hsu, 2007) blogs and wikis including comment spam, spam-blogs and link or spam farms (see Gyöngyi and Garcia-Molina, 2005 for a comprehensive taxonomy of web spam).

The literature reflects a concurrent concern about search engine rankings that often put scam sites high in search results (Burke, 2008). Such scam sites include non-official sites as well as sites designed to con unsuspecting users. Other concerns include the processes dictating the availability of or filtering out Websites from Library Pages because it is difficult to keep up with the changing Web and shifts in information from site to site (Joint, 2007). This kind of philosophy is also evident in the current attempts to filter 'unwanted content' (Foo, 2008a) on the World Wide Web, and perhaps the whole Internet, proposed by the Australian Government as part of their Cyber-safety Plan (DBCDE, 2008). These proposals raise further concerns, as stated by one member of the blogosphere:

> children will grow up expecting to be filtered, monitored, controlled and censored. Is this what we really want to teach them? Much better, I think, to teach them that freedom brings with it both dangers and responsibilities. (Seymour, 2008)

Hence, there is the need to train students in reading online, including "skills in locating relevant information from within an ever increasing volume, and using search engines, are especially important" (Verezub et al, 2008, np) and the skills to evaluate, holistically, the websites they find.

[1] While functional literacy is defined within UNESCO documents in terms of the literacy requirements for global development, this does not detract from the social situatedness necessary in such a definition. In a networked social situation, functional literacy is more nuanced and requires some attention to unravelling the level of literacy required to *function* in that social environment. This may be expanded to all previously defined literacies, specifically that individuals must be functionally literate within their social situation.

A further concern is the need to develop and understand new forms of literacy including "e-literacy, Hyper-literacy, or information or cyber-literacy" (Lewis, 2002, np). The emergence of these terms signals a shift in the way we read online. There are additional skills that we must employ to make sense of what we read. This is contrasted with the belief that search engine rankings imply endorsement of Websites by search engines by providing a form of 'authenticity by association' (Lewis, 2002), which calls into question our ready acceptance of information we find.

This paper uses the case of the 2008 Beijing Olympic online ticketing scam from August 2008 to investigate how some people were led into acceptance of information that was based upon fraudulent offerings, specifically, the sale of items (Olympic Tickets) that did not exist. The potential for public education to raise awareness about appropriate ways to evaluate and read online information is discussed. The paper concludes with a discussion of the potential for increasing literacy to ensure individuals are able to critically assess information they find online – to become hyperconnected readers.

Importance of Higher Levels of Literacy

There is no doubt that Information Literacy, that is, being able to assess the validity of information, is one of the most useful skills that can be developed through education (Verezub et al., 2008; McDougall, 2007). While there is much focus on digital literacy and e-literacy and increasing focus on visual literacy, there is a tendency to focus on the technical skills needed to participate in the Information Age (Golub, 2007). However, being able to assess the context of information provides individuals with a more discerning attitude towards information they receive or request. The 'success' of spam is suggested to be around 0.001 percent (Judge, 2003) of sent emails resulting in conversion, that is the sale of an item (Kanich, Kreibich, Levchenko, Enright, Voelker, Paxson, Savage, 2008). Unsolicited marketing email relies on individuals who may not yet be information literate and who accept the apparent legitimacy of offers with considerably large discounts, including those for various chemicals to enhance personal performance (eg Viagra for male sexual dysfunction). While people continue to believe (and investigate) these offers (Kanich, et al, 2008), spammers and scammers continue to offer them, as they are a lucrative source of information to facilitate their next scam, which may include identity fraud. Similarly, the greater awareness individuals have about the topic of their search for information, the more likely they are to critically review Web sites they interact with.

Previous research into online literacy includes Verezub et al.'s (2008) discussion of developing metacognitive strategies to enhance reading of online texts including becoming "proficient, aware, strategic or reflective readers". However, simply assessing a single source of text does not necessarily prepare individuals to identify fraud and scam sites. These sites require particular skills including metacognitive and critical skills and the ability to make connections between sites both visually and informationally as elaborated by Verezub et (2008). The next section seeks to demonstrate some of the critical skills that facilitate the recognition of potential scam sites, beginning with an analysis of what was so successful in the case of Beijingticketing.com.

Beijing Ticketing Scam

The Beijing Ticketing Scam became a major news story in the week leading up to the 2008 Olympics. Reports of people losing significant amounts of money made headlines with one report indicating 71 ticket scam websites had been identified by the International Olympic Committee (NineMSN, August, 7, 2008). Many people called for greater vigilance by official bodies to prevent such scams and asking why these sites were not taken offline (ABC News, August 4, 2008).

The Beijing Ticketing Scam is useful to highlight some of the indicators that should have raised questions in the minds of users and yet failed to "set off alarm bells" (Keizer, 5 August, 2008, np). Many reports tell of "computer savvy" and "internet entrepreneurs and software developers" being duped by the scams (Herald Sun, August 4, 2008). An analysis of this scam could show why those alarm bells should have been set off. Using known scams can effectively assist with providing examples of what to look for in e-commerce situations and to identify Web sites that should be avoided or reported to authorities.

Why Was the Scam So Successful?

Beijingticketing.com hit the news only days before the Olympics began (August 3) as people realised they were not receiving their tickets. Reports in the media indicated that individuals (in Australia) had lost sums as high as $AU 46000 with the total in the vicinity of $50 million (Magnay, 2008)[2]. Wills (2008, np) described the site as a "professional-looking site, which carried the official Beijing Games logo". This is confirmed by Keizer (2008, np), who describes the scam sites as being "particularly convincing, sporting professional designs and liberal use of Olympic logos". This can be seen in the screen capture of the site prior to its removal from the Internet (Fig. 1).

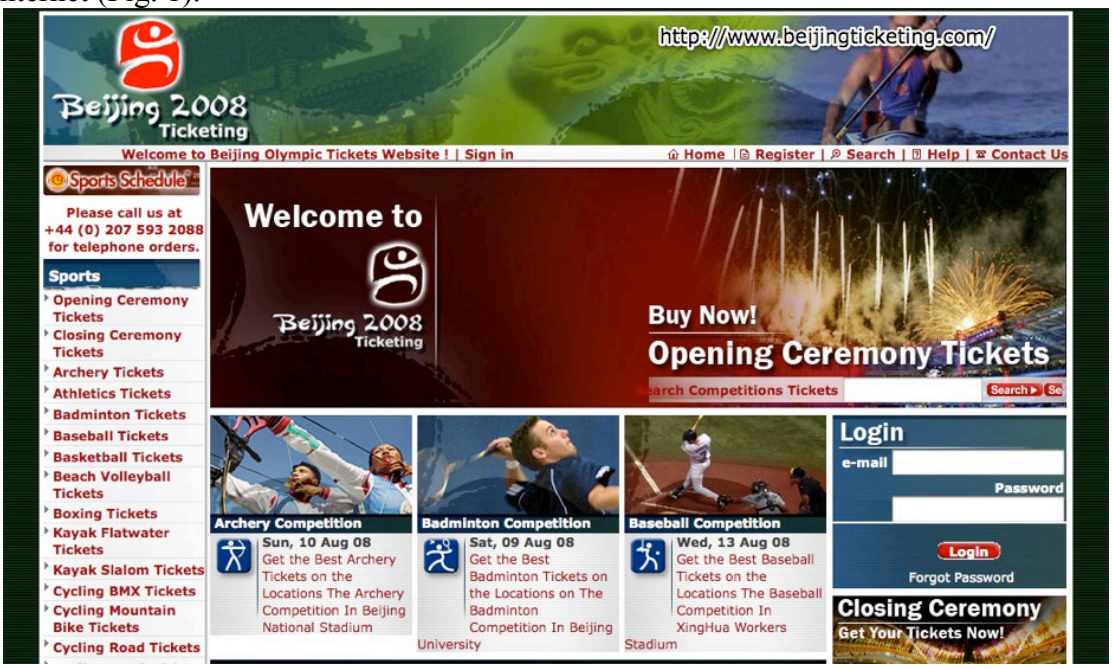

Figure 1: Screen shot of the scam Site

[2] These figures, reported by the mainstream media outlets, should possibly be subjected to the same critical treatment as scams and spam. Generally, a certain level of trust is implied in such figures being reported, although a healthy scepticism is still relevant.

The appearance of the Web site provided all the surface (visual) cues to enhance the confidence of users. There were ample pictures of sporting events using images sourced from previous Olympics, pictures of opening and closing ceremonies, the phrase "Buy Now" as well as a search facility to find exactly the event desired. It was an inviting site that tapped into the excitement associated with attending a world class, world-renowned event. However, visual analysis is not sufficient to determine validity of information.

The search engine optimisation techniques employed by the scammers were so successful that for a long time, it appeared at the top of search engine results pages (SERPS) for 'Beijing Olympic tickets', providing a quasi-officialness to the site (Burke, 2008) and causing individuals to place blame on Google. However, the scam site preyed on the narrow critical reading skills of the target audience, that is, people wanting to attend Olympic events, by providing them with what they thought was an 'official' site based on the search optimisation results and the general appearance of the site.

The Website included well-designed images (see Fig. 2) relating to security of information that could induce individuals to feel confident in the site. At one point in its history (see Internet Archive, 2008), it included not only a "satisfaction guarantee" and "safe and secure transactions" but also a "hacker safe" certification. These certifications can lead people to place trust in the site. A number of accrediting services exist primarily to enhance the trust users place in online commerce (see for instance McAfee Secure - http://www.mcafeesecure.com/us/merchants-intro.jsp) at what may be a significant cost to the business (Lanford and Hübscher, 2004).

Figure 2: Guarantees on the Website.

While it is easy to review the site as a known scam site, there are perhaps one or two signs that a deeper reading of the site may have provided to individuals who are both information literate and 'Olympic' literate. These signs did not appear relevant to a cursory analysis by some individuals (Keizer, 2008), but they were telling in light of the site being identified as a scam. The next section identifies these signs and outlines why they should cause caution.

How Could It Be Identified as a Scam?

The clues that indicate Beijingticketing.com was a scam were small and not significant enough to set off 'alarm bells' except perhaps in hindsight. One of the most obvious clues was the logo on the site and the 'favicon' or Favourites icon, which is used to bookmark sites. The favicon assists in establishing trust in the site, although many web surfers seem to be unaware of its relevance. Herzberg and Jbara (2008) discuss the potential for validation of favicons to enhance trust. However, many sites do not use favicons and some browsers do not display them. The favicon of the scam site was almost the same as the official site (see Fig. 3 for representations of the favicons of both sites). A cursory glance at the favicon is enough to evoke recognition

of the 'official' emblem of the Beijing Olympics. However, the two favicons are sufficiently different to arouse questions in the mind of a user, but only if the user is extremely familiar with the Olympic event.

	Actual Favicon (™ http://en.beijing.cn)
	Scam site Favicon (http://www.beijingtickets.com)

Figure 3: Screen capture of favicons for each site as they appear in the browser.

This is also the case with the logo used on the scam site. It is different from both its own favicon and the official emblem of the Beijing Olympics. There is sufficient similarity between the scam site's logo and the official Olympic emblem to invite more confidence and yet the differences should also 'ring alarm bells' of caution. Some reporters have described the site as 'carrying the official logo' (Wills, 2008) of the Beijing Olympics. However, early in the discussions in news sources, the logo was described parenthetically as "similar but not the same" as the Official Emblem (Magnay, 2008, np). Fig. 4 demonstrates that not only was the 'running figure' (BOCOG, 2008) dissimilar, but even the colour of the emblem was different. The figure in the Official Logo has more detail while the scam site was more stylised with much less detail. The colour of the scam logo was a deeper red and the scam logo was proportionately wider than the Official emblem. The scam logo also lacks the Olympic Rings that traditionally accompany all Olympic Emblems. These minute differences are easily overlooked and perhaps require extremely good eyesight, however, it remains that these details become obvious after the identification of the site as a scam and indicates the level of awareness individuals need to identify suspect sites.

	Official Beijing Olympic Emblem (™)
	Scam site Olympic Logo

Figure 4: Screen capture of the Official Olympics Emblem and logo of the scam site

While the scam website attempts to enhance its 'officialness' by its deceptive logo, it did not include the official slogan of the 2008 Olympics, "*One World, One Dream*". This is perhaps one indication of its non-affiliation with the Olympics and its status as a non-official and, indeed, illegal distributor of tickets.

Other sites that have been identified as potential scam sites include phrases such as "the only ticket agency with a 200% Order Guarantee" (http://www.olympics.bz/index.php) or "We ensure our orders with a 200% money back guarantee" (http://www.ticketcity.com/Sales-Policies.html), which has been interpreted as "double the refund if it failed to deliver the pre-purchased tickets" (KTUU.com, 2008). The evidence of this guarantee appearing on multiple Websites, with some purporting to be the 'only', is an indication of a scam.

The hacker safe certification linked to a certification site in the version stored in the Internet Archive for January 2008. This link did not appear in the live version viewed the day before the Website was removed. The appearance of a logo for a security company, whether or not an 'official' logo, provides the Website with a semblance of authenticity and leads individuals to greater levels of trust. The fact that these were not linked to any authenticating service after January is another sign to the limited trust viewers should place in the site.

The history of the scam site reveals how it became the top result in searches for 'Beijing Olympics Tickets'. Using the Way Back Machine (an archive of almost all content available on the web at http://www.archive.org/), we find the scam first appeared on 14 October 2007, just months after the official site (12 June, 2007). This indicates the length of time the scammers had to achieve their notoriety (specifically, high search engine results) as over one year. However, the belief that any Olympic committee could have achieved their removal without specific evidence is misplaced. There were no backlinks (links that would show up in the visitor statistics available to website owners) perhaps making it clear why it survived so long as there was no connection between the sites and individuals therefore visited the official sites for the Beijing Olympics through other paths. Had the scam site included such a link, the official Olympics Committee may have become aware of the site through these referrer links and been able to take action.

The frequency with which search results (particularly for news) give the same information at multiple sites from a single source potentially leads to a shallower approach to reading online (see for instance, Carr, 2008). Indeed, duplicate news items are identified by Google and can be included or excluded by the search engine. However, this does not mean the search engine is responsible. It is merely reacting to the tendency of news sources to pick up stories and republish them. Carr (2008) discusses how search engines, like Google, can potentially undermine our ability to reflect on information gained from Internet sources, and yet, we are spurred on by traditional news sources that simply re-present stories from the 'wire'. This process of repetition is indicative of the fast paced change in the information landscape with which we interact and it calls for a critical reading, and awareness of the hyperconnecteness of all information we find on the Web. Assessing each Website for the information contained in it, the quality of its design and the appearance of certifications can be a superficial approach to reading online. What is needed, rather, is to access each of the linked sites (the certification agencies) and any links to official bodies. These are activities that will assist readers to assess information and the authenticity of websites rather than implicitly trusting all sites on the Web. The Beijing ticketing site did not have any links to any official government or other Olympic sites within China, nor to the International Olympic Committee website.

The Beijing Ticket scam site seems to employ many scam techniques: staying out of official view; evoking the feel of a professional and official Olympic site; fooling even the most able and savvy users who seem to have succumbed to the effects of the site through their initial and cursory views (Wills, 2008). The enthusiasm for all things Olympic in an Olympic year seems to have worked in the scammers' favour. It is only through the process of registering to buy tickets that the nature of the site becomes clearer. The sheer amount of information requested to register is an 'alarm bell' that sets a scam site apart from others (Cortez, 2008). Requests for some information, such as credit card details and date of birth, should only be made at the time of purchase, if at all, rather than when signing up for information.

The Twitter Incident

Twitter, the microblogging site, was subjected to a phishing scam in early 2009. Individuals were sent a 'direct message' (a private message between two users) with a message such as "hey! check out this funny blog about you..." and a link. Because twitter messages are limited to 140 characters, a URL (universal resource locater) shortener is used resulting in a web link of the form http://tinyurl.com/ or a similar. These shortened links do not provide clues to the actual site one is visiting. However, the resulting site contains the full URL in the address bar of the browser. In the case of the phishing messages, the URLs of the sites were http://twitter.access-logins.com/ (a Facebook lookalike) and http://twitter.access-logins.com/login/[3] (a Twitter lookalike) rather than http://twitter.com. If a user logs into either of these sites, their login details are compromised. A number of web-savvy individuals fell for this scam. These scams often link back to the compromised site via links on the site (for example the 'About' page) and often the only clue to the nature of the phishing attempt is the URL of the initial page. This incident further highlights the need for holistic evaluations of web sites, which should include the URL of the web page.

Implications

The shifts being seen in the way we read are more than evident in both the literature and the above case. Carr (2008) complains that we have become superficial readers; that the speed at which information is presented prevents the deep reading required to fully comprehend it. However, Bawden's suggestion that "a complex and broad form of literacy is required" (2001, p 254) points to a need to become hyperconnected readers. This deeper understanding of literacy will likely enable most readers to analyse information and think critically about what they find.

The kinds of skills we need to develop go beyond Verezub et al's (2008) suggested analysis of a single source and suggest that comparative processes and continual reflection across different sources of information are needed – hyperconnected reading. Verezub et al's discussion focussed on interlinked information within a single web source (a horticultural website) gaining insights into "metacognitive strategies on hypertext comprehension" (2008, np). These metacognitive strategies within a single source are influential in reading online, however being able to critique information from multiple sources is a growing requirement of being literate in a hyperconnected information era. Understanding how information is interlinked and hyperconnected is a foundation skill. By building on these foundational skills and developing ways of identifying scams and other unsavoury practices will likely protect us better than a filtered web.

For teachers in networked classrooms, the skills and understanding of how phishing and other fraudulent practices work need to be embedded within their practice. Kumaraguru, Rhee, Acquisti, Cranor, Hong, Nunge, (2007) recommend embedding learning about phishing in a user's everyday context rather than directing them to a purpose built website. This allows the situated development of critical forms of literacy as highlighted by Turner (2007) above. Using known phishing web sites and other scams sites to demonstrate ways of identifying these sites allows students safely learn

[3] Both of these sites are now identified as Phishing sites by OpenDNS and a number of other services.

and question the pages they view. Thus students are afforded a wider range of premediate experiences (Billet, 2009) upon which to base future decisions.

Discussion

Whose responsibility is it to police scam sites and the Web in general? The options suggested in the literature are attempts at legislating protection for individual users similar to those discussed by Joint (2007) requiring librarians to vet and filter shifting information; similar programs currently under consideration by the Australian Government (Foo, 2008b) to block 'undesirable' content; or those of numerous other governments that filter internet information. Are we to rely on technology to keep us safe from technology?

Threats to individuals' perceptions of their own safety bring calls for more protection. However, like road safety for children, a more proactive educational program may be an alternative course of action. Road safety has succeeded by combining sensible rules and educational programs with increasing attention to the actions of road users, particularly children (see for instance, Lam, 2005). Internet safety, on the other hand, seems to be focussed on *prevention* of 'potential' rather than 'actual' harm, and blocking access to objectionable sites. Every week, a call seems to arise to defend people's sensibilities or to 'protect the children'. These calls, however, neglect the educational requirements of learning to live in a changing and hyperconnected world. Road safety campaigns have allowed us to live with changing technology (in this case cars, trucks, buses and motorcycles).

Learning to live with technology, both its good and bad aspects, is important and may be achieved through educating users and assisting in their analysis and assessment of Internet information in the form of Information Literacy, alternatively known as digital literacy, or e-Literacy which Verezub et al. (2008, np) describe as "literal, inferential and critical" reading and described here as hyperconnected reading. Such reading, when combined with general literacy of topics (for example knowing what the Olympic games are), may protect consumers and Web-users from known threats and scams and increase the likelihood of scams being identified early.

Calls to protect consumers from this kind of fraud reveal considerable challenges and problems for providers of information services. As Joint (2007) highlights, responsibility for filtering information from the Web is difficult, with trusted sites lapsing to the control of domain parking practices, that is, the use of a formerly well known websites or misspelt version of a page name (eg see the case of MikeRoweSoft.com in CNN, 2004), and page hijacking through the creation of 'rogue' Websites that emulate popular Websites. Search engine optimisation relies, in part, on tracking links to and from Websites. Referrer statistics (that is, how people found and accessed your site and what sites link to you) show where links are coming from (backlinks). The Beijing Ticket scam site did not link back to official sites.

Ironically, on the day of the commencement of the Olympics, there were still Websites selling tickets to the Olympics, which indicates that even when we know about them, they are hard to remove. Internet filtering techniques are not yet, nor likely will they be any time soon, sufficient to remove all threats to our safety. On the other hand, an educated populace will likely be more aware and armed against falling victim to these scams.

Conclusion

Just like learning to cross a road, learning to navigate the information landscape requires multiple layers of understanding. We deal with cars everyday and become familiar with their movement patterns and their capabilities. We are only just starting to learn the capabilities of the Web. Our Web safety relies on our understanding of the patterns of information, patterns that may be broken if calls to filter information from the Web are realised. While accidents do occur on the road, so too will some of us occasionally be conned.

The kinds of literacy needed to read online and to thwart being scammed are complex, requiring understanding of the relational patterns of information. These skills come from deeper analysis of Websites and consistent and reflective reading of information. Carr's (2008) concerns that we are losing our abilities for deep reading are perhaps true, given the frequency with which the phrase "information overload" occurs in our dealings with technology[4]. However, while we may feel pressed for time and skim read, blaming our overload on the technology is like blaming an accident on our need to get someplace in a hurry. However, the skills of 'reading', as posited at the beginning of this paper, are processes that do require development and this can only be done through conscious effort. Banning access to parts of the Internet and policing our usage is not sufficient to fix the problem due to inherent limitations of the technology (for a full list of issues and links to relevant information relating to the current Australian proposal see http://www.overclockers.com.au/wiki/Australian_Internet_Filtering).

Digital literacy and hyperconnected reading skills are more important than ever and provide a educational, rather than a technological, solution to a social problem. Using scam sites and similar processes where deeper readings reveal inconsistencies, as in the case of the Beijing Ticket Site, will not be possible with a censored and clean Web. All this will achieve is to open up the frontier for more cunning and harder to pick scams that we are not prepared to defend ourselves against. Just as no child (or adult) should be allowed free and unprepared access to roam the roads, so, too, we should train ourselves to read online. If we censor the Web, fail to call out harmful practices, and refuse to educate ourselves we may as well ban cars, trucks, buses and motorcycles from our cities.

References

ABC News, (2008), ACCC investigating Olympics ticket scam, *ABC Beijing 2008*, August 4, 2008, http://www.abc.net.au/news/stories/2008/08/04/2323589.htm, [viewed August 9, 2008].

Bawden, D., (2001), Information and digital literacies; a review of concepts. *Journal of Documentation*, 57 (2), pp. 218-259.

Billett, S. (2009) Conceptualizing learning experiences: Contributions and mediations of the social, personal, and brute. Mind, Culture, and Activity, 16(1), 32-47.

BOCOG, 2008, Beijing 2008 Emblem, International Olympic Committee website, http://www.olympic.org/uk/games/beijing/open_embleme_uk.asp [viewed 30 September, 2008].

[4] More than 1.5 million hits on Google for the phrase "information overload".

Bundy, A., (2004), One essential direction: information literacy, information technology fluency, *Journal of eLiteracy*, 1, 7-22

Burke, K., (2008) Bogus tickets still trading on internet, *Sydney Morning Herald*, August 7, 2008, http://www.smh.com.au/news/web/bogus-tickets-still-trading-on-internet/2008/08/07/1217702200817.html [viewed August 8, 2008].

Carr, N., (2008), Is Google making us Stupid? What the Internet is doing to our brains, *Atlantic Monthly*, July/August 2008 http://www.theatlantic.com/doc/200807/google, [viewed August 14, 2008].

CNN, (2004), Microsoft takes on teen's site MikeRoweSoft.com, CNN Technology, http://edition.cnn.com/2004/TECH/internet/01/19/offbeat.mike.rowe.soft.ap/index.html [viewed September 30, 2008].

Cortez, A., (2008), Phishers Play the Olympics, *TrendMicro*, http://blog.trendmicro.com/phishers-play-the-olympics/, [viewed August 8, 2008].

DBCDE, (2008), Cyber-safety Plan, Department of Broadband, Communication and the Digital Economy, Canberra http://www.dbcde.gov.au/communications_for_consumers/funding_programs__and__support/cyber-safety_plan [viewed January 5, 2009]

Dhamija, R., Tygar, J.D. Hearst, M., (2006), Why Phishing Works, Proceedings of the SIGCHI conference on Human Factors in computing systems, April 22-27, 2006 Montréal, Québec, Canada

Donnison, S., (2007), Digital Generation Pre-Service Teachers as Change Agents: A Paradox, *Australian Journal of Teacher Education*, 32 (4) http://ajte.education.ecu.edu.au/issues/PDF/324/Donnison.pdf

Foo, F., (2008a), Conroy coy on filtered web content, *Australian IT*, November 12, 2008 http://www.australianit.news.com.au/story/0,24897,24128728-15306,00.html [viewed August 8, 2008].

Foo, F., (2008b), Net censorship to cost users, *Australian IT*, August 5, 2008 http://www.australianit.news.com.au/story/0,24897,24128728-15306,00.html [viewed August 8, 2008].

Furnell, S., (2005), Internet threats to end-users:hunting easy prey, Network Security, July, 2005) 5-9.

Gee, J.P. (2000), Discourse and sociocultural studies in reading. Reading Online, 4(3). Available: http://www.readingonline.org/articles/art_index.asp?HREF=/articles/handbook/gee/index.html [viewed January 2, 2009]

Golub, E., (2007), Adding Societal Impact and Reflection to Information Technology Fluency Classes, *Journal of Literacy and Technology*, 8 (3), 47-62

Gyöngyi, Z., and Garcia-Molina, H., (2005), "Web spam taxonomy", Proceedings of the First International Workshop on Adversarial Information Retrieval on the Web (AIRWeb), 2005 in The 14th International World Wide Web Conference (WWW 2005) May 10 -14, 2005, Nippon Convention Center (Makuhari Messe), Chiba, Japan., New York, NY: ACM Press

Herald Sun, (2008), Olympic ticket scam dupes Australian, US and European fans, *Herald Sun,* August 4, 2008, http://www.news.com.au/heraldsun/story/0,21985,24124123-662,00.html, viewed August 9, 2008

Herzberg, A., and Jbara, A. (2008), Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks, *ACM Transactions on Internet Technology*, 8 (4) Article 16

Internet Archive. (2008), Beijingticketing.com search results for Jan 29, 2008 http://web.archive.org/web/20080129125519/http://www.beijingticketing.com/ [viewed August 9, 2008].

Joint, N., (2007), ‘‘When good sites turn bad’’: the ethics of digital libraries and internet legislation, *Library Review*, 56 (4), 278-284

Judge, P., (2003), The state of the spam problem, Educause Review, September/October 2003

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G.M. Paxson, V., Savage, S., (2008), Spamalytics: An Empirical Analysis of Spam Marketing Conversion, 15th Annual ACM Conference on Computer and Communications SecurityCCS'08, October 27–31, 2008, Alexandria, Virginia, USA.

Keizer, G., (2008), Olympic ticket scams just the start, says researcher, *Computer World*, August 5, 2008 http://www.techworld.com.au/article/255746/olympic_ticket_scams_just_start_says_researcher, [viewed August 8, 2008].

KTUU.com, (2008), Alaskans victims in Olympics scam, *KTTU TV*, August 6, 2008 http://www.ktuu.com/Global/story.asp?S=8806273 [viewed August 8, 2008].

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E. (2007), Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System, Proceedings of the SIGCHI conference on Human factors in computing systems, San Jose, California, USA

Lam, L.T., (2005), Parental risk perceptions of childhood pedestrian road safety: A cross cultural comparison, *Journal of Safety Research*, 36 (2), pp 181-187

Lanford, P., and Hübscher, R., (2004), Trustworthiness in e-commerce, Proceedings of the 42nd annual Southeast regional conference, ACM New York, NY, USA

Leu, D.J. Jr., Kinzer, C.K., Coiro, J.L., & Cammack, D.W. (2004), Toward a Theory of New Literacies Emerging From the Internet and Other Information and Communication Technologies, Edited by Ruddell, R.B., and Unrau, N.J., Theoretical *Models and Processes of Reading.* (5th ed.) International Reading Association, pp 1570-1630

Lewis, A., (2002), Hoax E-mails and Bonsai Kittens: Are You E-literate in the Docuverse? *First Monday*, 7 (8), August 2002, URL: http://firstmonday.org/issues/issue7_8/lewis/index.html [viewed August 9, 2008].

Livingstone, S., (2004), Media Literacy and the Challenge of New Information and Communication Technologies, *The Communication Review*, 7, 3–14.

Livingstone, S., (2008), "Internet Literacy: Young People's Negotiation of New Online Opportunities." Digital Youth, Innovation, and the Unexpected. Edited by McPherson, T. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press. 101–122. doi: 10.1162/dmal.9780262633598.101

Magnay, J., (2008), Ticket swindle leaves trail of losers, August 4, 2008, http://www.smh.com.au/news/latest-news/ticket-ripoff-leaves-trail-of-losers/2008/08/03/1217701854125.html [viewed August 9, 2008]

McDougall, J., (2007). Just Another Trendy Theory?: Finding Space in the Curriculum for Teaching Visual Literacy, *Journal of Literacy and Technology*, 8 (3), 23-46

NineMSN, (2008), Five charged in Olympics tickets scam, *Nine MSN*, Aug 7 2008 http://news.ninemsn.com.au/olympics/article.aspx?id=610209, [viewed August 8, 2008].

Niu, Y., Wang, Y., Chen, H., Ma, M., and Hsu, F., (2007), "A Quantitative Study of Forum Spamming Using Context-based Analysis," Proceedings of the 14th Annual

Network and Distributed System Security Symposium (NDSS), San Diego, CA, February, 2007.
Ruth, A. (2008), Don't Talk To Me About E-mail! Technology's potential contribution to bullying, *International Journal of Organisational Behaviour* 13, 2, pp 122-131
Schleppegrell, M. J., (2007), Len Unsworth, E-literacy for the language arts teacher, *E-literature for children: Enhancing digital literacy learning, Linguistics and Education*, 18 (1) Spring 2007, pp 93-95
Seymour, J., (2008) An alternative policy (v0.2): Filtered Network Providers (FNPs), http://broadbannedrevolution.blogspot.com/2008/01/alternative-policy-v02-filtered-network.html [viewed January 6, 2009]
Sutherland-Smith, W. (2002), Weaving the literacy Web: Changes in reading from page to screen *The Reading Teacher;* 55 (7), 662-669
Snyder, I., (2008), *The Literacy Wars*, Allen & Unwood, Crows Nest, Australia.
Symons, S., Langille, L. & Hemming, H., (2002), E-Literacy for the Workforce: Designing Effective Instruction. In G. Richards (Ed.), P*roceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2002* pp 1586-1589. Chesapeake, VA: AACE.
Turner, G., (2007), Cultural literacies, critical literacies, and the English school curriculum in Australia. *International Journal of Cultural Studies*, 10 (1), 105-114.
UNESCO, (2005), *Education for All, Literacy for Life*, EFA Global Monitoring Report, United Nations Educational, Scientific and Cultural Organization, Paris, France.
Verezub, E., Grossi, V., Howard, K. & Watkins, P., (2008), Building e-based literacy for vocational education and training students. *Australasian Journal of Educational Technology*, 24 (3), 326-338 http://www.ascilite.org.au/ajet/ajet24/verezub.html
Wills, K., (2008), Fraud victims turned away at Beijing Games opening, *Reuters*, August 8 2008, http://www.reuters.com/article/GCA-Olympics/idUSPEK23262120080808 [viewed August 18, 2008].

Acknowledgements

I acknowledge the ownership of the Trademarks (indicated by ™) used in this paper as belonging to the Beijing Organising Committee for the Olympic Games (BOCOG). Their use is for the sole purpose of demonstrating how trademarks may easily be confused by readers of web sites and does not imply BOCOG is in any way responsible, nor does it imply any endorsement of any products by the Author or BOCOG.