The security, privacy, and ethical implications of social networking sites

Warren, M. J. and Leitch, S. 2014, The security, privacy, and ethical implications of social networking sites. In Gupta, Manish (ed), *Handbook of research on emerging developments in data privacy*, IGI Global, Hershey, Pa., pp.329-338.

DOI: 10.4018/978-1-4666-7381-6.ch015

Chapter 15
The Security, Privacy, and Ethical Implications of Social Networking Sites

M. J. Warren
Deakin University, Australia

S. Leitch
RMIT, Australia

ABSTRACT

The chapter investigates the security and ethical issues relating to privacy and security. This chapter also examines the ethical issues of new forms of bullying that are being played out weekly in the media: cyber bulling, specifically on SNS such as Facebook. The traditional and direct forms of bullying are being replaced by consistent abuse via SNS due to the ease and accessibility of these new forms of communications.

BACKGROUND

The world has developed into a global community and the Internet is the thread that connects this global community. We have seen the Internet develop from the days of static web pages containing static information and static pictures (Web 1.0) to the current form of the Internet of today, Web 2.0. Today, Web 2.0 has moved away from utilising only static information and allows for the dynamic exchange of information through the use of video and audio. The important aspects of Web 2.0 is the social aspect of the technology development, which sees users generate new and ongoing content of pages via their interactions or commentary. We now see systems such as Facebook, Twitter being used by millions / billions of users across the global, this global usage results in developing ethical situations, this chapter explores two examples of social media and ethical situations.

DOI: 10.4018/978-1-4666-7381-6.ch015

INTRODUCTION

Information access, anytime, anywhere, any place, is one of the features of the twenty first century. Social Networking Sites (SNS's) are cyber spaces where people discuss ideas, share information, air their views and communicate to a global audience. SNS's such as Facebook, have become increasingly popular and are being used on a daily basis by millions of users across the globe. This vast usage can create fantastic opportunities but also brings with it a host of issues. One of these problems is the sharing of personal information with a wide audience and the associated security risks of doing so. The Internet has developed into a global social network and reflects many of the world wide social problems that society in general faces (Seendahera, 2009). This chapter examines a number of cases where physical, social and ethical situations have transferred into the technology mediated communication domains.

The chapter will investigate the security and ethical issues relating to privacy and security. This chapter will as well as examine the ethical issues of new forms of bullying that is being played out weekly in the media; that of cyber bulling, specifically on SNS such as Facebook. The traditional and direct forms of bullying are being replaced by consistent abuse via SNS due to the ease and accessibility of these new forms of communications.

SECURITY AND PRIVACY ISSUES OF SNS

Individuals often fail to understand the implications of making personal information public through SNS's such as Facebook. Research on various organisations by the Society of Corporate Compliance and Ethics and the Healthcare Compliance Association revealed that 24% of the organisations had disciplined their employees for inappropriate behaviour on SNS's and that this behaviour had caused embarrassment for the organisation (Whitney, 2009). For example, pictures uploaded by a finance industry employee disclosed a colleague faking a sick day and the subsequent outcome was that the employee lost their job (McCarthy, 2008).

Research also has shown that SNS's are leaking individual's identity information to third parties including data aggregators, which track and aggregate user's viewing habits for targeted advertising purposes (Warren & Leitch, 2014). One implication for users is having tracking cookies associated with their user identity information taken from their SNS profile. This makes tracking user's movement across several websites much easier. Although user identities are not directly available to third parties who track users through IP (Internet Protocol) addresses, these IP addresses can be easily related to a particular user and therefore disclose their personal information obtained through the SNS's (Vijayan, 2009). The leakage of personal information means that the third parties not only obtain a collated collection of users' behavior but can also discover the viewing habits of specific individuals (Krishnamurthy & Wills, 2009).

Personal information may also be made available through secondary leakage targeting external applications (Krishnamurthy & Wills, 2009). Facebook uses a large number of third party applications as a part of its platform; these are provided for entertainment, education and social purposes. However, Facebook does not have any control over the third party application providers and websites supported through its platform. Publicly available information is made available to these third party applications and websites once a user begins to use them. Before approving third party applications or websites, Facebook requires the providers to agree to Facebook's terms of user information disclosure and takes technical measures to ensure that only authorised information is delivered to these third party vendors. Estimates in 2011, identified 100,000 third

party applications that allowed information to be shared accidently between Facebook third party applications (BBC, 2011a).

SNS's enable malware to spread, which is due to malware's ability to access personal information. Increased use of SNS's such as Facebook and YouTube increase the chance of malware or peer phishing attacks that can potentially cause serious damage to organisational data security (Socialman, 2009). For example there were concerns regarding a data leak after a hacker broke into the 'Top Friends' application on Facebook' making users private information visible (Goldie, 2008). In 2012, a computer worm (Ramnit) stole 45,000 login credentials from Facebook users in the UK and France; this information could have been potentially used in a social engineering attack (BBC, 2012a).

Corporate organisations use SNS's for many different reasons. One use is to utilise their information to create strategic advantage by growing or gaining a competitive advantage. Another important use is that of a marketing tool in order to increase the organisation's business profile. Employees within the organisation generally create an organisational profile on Facebook as a way of informally communicating with customers, sharing information, promoting products, getting informal product feedback and building brand loyalties (New York Times, 2008). By building these organisational profiles, employees are able to communicate and interact with customers from all over the world, however this can result in data leakage and cause serious issues for the organisations as employees may accidently post information about the organisations latest products, for example, pictures of the latest iPhone.

Organisations may have concerns about Facebook and its usage; these concerns also relate to individuals that the organisation communicates with (employees, customers, etc.) and those individuals' right to privacy. Organisations can monitor current and potential employees through SNS's and some colleges and schools even keep track of their students' posts on SNS's. Police can use online information for investigative and tracking purposes (Jones et al, 2008), such as during the English riots of 2010. Facebook was used by the rioters to post information about their activities, and as a way to incite other individuals to join them in rioting. After the riots had ceased, police used the rioters posts as evidence to prosecute and imprison the individuals concerned (BBC, 2011b).

Facebook users can restrict certain information from being viewed from different cohorts, including friends. In 2009, Facebook altered its privacy settings, including the control over who sees individual messages (BBC, 2009). This meant that Facebook users could amend their access rights regarding information they posted so that specific individuals could, for example, view their postings but not their photos. In 2010, Facebook announced a new 'groups' feature that allowed users to specify circles of friends with whom they want to share data, in essence allowing users to categorise user friends and share information with only certain groups of friends (BBC, 2010). The ways in which information can be shared within Facebook is constantly changing, and one of the key issues is whether users are able to keep up with these changes and calibrate the settings so that their privacy is protected.

Another issue surrounding privacy and information safety in SNS's is the candidness of SNS's to communicate to users what information is private and what is public. This is clearly laid out in Facebook's policy documents, however, it is likely that very few of the 1.28 billion monthly users (Facebook, 2014) have taken adequate time to familiarize themselves with these documents and change their settings accordingly. Another privacy matter is trusting that those that have access to any personal information (such as those on a friend's list) will treat personal information, in the form of birth dates, status updates and photos in an ethical manner and not disseminate or use the information in an unethical fashion. This wholly relies on an individual and their own conscience, however it is prudent of users of such SNS's to take responsibility

for their own actions rather than blaming a SNS. Taking responsibility would include making sure that they check their privacy settings; only making information available that they are comfortable with sharing; and only adding people to their "friend list" who are actually friends, or known to the user, in keeping with the original purpose of Facebook, rather than the more recent use of adding as many "friends" as possible.

There is also the worrying trend of whether Facebook friends actually exist in reality. An internal review of Facebook's customer base identified 83 million illegitimate accounts (BBC, 2012b). These fake pages ranged from companies settings up individual profile pages, so that these fake individuals can "like" the companies products or services to fake pages setup for pets that can "like" and interact with their owners.

ETHICAL ISSUES OF CYBER BULLYING AND ANTISOCIAL BEHAVIOUR

In recent years there has been extensive research conducted in the sphere of bullying via electronic means, often termed cyber bullying. Previously, work undertaken in this arena was mainly in workplaces that used technology mediated communication means for group work, team and skill building. This chapter will look at cyber bullying in adolescent cases and online antisocial behaviour.

What constitutes bullying as opposed to everyday conflicts that often occurs with children and teenagers, is that bullying is defined as "repeatedly and over time, to negative actions on the part of one or more other students who are or perceived to be stronger" (Olweus, 1993). Bullying also highlight the motivation, where there is a genuine intent to cause harm and that the abuse is consistently repeated over a period of time, rather than an on-off conflict or argument (Whitney & Smith, 1993; Olweus, 1999, Mishna, 2011).

The traditional view of bullying in the school yard, such as name calling and other verbal abuse, physical assault, or humiliation, has now expanded into cyber bullying. Cyber bullying can take many forms and can refer to the use of emails, mobile communication messaging, website postings, blogging, and the misuse of pictures as a way to spread rumours, humiliate, isolate, embarrass of frighten those being victimised (Smith et al, 2006; Willard 2005).

Those engaging in bullying who are prepubescent tend to engage in direct bullying behaviours, whilst those who are in their teenage years move more towards cyber bulling. Female bullies tend to use less direct strategies than their male counterparts (Wolke, 2010). Unlike traditional bullying, cyber bullying is not only perpetuated by individuals against another individual. It is becoming more prominent for groups to become the attacker, perhaps due to the anonymity of the Internet and the fact that this anonymity can lead to individuals forming a group with a pack mentality. This pack mentality has developed into the concept of flaming, Flaming is defined as displaying online hostility by insulting, swearing or using otherwise offensive language (Moor et al, 2010). A United Kingdom study in 2008 reported that up to 10% of students had been cyber bullied (Smith et al, 2008) whilst a Canadian study undertaken in 2009 reported a rate of 35% (Cassidy et al, 2009). A predominant conclusion in much research (Olweus, 1993, Wilton, 2011) is that rather than having school policies push to eradicate bullying, a better method for extinguishing bullying would be to "teach" young people in the home about the unacceptable nature of bullying behaviour. This raises an even more important aspect relating to cyber bullying in that in a technologically savvy world many parents are unaware of their children's actions and behaviours online, due to them not being aware about how the SNS and other technologies work which results in them not closely monitoring what is occurring. It is easy for a parent to chastise bullying behaviour

between siblings or friends when it occurs in the home, but less easy to control and monitor such interactions and behaviours when they take place through technological means (Leitch & Warren, 2012) in an unmediated space.

Another element of antisocial behaviour is that of vigilantism. Whilst the perpetrators believe they are in the "right" and are defending others they are often engaging in the same behaviours as cyber bullies by defacing and attacking individual's SNS pages and engaging in patterns of harassment (Wehmhoener, 2010).

The chapter will explore a number of case studies and highlight the issues related to SNS's.

CASE STUDY 1: THE JESSI SLAUGHTER INCIDENT, A USA CASE

Based upon news reports (ABC 2010a, ABC 2010b, CBS, 2010 Farquhar, 2010). Jessi Slaughter was a pseudonym (real name Jessica Leonhardt) for an 11 year old girl (living in the USA) who rose to prominence in the media through dramatic events that unfolded through her use of SNS. The situation began with postings on a website called StickyDrama (which can be described as a blogging, rumour and gossip site contributed to by teenagers). The postings on this website accused Jessi of being involved with a member of a band, which she denied. She reacted to this by posting videos and content of herself and attacking the people she thought had defamed her. The situation escalated when individuals gained personal information including home phone numbers and Twitter account details about her and posted this information on various other sites. She was a victim of prank calls at home and she received numerous hate emails. In spite of this, Jessi continued to taunt the anonymous posters by blogging and commenting on the situation (Mathieu, 2011). In a final act, the young girl created a video which was subsequently posted on YouTube, in which she delivered a tearful and angry rant to those perpetuating the acts, at one point her father is present in the video and delivers his own angry message to the anonymous posters. This video brought global attention to Jessi and the issue of cyber bullying and received over 785,000 views.

An important aspect of the case study was that personal information related to Jessi was posted on 4Chan. 4Chan is a simple image based bulletin board where anyone can post comments and share images and is governed by a site set of rules that do not allow "flaming" (4Chan, 2012). What happened was that Jessi story appeared on the message boards of 4Chan, with the threats against Jessi coming fast and furious (ABC, 2010a). This enflamed the situation even further. A sad aftermath of the situation was that people made fun of Jessi by making parody videos of her (including song remixe's and comedy sketches) and posted them on YouTube. The most popular of these videos received over 900,000 views on YouTube.

Jessi's story highlights a number of ethical issues which, depending on the perspective of the parties involved, will change the interpretation of the case. In regards to Jessi Slaughter, a major issue was the ability and desire of an 11 year old to post inappropriate material on SNS. Another concern was the sub optimal parental control and the lack of awareness regarding her online activities.

Another factor was the action of the 4Chan site which allowed for the systematic attack on an 11 year old (legally a child) by anonymous posters, enabling the use of SNS to escalate an issue rather than reporting the inappropriate material to legal authorities. Further, posts on 4Chan breached their own behaviour rules; they were unable to police themselves, and remove, or stop bullying posts.

These ethical issues highlight that SNS's have a social responsibility to have some control over the content and behaviour of those using their services. In recent years SNS have taken active steps to control bullying issues, however incidences have not decreased dramatically

regarding the number of cyber bullying cases, neither have the severity of the cases diminished. The governance of these services are clearly lacking.

CASE STUDY 2: THE IMPACT OF PUBLIC OPINION, AN AUSTRALIAN CASE

In Australia, the murder of Trinity Bates in Queensland, Australia in February 2010 saw much Internet actively, including Facebook pages being set up. Some were tribute sites to mourn the loss of a child, others were hate sites set up by web vigilantes against the man accused of the murder. The Queensland Premier sent an open letter to Facebook's CEO asking "what it will do to block the 'sickening' hijacking of Internet memorials?" (Herald Sun, 2010). Whilst the Queensland Premier was concerned mainly about the users posting Internet pornography and other inappropriate material on the memorial sites, of as much concern was the ethical issue surrounding the use of Facebook to vilify and prejudge the accused defendant. The man charged with the murder has been named in the mainstream press, but the vigilantes went further, posting much more personal information, such as addresses and information about the defendant's family members. Facebook answered the letter by releasing a statement from its US based director of communications and public policy. Defending Facebook's monitoring systems, the response stated that users could draw attention to offensive content by clicking on a "report" button beneath any post on the SNS. This answer has done little to placate people who feel their grief has been compounded by the actions of a few; they fail to understand why there is a lack of control and limited monitoring taking place on many SNSs (The Australian, 2010a).

The comments on the vigilante sites may have major consequences for legal trials and could lead to them being aborted. This could mean that jury selection could be put at risk because the process of innocence until proven guilty could be compromised. In terms of the Trinity Bates example, how could someone have a fair trial in Queensland, when public opinion has already found a person guilty?'' (The Australian, 2010b). It appears that governments are struggling to deal with new media and are playing catch up with methods of dealing with the legal issues that arise from SNS use in these situations. This incident has clearly highlighted the lack of security and monitoring on SNSs, but also the ethical issues that emerge when free speech on which such sites are based collide with legal pejoratives. The fact that such software could severely impact our judicial system, a fundamental core of society, means that this is an issue of great importance to all societies and requires higher regulation. Facebook currently has a low user to staff ratio with only 1000 staff across the world, therefore there are simply not enough resources to manage all the information that has been uploaded and posted in real time (The Australian, 2010b).

The solution to this situation is complicated. One option may be to employ more staff and put structures and boundaries in place to clearly define what is considered unacceptable Facebook behaviour. In doing this, however, we are then fundamentally changing the core of Facebook and allowing a third party (government or public opinion) to decide what is, or is not, acceptable to society (Leitch & Warren, 2011). A more successful long term strategy would be to improve education and self regulation of such sites, but success is dependent upon the reliance of most people to act in a responsible manner and set their own rules and boundaries. As a result of the Trinity Bates case, the Australian Federal Government announced that they will create an online ombudsman to deal with concerns regarding SNSs and inappropriate content (The Australian, 2010c). The plan was later abandoned.

The sheer number of people using SNS makes it difficult to monitor misuse, both for law enforcement officials and site administrators. Tim Sparapani (Facebook's Director of Public Policy) estimates that Facebook users spend 18 billion minutes on the site each day. "We have 400 million active users and a tiny, tiny staff. We need to find novel ways to handle that kind of crushing amount of activity. It's the burden of being so immensely popular," (Time Magazine, 2010).

Some victim advocates believe that, as well as offenders losing civil liberties when they are found guilty of a crime, they should also lose their "cyberliberties" (Time Magazine, 2010). Each SNS is dealing with these issues in different ways and governments are strategizing to put into place policy and law to minimise the risks. Facebook currently bans people who have been convicted of sexually based offences but has no specific policy for those convicted of other sorts of crimes; "policing" this policy is, not surprisingly, difficult, and therefore, a number of countries and states have been required to bring about their own legislation. The US state of Illinois, has made it illegal for sex offenders to use SNS, and if found doing so can be charged with a felony offence. In the UK, however, plans to do something similar have been thwarted as it was believed these plans breach human rights law (Doward, 2009). The issue arose when it was revealed that the police would be asked to share sex offenders' details and email addresses with SNS administrators. These types of policies do not deal with the "average" cyber bully who may not have a criminal record. In the same way, identifying and prosecuting traditional bullying behaviour in schools and workplaces is challenging when we add in the electronic means of delivery, the 500 million users of SNS, along with the veil of anonymity, and the "right to free speech, the expectation that cyber bullying can be reduced in the near future is unlikely.

It is further demoralising that the US Federal Communications Decency Act clearly states that, "web sites aren't responsible for harassment by users" (Davis, 2009) and therefore cannot be held legally liable. This fact does little to calm the users who are becoming increasingly frustrated with the lack of concern regarding personal privacy and security from abuse and bullying.

CONCLUSION

In conclusion, the security and privacy threats that exist within the general Internet community also relate to SNSs. In many cases these risks are greater due to the sheer number of SNS users as well as the fact that users place their trust in safeguarding personal information in their friends' hands. As the number of SNS users and third party applications increase, so will the security risks.

The chapter focuses on two case studies, one relates to the USA and one to Australia. In both of these cases the ability not to resolve the ethical dimensions resulted in the cases becoming escalating to major incidents. The impact of SNS and the Internet has brought great benefits to society. The problem is, it has brought negative issues as well, with many of the negative issues mirroring the physical world, in particular the issue of cyber bullying or the smearing of good causes. This chapter has highlighted the weakness of SNS providers to protect against these issues; this weakness could be due to limited governance models or the ability of SNS providers to react in real time to incidents.

FUTURE RESEARCH DIRECTION

The future research direction will be focused on analysing future ethical situations in relation to social media and learning lessons from those ethical situations. This analysis would help to inform the contributed debate about the global social impact of social media.

REFERENCES

American Broadcasting Company (ABC). (2010a). *'Jessi Slaughter' says death threats won't stop her from posting videos on the internet*. Retrieved from: http://abcnews.go.com/GMA/Technology/jessi-slaughter-viral-tweens-violent-online-rant-spurs/story?id=11224731

American Broadcasting Company (ABC). (2010b). *Do kids need more privacy protection on social networks?* Retrieved from: http://abcnews.go.com/WN/social-networking-privacy-kids-protected-online-world-news/story?id=11831552

BBC. (2009). *Facebook gives users more control of privacy*. Retrieved from: http://news.bbc.co.uk/2/hi/technology/8404284.stm

BBC. (2010). *Facebook unveils 'groups' feature and user controls*. Retrieved from: http://www.bbc.com/news/technology-11486427

BBC. (2011a). *Facebook profile access 'leaked' claims Symantec*. Retrieved from: http://www.bbc.com/news/technology-13358293

BBC. (2011b). *Four on trial accused of using Facebook during riots.* Retrieved from: http://www.bbc.co.uk/news/uk-england-lancashire-15382412

BBC. (2012a). *Worm steals 45,000 Facebook passwords*. Retrieved from: http://www.bbc.com/news/technology-16426824

BBC. (2012b). *Facebook has more than 83 million illegitimate accounts*. Retrieved from: http://www.bbc.com/news/technology-19093078

Cassidy, W., Jackson, M., & Brown, K. N. (2009). Sticks and stones can break my bones but how can pixels hurt me? Students' experiences with cyberbullying. *School Psychology International*, *30*(4), 383–404. doi:10.1177/0143034309106948

CBS. (2010). *'Jessi Slaughter' YouTube cyberbully case: 11-year-old tells GMA she didn't want it to go this far*. Retrieved from: http://www.cbsnews.com/8301-504083_162-20011349-504083.html

4 . Chan. (2012). *Rules*. Retrieved from http://www.4chan.org/rules

Davis, W. (2009). *Facebook harassment suit could spur cyberbullying laws*. Retrieved from: http://www.mediapost.com/publications/index.cfm?fa=Articles.showArticle&art_aid=114854

Doward, J. (2009). Bid to block pedophiles from Facebook fails. *The Guardian.* Retrieved from: http://www.theguardian.com/technology/2009/nov/08/facebook-sex-offenders-law

Facebook. (2014). *Statistics*. Retrieved from: http://newsroom.fb.com/company-info

Farquhar, P. (2010). *Jessi Slaughter and the 4chan trolls - The case for censoring the internet.* Retrieved from: http://www.news.com.au/technology/jessi-slaughter-and-the-4chan-trolls-the-case-for-censoring-the-internet/story-e6frfro0-1225894369199#ixzz1lHbLxHqO [

Goldie, L. (2008). Facebook to discuss security with ICO after data leak. *New Media Age*. Retrieved from: http://www.nma.co.uk/news/facebook-to-discuss-security-with-ico-after-private-data-leak/38591.article.

Herald Sun. (2010). *Governments powerless to stop Facebook vandalism, says IT expert*. Retrieved from: http://www.heraldsun.com.au/.../governments-powerless-to-stop-facebook-vandalism-says-itexpert/story-e6frf7jx-1225834291255

Jones, S., Millermaier, S., Goya-Martinez, M., & Schuler, J. (2008). Whose space is MySpace? A content analysis of MySpace profiles. *First Monday*, *13*(9). doi:10.5210/fm.v13i9.2202

Krishnamurthy, B., & Wills, C. (2009). On the leakage of personally identifiable information via online social networks. In *Proceedings of 1st ACM Workshop on Online Social Networks*. Barcelona, Spain: ACM. doi:10.1145/1592665.1592668

Leitch, S., & Warren, M. (2011). The ethics of security of personal information upon Facebook. In ICT ethics and security in the 21st century: New developments and applications (pp. 46-65). IGI Global.

Leitch, S., & Warren, M. (2012). Cyber-bulling and vigilantism: Should social media services be held to account. In *Proceedings of Sixth Australian Institute of Computer Ethics Conference*. Melbourne, Australia: Academic Press.

Mathieu, S. E. (2011). *Misogyny on the web: Comparing negative reader comments made to men and women who publish political commentary online*. (Thesis: Master of Arts). University of Missouri, Columbia, MO.

McCarthy, C. (2008). You, there: Step back from the webcam. *Cnet News*. Retrieved from: http://news.cnet.com/8301-13577_3-9853908-36.html

Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2011). Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims. *Children and Youth Services Review*, *34*(1), 63–70. doi:10.1016/j.childyouth.2011.08.032

Moor, P., Heuvelman, A., & Verleur, R. (2010). Flaming on YouTube. *Computers in Human Behavior*, *26*(6), 1536–1546. doi:10.1016/j.chb.2010.05.023

New York Times. (2008). *How to use social networking sites for marketing and PR*. Retrieved from: http://www.nytimes.com/allbusiness/AB11702023_primary.html

Olweus, D. (1993). *Bullying in schools: What we know and what we can do*. Oxford, UK: Blackwell Publishers.

Olweus, D. (1999). Sweden. In P. K. Smith, Y. Morita, J. Junger-Tas, D. Olweus, R. Catalano, & P. Slee (Eds.), *The nature of school bullying: A cross-national perspective* (pp. 7–27). London: Routledge.

Seendahera, V., Warren, M., & Leitch, S. (2011). A Study into how Australian banks use social media. In *Proceedings of PACIS '11*. Brisbane, Australia: Academic Press.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, *49*(4), 376–385. doi:10.1111/j.1469-7610.2007.01846.x PMID:18363945

Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). *An investigation into cyberbullying and its forms, awareness and impact and the relationship between age and gender in cyberbullying*. Research Report, University of London. Retrieved from: http://www.antibullyingalliance.org.uk/downloads/pdf/cyberbullyingreportfinal230106.pdf

Socialman. (2009). *Allowing staff to use Orkut? Better take care*. Social Unwire India. Retrieved from: http://www.social.unwireindia.com/2009/07/allowing-staff-to-use-orkut-better-take-cover

The Australian. (2010a). *Bligh hits out at sick net sites*. Retrieved from: http://www.theaustralian.com.au/politics/state-politics/bligh-hits-out-at-sick-net-sites/story-e6frgczx-1225834063831

The Australian. (2010b). *Facebook vandal complaints futile.* Retrieved from: http://www.theaustralian.com.au/australian-it/facebook-vandal-complaints-futile/story-e6frgakx-1225834303404

The Australian. (2010c). *Online ombudsman for Facebook woes*. Retrieved from: http://www.theaustralian.com.au/australian-it/online-ombudsman-for-facebook-woes/story-e6frgakx-1225834756343

Time Magazine. (2010). *How prisoners harass their victims using Facebook*, Retrieved from: http://www.time.com/time/business/article/0,8599,1964916,00.html#ixzz0gb2oD8Ge

Vijayan, J. (2009). *Social networking sites leaking personal information to third parties.* Retrieved from: http://www.networkworld.com/news/2009/092409-social-networking-sites-leaking-personal.html

Warren, M., & Leitch, S. (2014). *Be safe, be social*. IDG Communications.

Wehmhoener, K. (2010). *Social norm or social harm: An exploratory study of internet vigilantism.* (Masters Thesis). Iowa State University.

Whitney, I., & Smith, P. K. (1993). A survey of the nature and extent of bullying in junior/middle and secondary schools. *Educational Research*, *35*(1), 3–25. doi:10.1080/0013188930350101

Whitney, L. (2009). *Employers grappling with social network use*. Retrieved from: http://news.cnet.com/8301-10797_3-10360849-235.html

Willard, N. (2005). *Educators guide to cyberbullying and cyber threats*. Centre for Safe and Responsible Internet Use. Retrieved from: http://www.csriuorg/cyberbully/docs/cbcteducator.pdf.

Wilton, C., & Campbell, M. A. (2011). An exploration of the reasons why adolescents engage in traditional and cyber bullying. *Journal of Educational Sciences and Psychology*, *1*(2), 101–109.

Wolke, D. (2010). Bullying: Facts and processes. *Worcester Medicine*, *74*(4), 13–15.

ADDITIONAL READING

Kamel, N., Boulos, M., & Wheeler, S. (2007). The emerging Web 2.0 social software: An enabling suite of sociable technologies in health and health care education. *Journal of Health Information and Libraries*, *24*(1), 2–23. doi:10.1111/j.1471-1842.2007.00701.x PMID:17331140

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. doi:10.1016/j.bushor.2009.09.003

Pallegedara, D., Warren, M., & Mather, D. (2013) Ethical Aspects of Controlling Information Disclosure on Social Networking Sites, *Proceedings of the 7th Australian Computer Ethics Conference*, Melbourne, Australia.

KEY TERMS AND DEFINITIONS

Facebook: Online system to allow exchange of information between agreed parties.

Internet: An interconnected system of networks that connects computers around the world via the TCP/IP protocol.

Risk: The possibility of suffering harm or loss; danger.

Security: Something that gives or assures safety, such as measures adopted by a government to prevent espionage, sabotage or attack, or measures adopted, as by a business or homeowner, to prevent a crime.

SNS: Social Networking Site.

Social Networking: A term to describe websites that allow people to join a social network and exchange information with their online friends.

Threat: An indication of impending danger or harm.

Web 1.0: Web pages from earlier Web applications, the information is static.

Web 2.0: Web pages from current Web applications, the information is dynamic and interactive.