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