

Social Networking and Online Privacy: Facebook Users' Perceptions



DEIRDRE O'BRIEN* AND ANN M. TORRES**

ABSTRACT

This study investigates Facebook users' perceptions of online privacy, exploring their awareness of privacy issues and how their behaviour is influenced by this awareness, as well as the role of trust in an online social networking environment. A cross-sectional survey design is used. The sample frame is a network of Facebook friends; 285 survey responses were collected giving a response rate of 47.5 per cent. The study reveals over half of Facebook users have a high level of privacy awareness; however, an element of uncertainty is evident. Privacy concerns are prevalent especially relating to third parties' access to Facebook users' information. Over three-quarters of users have changed their privacy settings to tighter controls, prompted largely by privacy concerns. The most active period for change to privacy settings was 2010, reflecting a response to the controversy surrounding Facebook's privacy approach. Only one-quarter of users trust Facebook, yet the majority of users believe both Facebook and users have an equal obligation to protect users' information.

Key Words: privacy; trust; social networking; Facebook

INTRODUCTION

The social networking phenomenon is consuming the lives of millions of users around the world. Since the inception of the first social networking site, SixDegrees.com in 1997 (Boyd and Ellison, 2008), the social networking craze has grown beyond all expectations. Nielsen (2009) reports two-thirds of internet users are using social networking and blogging sites. The rate of adoption of social networking sites continues to grow as individuals search to become part of a virtual community, to share opinions and to connect and socialise with people of similar interests (Chaffey et al., 2009). Social networking users appear to be

* Tourism Ireland

** Department of Marketing, J.E. Cairnes School of Business & Economics, NUI, Galway

comfortable living a part of their lives openly and freely through online networks, often oblivious to the risks (Rosenblum, 2007). While privacy risks tend to be underplayed on social networking sites, the reality is the public sphere that is the internet means millions of users around the world are interacting and socialising in an extremely open and public environment. Unless protective controls are actively used social networking users risk losing control over their personal information, which subsequently erodes online privacy. Leading social networking site Facebook recently reached a milestone of 500 million users (Wortham, 2010). Since the website became a public access model in 2006 the growth of the website has been extraordinary: Facebook has developed and commercialised rapidly, introducing new features and services for Facebook users. However the continued development has come at a price to the user: a loss to their privacy. Facebook users continue to exhibit growing concern regarding lapses in privacy on the online social network. The concern reached its peak in December 2009 when Facebook, by default, made all users' information publicly available (Rothery, 2010). The controversy surrounding Facebook's continued lapses in privacy has been in the media spotlight in recent months and the topic of privacy on social networking sites has become a worldwide debate. This study examines Facebook users' perceptions of online privacy in a social networking context. Facebook users' current awareness of privacy issues and the influence of this awareness on behaviour are closely examined. Privacy is strongly related to trust. Once Facebook users' privacy perceptions are established trust levels on Facebook are also assessed.

The paper begins with an overview of the current body of literature assessing the concepts of trust and privacy in an offline, online and social networking environment. Leading social networking site Facebook is then closely examined in terms of its business evolution and subsequently the change in its attitudes towards privacy. The literature is followed by a breakdown of the methodology employed for this research study. The findings section presents the results of the cross-sectional survey instrument used within this study, while the discussion translates this data into meaning and assesses its importance relative to the current body of literature available. The paper concludes with a brief overview of the practical and theoretical implications of the findings and outlines future research paths.

LITERATURE REVIEW

The concepts of privacy and trust are inextricably linked. Seigneur and Jensen (2004) recognise both a link and conflict between the two concepts. 'Privacy refers to the moral right of individuals to avoid intrusion into their personal affairs by third parties' (Chaffey et al., 2009: 139). Privacy of personal information is one of the main spheres of the concept of privacy (Mills, 2008) and the main focus within this study. Seigneur and Jensen (2004) highlight that information can be classified as personal when it can be connected with or linked back to a certain individual. Caudill and Murphy (2000) admit it is not true to classify personal information as the opposite of information available in the public domain, but rather personal information encompasses both public and private information. The public fraction of personal information continues to increase as the internet facilitates the ease of gathering and distributing customer information (Caudill and Murphy, 2000).

Central to the concept of privacy is the notion of control, and the entitlement an individual has to exercise the desired control over their personal information (Van Dyke et al., 2007). A breach of privacy 'occurs when an organisation in its efforts to pursue the organisation's objectives collects, stores, manipulates or transmits personal information unbeknownst to the individual,' (Hann et al., 2007: 15), thus compromising an individual's control over their personal information.

'Trust is a complex and abstract concept, it is difficult to define and to identify the elements that construct it' (Wang and Emurian, 2005: 107). Trust has been defined as 'a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviours of another' (Rousseau et al., 1998: 395). Trust has additionally been classified as 'social complexity reducing strategies' (Gefen et al., 2003: 55): a requisite in human behaviour and therefore a means of achieving human cooperation (Patton and Josang, 2004). Trust is also described as cognitive (an opinion), affective (a feeling) and conative (a choice) (Koehn, 2003). Koehn (2003: 7) recognises that while trust has been defined and interpreted in many different ways, a common element does exist: 'an expectation of goodwill'. Ability (skills and competencies), benevolence (concern for the other party) and integrity (character of an individual) are the three widely accepted dimensions of trust (Mayer et al., 1995).

Seigneur and Jensen (2004) recognise a link and conflict between these two concepts. Both concepts are concerned with knowledge about an individual (Seigneur and Jensen, 2004). Knowledge must be shared in order for trust to exist, while privacy is concerned with protecting or containing knowledge. Conflict can emerge in striving for these desired ends. In order to achieve trust, information must be shared between two entities; the more knowledge is shared the greater the bond of trust that can be formed (Seigneur and Jensen, 2004). However the sharing of information openly between two entities in turn will lead to a loss of privacy to either or both parties (Seigneur and Jensen, 2004). While conflict exists the reality is trust and privacy are inextricably linked. Metzger (2004: 1) argues 'trust is perhaps the most important influence on information disclosure'. Privacy, in turn, is strongly linked to control. An individual has control over their personal information and must be willing to release control in order to part with, or openly disclose, personal information. A certain level of trust must exist for individuals to be willing to sacrifice control over their information, or they will seek something of value in return (Olivero and Lunt, 2004). As privacy concerns rise trust levels will be affected, which in turn will restrict interactions and exchanges between entities and vice versa.

The transfer of trust to the online environment amplifies the importance of trust. Wang and Emurian (2005) emphasise trust is context dependent. The nature of the online environment, in terms of being 'less verifiable [and] less controllable', creates a greater need for trust online (Gefen, 2002: 3). The lack of physical contact, loss in social cues and limited web interface all contribute to creating an unknown environment and unfamiliar process, generating fear and uncertainty among internet users (Gefen et al., 2003; Metzger, 2004). Bart et al. (2005) highlight the fact that the focus of trust online relates to the website, the internet as a channel and the technology. Online trust concerns 'consumer perceptions of how the

site would deliver on expectations, how believable the site information is, and how much confidence the site demands' (Bart et al., 2005: 134). Lee and Turban (2001) emphasise that other important elements of online trust include the internet merchant themselves and the trust placed in them by the consumer, trustworthiness of the internet as a distribution or consumption channel, and company size and reputation. Wang and Emurian (2005) identify a number of characteristics of both trust and online trust. While there are many similarities between the characteristics of online and offline trust, some differences exist. Firstly, similar to traditional trust, in online trust two parties must exist: the trustor online represents the consumer and the trustee is the website (Wang and Emurian, 2005). Secondly, in an online setting an unfamiliar environment exists. Wang and Emurian (2005) note that this environment enables merchants to behave in an unpredictable manner, creating an exposed environment that warrants the need for trust. This insecure environment meets the vulnerability characteristic of trust. Thirdly, the vulnerable environment leads individuals to take risks (actions) (Wang and Emurian, 2005). Online, actions relate to two specific behaviours: browsing and shopping. The final characteristic of trust relates to a subjective matter. Online, the level of trust needed per transaction varies from individual to individual and also from transaction to transaction (Wang and Emurian, 2005). This characteristic is similar to traditional trust. However, attitudes to technology also come into play in the online environment when considering a subjective viewpoint (Wang and Emurian, 2005).

There are a number of barriers to trust in the online environment. These barriers include perceived risk, website design and content, the user themselves and privacy concerns. Privacy concerns are considered the greatest barrier of them all because 'the internet, by design, lacks unified provisions for identifying who communicates with whom; it lacks a well-designed identity infrastructure' (Leenes et al., 2008: 1). Privacy concerns include online information collection techniques such as cookie technology involving extreme surveillance. The use and analysis of data is also a concern due to unethical merging and data mining practices to profile customers (Tavani, 2011). The instant recording and permanence of activity, loss of control and ownership of data also create barriers to online activity (Tavani, 2011). Overcoming privacy concerns online is crucial in order for trust to develop, which in turn prompts online activity including purchases, repeat purchases and positive word-of-mouth (Liu et al., 2005). Van Dyke et al. (2007) and Metzger (2004) recognise high privacy concerns can affect trust levels online and in turn constrain an individual's willingness to transact or interact online. Liu et al. (2005) present a privacy-trust behavioural intention model which depicts the importance of providing online users with control (notice, access, choice and security) over their personal information to overcome privacy concerns and enable trust to develop. Sheehan and Hoy (2000) re-emphasise the importance of control to the concept of privacy by also highlighting a number of control factors likely to influence an individual's level of privacy concern. These factors include awareness of information being collected, information usage, information sensitivity and familiarity with the entity collecting the information.

The heightened importance of trust online and the greater need for privacy online is evident within the context of online social networking. According to Boyd and Ellison

(2008), the concept of social networking sites is concerned with building links with existing contacts and displaying one's social network online and also instigating relationships with new contacts, who share similar interests and views, in an online environment. In a social networking environment the focus is centred on openness and sharing of information. Trust is a central factor in the social exchange theory and considered an important factor in information disclosure (Dwyer et al., 2007). Individuals assess the benefits against the risks in a social exchange, and trust is vital in encouraging individuals to partake in the exchange and disclose information (Metzger, 2004). This assessment is considered relevant within a social networking environment. In terms of privacy in a social networking context, a privacy paradox, as suggested by Barnes (2006), exists. Social networking users claim to be concerned about risks to privacy, yet do little to safeguard their information (Dwyer et al., 2007). Often users openly disclose detailed and personal information on these networks, comfortable living a part of their lives online (Rosenblum, 2007). Debatin et al. (2009) argue the desire for social interaction by social networking users outweighs their concerns about privacy and disclosure of personal data, while Rosenblum (2007: 47) believes social networking users 'don't exercise the same common sense because they conceive of themselves as interacting in a protected environment'. However, there are many privacy risks on social networking sites including the instant recording and documentation of information creating lasting digital dossiers, identity theft, stalking, damage to reputation, undesired contact, loss of control and risk of third parties accessing users' information (Debatin et al., 2009; Mannan and van Oorschot, 2008; Rosenblum, 2007). While most research notes a carefree attitude towards or lack of awareness of the risks associated with sharing personal information on social networking sites, new research has observed changing trends. Madden and Smith (2010) recognise more and more social networking users, especially younger adults (18–29 years), are growing increasingly vigilant and conscious of their online activity as they now consider the reputation and dossiers they are creating and making available to employers, co-workers and friends.

METHODOLOGY

Case Study

An exploratory case study is the chosen research method for this study. Upon review of the significant body of literature on social networking sites and online privacy and trust, Facebook was considered the most endemic social networking site associated with these issues. The literature review, along with the continued climb in users, despite the controversy surrounding Facebook and its approach to privacy, deemed the social networking site the most suitable for this study. Examining Facebook as a case study enables a thorough understanding to be gained into the characteristics and operations of the social networking site. The case study formula also helps to dissect the social networking site's overall stance on privacy, the prime focus of this research study. This secondary research method helps lay the foundations for this study before proceeding to the primary research method, which involves exploring Facebook users' perceptions of privacy in a social networking context. The study is concerned with uncovering the level of awareness of privacy risks on

the social networking site by Facebook users and assessing how this awareness influences their online behaviour, thus exploring relationships; that is, how awareness influences behaviour. The project subsequently explores the concept of trust in a social networking context in an attempt to 'seek new insights' on the role of trust in a social networking environment (Robson, 2002: 59). In light of the recent controversy surrounding privacy on Facebook, this study aims to examine Facebook users' current perceptions of privacy. The study is therefore cross-sectional as it examines perceptions of privacy at one particular moment in time.

Case study research is a multi-method research approach and involves adopting a number of data collection and analysis techniques, including qualitative and quantitative methods. This overall research approach enables a comprehensive study to be developed offering a thorough insight into the complexity of the social networking phenomenon. The methodology section therefore begins by offering a background description on the case study of Facebook compiled from an in-depth review of secondary data resources relating to the social networking site, including books, journal articles, newspaper articles and the policies and guidelines within the social networking site. The research design in the form of a survey design is then presented with a breakdown of both qualitative and quantitative data collection and analysis techniques used to examine Facebook users' perceptions of privacy and trust on the social networking site.

Background Case Description

Facebook and Privacy

In recent months, the issue of privacy on social networking sites has come to the forefront as a result of the media controversy surrounding the social networking site Facebook. Facebook, the number one social networking site, has 500 million active members (Wortham, 2010) and continues to climb. The success of the network site is credited to its 'simple design [and] broad demographic appeal' (Nielsen, 2009: 9). Facebook began as a social networking website restricted to United States college students. However in 2006 the site became a public access model (Fletcher, 2010). The subsequent growth and expansion of the social networking site has been unprecedented. Facebook statistics reveal 50 per cent of active users log into Facebook every day, and the average user has 130 friends and is linked to 60 pages, groups and/or events (Facebook, 2010). Facebook sees 25 billion pieces of information shared a month, 1 billion unique images posted a week and the 'Like' button clicked on average 100 million times a day (Fletcher, 2010), demonstrating the popularity of the website. Previous studies by Govani and Pashley (2005), Gross and Acquisti (2005) and Jones and Soltren (2005) show Facebook users disclose high levels of accurate personal information on the social networking site. Debatin et al. (2009: 102) found Facebook users have a large number of Facebook friends (300+) to whom a high level of personal information is disclosed, and the study concluded Facebook networks often represent a 'loosely defined group'. The data shared on Facebook 'feeds a bottom line' (Fletcher, 2010: 23) and has strong commercial value. Information on social networking sites is increasingly accessible to advertisers and marketers, prospective employers, universities and state

institutions (Debatin et al., 2009; Rosenblum, 2007). The growing accessibility of users' information means a growing loss of privacy.

Facebook has continually introduced new features and services including the Newsfeed, Facebook Beacon, Facebook Advertisements and Facebook Platform, which subsequently lead to changes in the privacy settings and the privacy policy (less privacy) (Fletcher, 2010). Table 1 presents a timeline of Facebook's actions that have caused privacy concerns for its users over a four-year period. With each additional expansion to the website has come a growing level of discontent and concern and a general feeling that 'the company was eroding privacy and making substantial information public' (Rothery, 2010: 23). In December 2009 the concern reached a peak when Facebook, by default, made users' information publicly available (Rothery, 2010). Facebook have continually made it possible for users to control their privacy settings to protect their personal data and limit who has access to this information; however users do not always employ these safeguards. Rothery (2010: 23) notes many users 'are not aware of this option [to change privacy settings] and find it confusing and complicated to navigate'. Govani and Pashley (2005) report that the majority of Facebook users (84 per cent) are aware of privacy risks on the social networking site and of the option to adjust privacy settings; however many users (48 per cent) fail to make any adjustments. Gross and Acquisti (2005) found only 1.5 per cent of Facebook users surveyed adjusted settings, Jones and Soltren (2005) found 64 per cent made changes and Debatin et al. (2009) found 69 per cent of users adjusted their settings. Kirk (2010: 102) notes Facebook's settings are 'confusing, frequently change and some users aren't aware of the options, putting their personal data at risk'. Bilton (2010) highlights the fact that, prior to May 2010, Facebook users had to tackle 50 settings and 170 choices in order to be able to manage their privacy settings on the social networking site. Mannan and van Oorschot (2008) believe if social networking sites provided easy-to-use and easily accessible privacy tools attitudes and behaviour towards online privacy would change. A study conducted by Hoadley et al. (2010), investigating Facebook users' responses to the introduction of the News Feed and Mini Feed in 2006, supports this view. Hoadley et al. (2010) highlight in their study the importance for social networking sites to provide easy-to-use interfaces for privacy settings, to enable users to adjust their privacy settings to suit their individual preferences. The study found Facebook users actually enjoyed the News Feed once Facebook provided substantial control mechanisms. Control is central to achieving online privacy and providing users with the ability to manage their information clearly influences their attitudes and behaviour towards privacy issues, and in turns their trust in the social networking site.

Facebook's privacy policy puts forward a detailed overview of how Facebook uses and shares information with third parties. The policy also presents advice on the steps users should take to ensure their personal information meets their desired privacy. The policy emphasises that the onus is on the user to take the necessary steps to protect themselves and highlights the risks involved if steps are not taken. However research shows the majority of Facebook users do not read the privacy policy. Govani and Pashley (2005) found 80 per cent of Facebook users surveyed had not read the privacy policy and Jones and Soltren (2005) found 89 per cent of Facebook users failed to review the policy. Bilton

(2010) points out that Facebook's privacy policy is a lengthy, tedious and complex 5,830 words and arguably a main reason why so many users have not read the privacy policy.

The changes made by Facebook to their privacy settings in December 2009 and the subsequent introduction of Instant Personalisation (where third-party websites piggyback on users' activities) in April 2010 spurred the recent debate on the topic of privacy and

Table 1: Profiling Facebook

6 September 2006	News Feed: Users are given a stream of updates about their friends' activities and changes to their profile on Facebook.
24 May 2007	Facebook Platform: Platform is the use of social networking APIs (Application Programming Interface) which integrates third-party content into a social networking site and when a user interacts with this content gives the third party access to this information (Felt and Evans, 2008). Third parties can then interact with the 'open graph', which is a profile of all users and how they interact on these websites and with whom.
September 2007	Non-Facebook members are allowed to search users' profiles (which are not access restricted) (Mannan and van Oorschot, 2008).
6 November 2007	Facebook Beacon: Users' activity on third-party sites is shared with friends, e.g. purchases on third-party websites. Users were automatically enlisted, causing huge uproar relating to privacy concerns. Facebook was forced to apologise for the controversy and make the Beacon feature an opt-in system. In December 2007 Facebook users were given the option to completely turn off Beacon. On 21 September 2009 Facebook announced the cessation of the Beacon Feature (O'Neill, 2009).
6 November 2007	Facebook Ads: Marketers can target audiences based on users' behaviour and activity on the website.
4 December 2008	Facebook Connect: 'Portability feature' whereby an individual's Facebook profile follows them around the web and enables a user to comment on other sites without actually having to be registered to the other site; development of Facebook Platform.
9 February 2009	Like Feature: A button is added to Facebook whereby users can inform friends they are fans of particular content they are clicking on within the social networking site.
December 2009	Rollout of complicated privacy settings: By default, Facebook users' information is made publicly available to everyone on the internet. This action generates huge controversy and many groups speak out in opposition (Rothery, 2010).

(Continued)

Table 1: (Continued)

21 April 2010	Open Graph: Involves extending the 'Like' button to third-party websites whereby a user surfing the web can click the 'Like' button on content across the website. 'Like' buttons are clicked almost one million times a day, providing a wealth of customer information to the company. Open graph aims to develop new content and identify further links with other users on Facebook, encouraging further interaction; another development of Facebook Platform.
21 April 2010	Instant Personalisation: Where third-party websites are allowed 'piggyback' on users' activities on the website to enable more tailored offerings and recommendations. Users, like with Beacon, were again automatically enrolled.

Data source: Fletcher (2010)

social networking sites and has placed Facebook in the media spotlight (Fletcher, 2010). The continued protests and negative media attention eventually prompted Facebook to re-evaluate its privacy controls. In May 2010 the company introduced simple user-friendly controls to enable users to effectively protect themselves online. Despite the continued criticism of Facebook and its approach to privacy, millions of new accounts are set up each month (Brustein, 2010). Facebook is increasingly been seen as a social utility: 'services everyone uses, no matter how much people dislike them' (Brustein, 2010: 1). The term 'satisfice', introduced by Herbert Simon in 1956, is relevant to the Facebook phenomenon. 'Satisfice' unites the words 'satisfy' and 'suffice' and recognises that people often make choices based on their friends' activities, although they are not completely satisfied with the service or customer experience (Hesseldahl, 2010). In other words, people become tolerant of dissatisfactory elements in order to share in experiences with others. Hesseldahl (2010) recognises this tolerance within a social media context, which also holds true in the case of Facebook. The lack of alternatives also helps to cement Facebook's dominance in the social networking marketplace (Brustein, 2010).

Facebook and Trust

The literature has highlighted the importance of overcoming privacy concerns in order to achieve trust in an online context. The question emerges as to whether the issues regarding privacy on the social networking site Facebook has caused trust levels to suffer as a result. A study conducted by Acquisti and Gross (2006), during the early stages of Facebook, reveals users' trust in Facebook was greater compared with members of other social networking sites like Friendster and MySpace. This finding is supported by Dwyer et al. (2007) who note higher trust levels on Facebook in comparison with MySpace. However, Facebook's business model has changed from its original format which was the focus in the Acquisti and Gross (2006) and Dwyer et al. (2007) studies. Facebook's original model was based on a closed system for university and college use, and control and privacy were at the heart of the social networking structure. Rothery (2010: 24) makes reference to Kurt

Opsahl, a senior legal representative at the Electronic Frontier Foundation (EFF), a digital rights advocacy and legal organisation, who said:

Facebook originally earned its core base of users by offering them simple and powerful controls over their personal information. As Facebook grew larger and became more important, it could have chosen to maintain or improve those controls. Instead, it's slowly but surely helped itself –and its advertising and business partners – to more and more of its users' information while limiting the users' options to control their own information.

Facebook appears to have lapsed in the development of appropriate privacy controls for its users while expanding the development of its overall business model. As identified in the literature review, restricting an individual's control over their information online causes privacy concerns and adversely affects trust levels.

Research Design

The research design adopts a survey research design. According to Bryman and Bell (2007), a survey research design is where data are collected primarily through questionnaires or structured interviews and involves examining more than one single case. This research study involves initially conducting focus groups to help inform the development of the prime research, the survey. The population for the research study is active Facebook users.

Focus Groups

Qualitative research, in the form of focus groups, is used as part of the research design to generate discussion around the topics of online privacy, trust and social networking among a small sample of social networking users. The discussion provides an insight into online behaviour of social networking users and also examines their attitudes to privacy and trust in the social networking context. The focus groups have a key role to play in the development of a survey questionnaire. According to Ghuari and Grønhaug (2002: 109), focus groups produce 'very rich and in-depth data expressed in respondents' own words and reactions'. Analysis of the focus group involves qualitative analysis and entails identifying emerging themes, and summarising and categorising data collected. Domegan and Fleming (2007: 160) recognise focus groups can compliment further investigations as they help 'develop ideas and insights before proceeding toward further investigation into the topic of interest'.

Survey

Quantitative research in the form of a cross-sectional survey is being employed for this research and represents the second and prime stage of the research design. Survey research employs 'a fixed questionnaire with pre-specified questions' (Sudman and Blair, 1998: 154). The focus group analysis is being used to inform the formulation of the survey. The survey enables a large amount of data to be collected relating to Facebook users' perceptions of online privacy in a social networking site. It is important for this study to obtain views and opinions from a large number of Facebook users so that meaningful comparisons and conclusions can be drawn. The survey research enables standardised

questions to be asked across a large sample and facilitates ease of comparison (Saunders et al., 2009), and is therefore considered an appropriate research method for this study. Quantitative analysis in the form of statistical analysis is being used to examine the data gathered through the survey.

Data Collection: Focus Groups

Three focus groups were conducted in 2010 with active Facebook members from three different age groups – 18–21 years, 22–29 years and 30 years plus – to observe different attitudes and concerns relating to privacy and trust in an online social networking context. (For the cross-sectional survey research the 22–29 age group was divided into two groups: 22–25 and 26–29 years.) The focus group results showed that an element of uncertainty exists with regard to privacy issues on Facebook and also uncovered a contradiction in terms of privacy concern and social networking behaviour; that is, while concerns were evident, Facebook users openly share detailed personal information on Facebook and happily communicate and interact in this public forum. (Focus group results are presented in Table 2). These findings helped guide the development of the cross-sectional survey.

Data Collection: Survey

The survey aims to examine Facebook users' level of awareness of privacy issues on the social networking site to determine how this awareness influences behaviour and to uncover the level of trust that exists on Facebook. The survey sample frame is represented by a network of Facebook friends (the researcher's Facebook friends and friends of friends). The study was undertaken in 2010. The survey was distributed to 600 active Facebook users and 285 responses were collected, representing a response rate of 47.5 per cent. As the target audience for the cross-sectional survey is Facebook users, a web-based survey was considered the most appropriate data collection instrument. Survey Monkey, a web-based tool, was employed for the design, distribution and analysis of the survey instrument. A Facebook e-mail was sent directly to the researcher's Facebook friends and friends of friends, inviting Facebook users to participate and directing them to the web-based survey instrument. Twenty-three questions in total comprised the survey. These questions were generated by reviewing the literature, adopting and adapting questions from previous successful research studies (Govani and Pashley, 2005; Gross and Acquisti, 2005), extracting statements from Facebook's privacy policy and using statements generated in the focus group discussion. Analysis involved descriptive statistics, filters, cross-tabulations and running analysis across age groups.

Survey Monkey: A Research Tool

Survey Monkey is an online tool that assists in the design, distribution and analysis of web-based surveys. A web-based survey enables the fast rollout of the survey and was considered the best format for the sample audience to complete the survey in a fast and efficient manner. Descriptive statistics are used to present the results of the different measures used in the survey and analysis was undertaken across age groups. Responses are filtered to help uncover patterns within the data and provide a 'subset of overall data to be

Table 2: Focus Group Results

Section A: Social Networking Use and Activity			
Key Topics	Group 1: 18–21 Years	Group 2: 22–29 Years	Group 3: 30+ Years
<i>Social Networking Sites (SNS) used</i>	<ul style="list-style-type: none"> Facebook 	<ul style="list-style-type: none"> Facebook Twitter LinkedIn 	<ul style="list-style-type: none"> Facebook LinkedIn
<i>Purpose for using Facebook</i>	<ul style="list-style-type: none"> To keep in touch with friends at home/in college 	<ul style="list-style-type: none"> To keep in touch with friends Snooping 	<ul style="list-style-type: none"> To keep in touch with friends and family Snooping
<i>Activities on Facebook</i>	<ul style="list-style-type: none"> 'Everything': posting comments and links, updating status, uploading photos, snooping, clicking the 'Like' button, joining groups, and using games and applications 	<ul style="list-style-type: none"> Mainly snooping; also will join groups and click 'Like' button regularly Occasionally will post information, make comments, update status, upload photos, and use games and applications 	<ul style="list-style-type: none"> Mainly photos, snooping and also will join many groups and click 'Like' button regularly Occasionally will post information, make comments, update status, upload photos, and use games and applications
<i>Third parties on Facebook</i>	<ul style="list-style-type: none"> Advertisements: take little notice and never click through Games/applications: realise games/apps are run by third parties 	<ul style="list-style-type: none"> Advertisements: realise they are highly targeted, never click through Games/applications: realise games/apps are run by third parties and understand third parties gain access to one's profile in return for use 	<ul style="list-style-type: none"> Advertisements: some thought the ads were targeted while others did not agree; never click through Games/applications: believe games/apps are run by Facebook, while others thought they were run by third parties

(Continued)

Table 2: (Continued)

Key Topics	Group 1: 18–21 Years	Group 2: 22–29 Years	Group 3: 30+ Years
<i>Duration spent on Facebook</i>	<ul style="list-style-type: none"> • Two/three times a day • Length of time depends on who is online 	<ul style="list-style-type: none"> • Once–four times a day • Whenever online • Generally few minutes per log in • Varies depending on who is online 	<ul style="list-style-type: none"> • Once/twice a day • Once to three times a week • Once every two weeks • Few minutes per log in
<i>Friends</i>	<ul style="list-style-type: none"> • 200 plus to 300 plus and 'no idea' • Classify Facebook friends as 'friends and acquaintances' • Would accept friend request from someone who was known though not known that well • Would ignore friend request from strangers 	<ul style="list-style-type: none"> • 100 to 300 plus and 'no idea' • Know every one of their Facebook friends to greet but would not engage in conversation with all • Would ignore friend request from people not known well • Would ignore friend request from strangers 	<ul style="list-style-type: none"> • 80 to 100 • Know every friend on Facebook friend list very well • Cautious and selective in choosing and accepting friends • Would ignore friend request from people not known very well • Would ignore friend request from strangers
Section B: Privacy and Trust Issues on Social Networking Sites			
Key Topic	Group 1: 18–21 Years	Group 2: 22–29 Years	Group 3: 30+ Years
<i>Privacy settings/policy</i>	<ul style="list-style-type: none"> • Have adjusted privacy settings (some since start, others recently in line with Facebook changes) • Found them easy to understand but took a long time to change • Have not read privacy policy 	<ul style="list-style-type: none"> • Have adjusted privacy settings (some since start, others more recently in line with Facebook changes) • Some found them difficult to find and use, others found them easy to interpret but took a long time to complete • Have not read privacy policy 	<ul style="list-style-type: none"> • Have adjusted privacy settings (recently in line with Facebook changes) • Needed to be shown where to change settings and how • Found them difficult to understand • Have not read privacy policy

(Continued)

Table 2: (Continued)

Key Topic	Group 1: 18–21 Years	Group 2: 22–29 Years	Group 3: 30+ Years
<i>Security risks</i>	<ul style="list-style-type: none"> • Aware of viruses • Would recognise them • Not sure who is responsible 	<ul style="list-style-type: none"> • Aware of viruses • Would recognise them • Believe hackers are responsible 	<ul style="list-style-type: none"> • Aware of viruses • Would not recognise them unless informed of threat • Not sure who is responsible
<i>Privacy concerns</i>	<ul style="list-style-type: none"> • Uneasy about information being sold to third parties • Don't think about risks when online 	<ul style="list-style-type: none"> • Worry about lack of control • Concerned about stalking • Don't think about risks when online 	<ul style="list-style-type: none"> • Concerned about identity theft • Worried about employers and prospective employers gaining access to their profiles and online activity • Concerned about threats moving offline (stalkers, robbery if away)
<i>Information disclosure</i>	<ul style="list-style-type: none"> • Don't disclose anything if they wouldn't want others to see • Believe Facebook is public place • Believe profile is restricted but think others can gain access to information 	<ul style="list-style-type: none"> • Don't disclose anything if they wouldn't want others to see • Cautious with what is disclosed • Believe Facebook is a public place • Believe profile is restricted but think others can gain access to information – unsure how 	<ul style="list-style-type: none"> • Minimal posting • Cautious with what is disclosed • Take steps to restrict access but believe others can still gain access to information – unsure how

(Continued)

Table 2: (Continued)

Key Topic	Group 1: 18–21 Years	Group 2: 22–29 Years	Group 3: 30+ Years
Trust	<ul style="list-style-type: none">• Trust friends• Have no control over other users – will ask friends to take something down• Don't see a need for trust of Facebook – not disclosing anything that warrants the need for trust	<ul style="list-style-type: none">• Trust friends• Have no control over other users – will ask friends to take something down• Don't see a need for trust of Facebook – not disclosing anything that warrants the need for trust	<ul style="list-style-type: none">• Trust friends• Have no control over other users' behaviour but recognise the ability to control who to be friends with (very selective)• Don't see a need for trust of Facebook – not disclosing anything that warrants the need for trust

analysed' (Survey Monkey, 2010: 1). Cross-tabulations are additionally employed whereby two or more variables are analysed simultaneously: 'the premise is to look at the responses to one question in relation to responses to one or more other questions' (Domegan and Fleming, 2007: 438).

Validity

To ensure face validity for this study, the literature on privacy and trust was extensively examined, which enabled the key themes to emerge and in turn helped formulate valid focus group questions. Efforts to maintain validity in the focus group research method involved evaluating the focus group questions after each discussion to ensure the appropriate topics – to answer the research questions and objectives – were covered. Amendments were made to the list of questions when topics emerged in the discussion not foreseen by the researcher. With regard to the survey instrument, reviewing the literature, adopting and adapting questions from previous studies, extracting statements from Facebook's privacy policy and using statements generated in the focus group discussion within the survey instrument helped ensure face validity of the survey questions.

Reliability

To ensure reliability within this research, a pilot test of the survey instrument was conducted to verify the survey questions were properly worded and appropriate for the chosen target group. How the survey was administered also helped ensure reliability within this research study. The survey was distributed through a systematic e-mail with accompanying cover letter providing clear instructions on how to complete the survey, and was also administered through the web-based survey tool Survey Monkey. Survey Monkey helped ensure the layout and format was clear and instructions were provided with individual questions so respondents knew exactly what was being asked and how to answer the question. Additionally, Survey Monkey enables automatic data compilation helping to reduce human error in data input, contributing to the reliability of this study.

Limitations of the Research Study

Convenience sampling was chosen as the most viable sampling technique; therefore caution is warranted in the generalisability of the results. The survey was distributed through the researcher's Facebook friends and friends of friends. Given the age of the researcher, the majority of the sampled respondents occupy the 22–25 age group. However, every effort was made to access other age groups through friends of friends. A risk of response bias is possible because the survey was distributed through the researcher's Facebook friends. Response error is also a possible limitation where social desirability might have been a guiding factor over honest and truthful remarks. Participants may have disclosed answers they believed the researcher wanted to hear. There is a risk of item response as a small number of survey respondents did not complete all answers on the survey; however because the number of missing values is so small it is unlikely to affect the overall results.

RESULTS

Characteristics of Study Sample

Table 3 provides an overview of the basic characteristics of the study sample.

Table 3: Characteristics of Study Sample

Participants	Males N=126 %	Females N=159 %	Total N=285 %
Gender	44.2	55.8	100.0
Age category			
18–21 years	27.0	17.6	21.8
22–25 years	52.4	60.4	56.8
26–29 years	12.7	10.7	11.6
30+ years	7.9	11.3	9.8
Facebook member for:*			
3 years	23.0	30.2	27.0
2 years	35.7	37.7	36.8
1 year	28.6	20.8	24.2
Less than a year	12.7	11.3	11.9
Reasons for joining Facebook			
A friend suggested it	74.6	64.8	69.1
Received a promotional e-mail	1.6	2.5	2.1
To keep in touch with existing friends/family	57.9	66.7	62.8
To track down old friends/family members	11.9	20.8	16.8
To express opinions	4.8	1.3	2.8
To meet new people	4.8	3.1	3.9
To get a job	—	0.6	0.4
To find a date	—	—	—
To look at others' profiles	19.8	13.8	16.5
Other	4.8	1.3	2.8

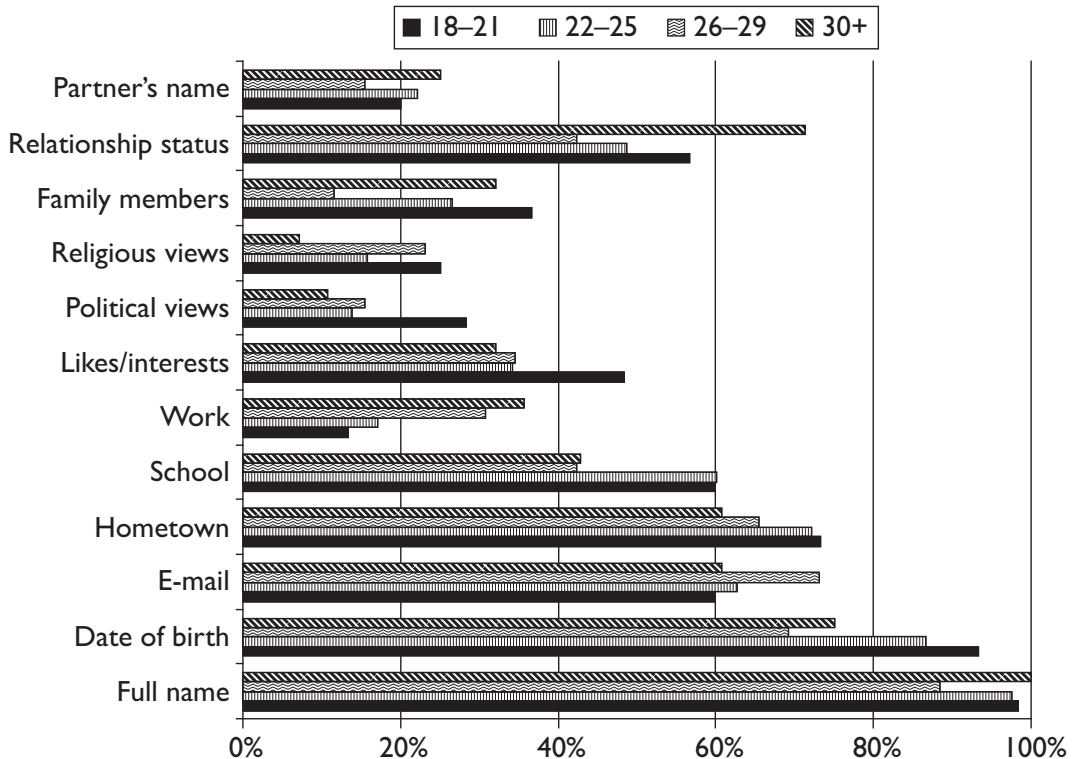
* Facebook member: How long has a Facebook user been a member/user of the social networking site

Information Disclosure, Activity and Use

The vast majority of all respondents disclose their full name (97.1 per cent), date of birth (85.3 per cent), hometown (70.6 per cent) and e-mail (62.9 per cent) on their Facebook profile. More than half (52.2 per cent) disclose their relationship status and 56.6 per cent reveal their schooling details. Facebook users surveyed are least likely to disclose phone

numbers, both home numbers (1.8 per cent) and mobile numbers (9.9 per cent). Figure 1 provides details of the main information types disclosed by Facebook users across age. Overall, the youngest age group examined (18–21) disclose the most information.

Figure 1: Information Disclosure on Facebook across Age Groups

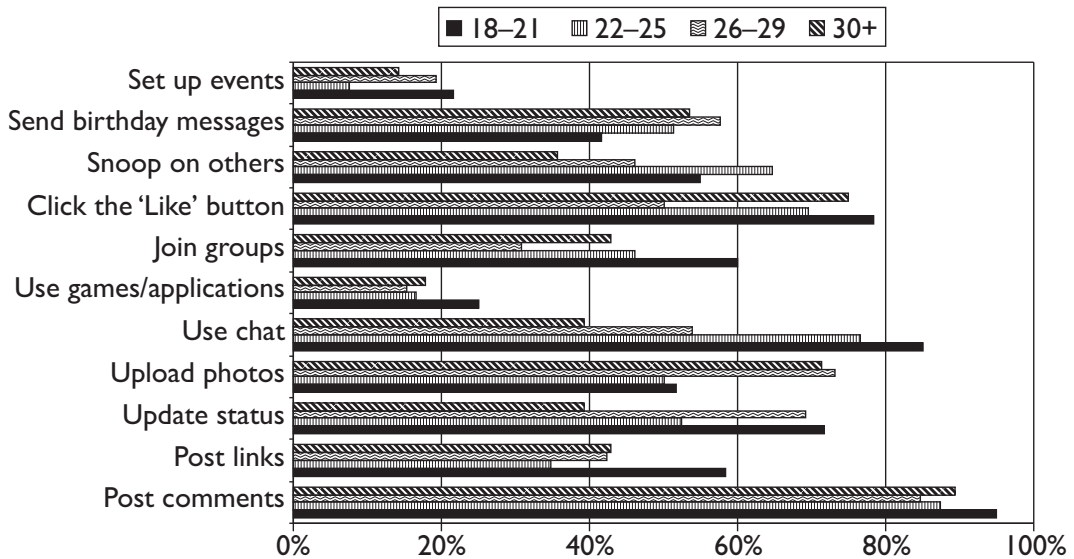


Posting comments (89 per cent) is the most popular Facebook activity. Using chat (72.4 per cent) and clicking the 'Like' button (70.2 per cent) are the next most popular activities. Snooping on others (57 per cent), updating one's status (57 per cent), uploading photos (54.8 per cent) and sending birthday messages (50 per cent) are also popular activities. Figure 2 provides details of the leading Facebook activities across the different age groups examined.

With regard to frequency of log-in, 47.4 per cent of respondents log into Facebook 'many times a day'; 53.3 per cent of these users are in the 18–21 age group. More than two-thirds (69.6 per cent) of Facebook users spend up to 30 minutes on Facebook per log-in. The 18–21 age group represents the group that spends the most time on Facebook per log-in. The majority (59.2 per cent) of respondents update their profile 'less than once a week'. The 18–21 age group report updating their profile more frequently than any other age group.

Almost one-third of respondents (30.9 per cent) have between 200 and 299 Facebook friends, 23.9 per cent have 100–199 friends and 21.7 per cent have 300–399 friends. The 30

Figure 2: Leading Facebook Activities across Age Groups



plus age group members are likely to have the least number of Facebook friends (42.9 per cent of this group have between 1 and 99 friends). The 26–29 age group members are likely to have the highest number of Facebook friends (26.9 per cent of this group have between 300 and 399 Facebook friends). The vast majority of users describe their friends as ‘close friends’ (80.9 per cent), ‘friends that you may not be close to’ (76.8 per cent) and ‘people you know but may not be close to’ (75.4 per cent). Table 4 provides a summary of information disclosure, activity and use on Facebook across all age groups surveyed.

Table 4: Summary of Information Disclosure, Activity, Privacy Settings and Privacy Policy across Age Groups

Age Group	18–21	22–25	26–29	30+
Percentage of respondents	21.8%	56.8%	11.6%	9.8%
Information Disclosure and Activity				
Information disclosure (main details disclosed)	<ul style="list-style-type: none"> • Full name • Date of birth • Hometown • Highest disclosure of information on Facebook 	<ul style="list-style-type: none"> • Full name • Date of birth • Hometown 	<ul style="list-style-type: none"> • Full name • E-mail • Date of birth 	<ul style="list-style-type: none"> • Full name • Date of birth • Relationship status

(Continued)

Table 4: (Continued)

Age Group	18–21	22–25	26–29	30+
Main activities	<ul style="list-style-type: none"> • Post comments • Use chat • Click the 'Like' button • Most active users 	<ul style="list-style-type: none"> • Post comments • Use chat • Click the 'Like' button 	<ul style="list-style-type: none"> • Post comments • Upload photos • Update status 	<ul style="list-style-type: none"> • Post comments • Click the 'Like' button • Upload photos • Least active users
Facebook friends	<ul style="list-style-type: none"> • 200–299 Facebook friends • Broadly defined group of 'friends' • Will befriend people met once and strangers 	<ul style="list-style-type: none"> • 200–299 Facebook friend • Broadly defined group of 'friends' • Will befriend people met once and strangers 	<ul style="list-style-type: none"> • 300–399 Facebook friends • Broadly defined group of 'friends' • Will befriend people met once and strangers 	<ul style="list-style-type: none"> • 1–99 Facebook friends • Broadly defined group of 'friends' • Least likely to befriend people met once and strangers
Privacy Settings				
Changed settings	73.3%	79.7%	92.3%	67.9%
Leading periods for change	Jan–April 2010	Jan–April 2010	May 2010 onwards	Jan–April 2010
Prompted by	Privacy concerns	Privacy concerns	Privacy concerns	Privacy concerns
Settings set to	Friends only (77.3%) – Tightest control	Friends only (80.8%) – Tightest control	Friends only (82.6%) – Tightest control	Friends only (100%) – Tightest control
Confidence in settings	63.6%	62.4%	39.0%	47.4%
Privacy Policy				
Policy read	5.1%	12.7%	28.0%	28.6%
Not read because:				
Too long	42.9%	53.3%	55.6%	50.0%
Not interested	39.3%	34.8%	44.4%	25.0%

Facebook Privacy Settings

Over three-quarters of users (78.3 per cent) have changed their Facebook settings. Over one-third (38.9 per cent) of Facebook users changed their settings when they signed up for Facebook and 37.9 per cent changed their privacy settings in 2010 (Table 5). Comparisons

Table 5: Privacy Settings – Changes and Reasons for Change

Yes to Changing Privacy Settings	Total N=213 %
Facebook settings first changed (N=211):	
When I signed up for Facebook	38.9
2006–2009	14.7
Jan–April 2010	24.2
May 2010 onwards	13.7
Not sure	8.5
Prompted to change by (N=210):*	
Friends/family	27.1
Work colleagues	7.1
An e-mail	3.8
Privacy concerns	74.8
The media	16.2
Groups on Facebook	0.5
Facebook, the company	12.4
Other	6.2
Privacy settings are currently set at (N=211):	
Friends only	82.0
Friends of friends	6.6
Everyone	0.5
Recommended	1.4
Customised	9.5
Confident privacy settings are changed to suit you (N=211):	
Yes	58.8
No	11.4
Not sure	29.9

* Prompted to change: Respondents were given the option to tick from the multiple answers listed to clarify reasons for changing their privacy settings

were made between the length of time respondents have been members of Facebook and when respondents changed their privacy settings. There are two active time periods for changes to privacy settings. The first time period is when users signed up for Facebook. Newer Facebook members (less than a year: joined during second half of 2009 or first half of 2010) report higher responses to making changes to their settings when they first signed up for Facebook compared with those who joined earlier. The second most active time period for changes to privacy settings is during 2010. The leading motivator for adjusting privacy settings is privacy concerns (74.8 per cent). The overwhelming majority of respondents (82 per cent) adjusted their privacy settings to the friends only option. Over half (58.8 per cent) of Facebook users are confident the adjustments they made meet their desired protection; however 29.9 per cent are 'not sure'. One-fifth (21.7 per cent) of Facebook users surveyed have not changed their privacy settings. The main reason for not changing privacy settings is users 'do not see the need' (60.3 per cent), while 34.9 per cent 'do not know how' to change them. Of the 60.3 per cent who do not see the need to change their settings, the majority of respondents (76.5 per cent) are in the 18–21 age group.

Subjects were asked to identify privacy concerns on the social networking site Facebook. 'Information being accessible to third parties' (67.8 per cent), 'information being sold to third parties' (61.3 per cent) and 'risk to employment prospects' (51 per cent) are the most worrying factors for all Facebook users. Facebook users who have changed their privacy settings have more worries regarding the social networking site in comparison to Facebook users who have not changed their settings.

Privacy Policy

Only 14.1 per cent of Facebook users have read the privacy policy. The older age groups (26–29 and 30+) are more likely to have read the privacy policy in comparison to the younger age groups (18–21 and 22–25) (28 per cent and 28.6 per cent versus 5.1 per cent and 12.7 per cent) (see Table 4). Half of the respondents (50.7 per cent) have not read the privacy policy because it is 'too long'; while 35.8 per cent have 'no interest' in reading the policy. Facebook users who have read the policy report more worries on the social networking sites in comparison to those who have not read the policy.

Privacy Statements

Facebook users were presented with a number of statements relating to their awareness of activities concerning privacy (what information is protected, how information is shared and who has access) on the social networking site and also on the influence of privacy on their online behaviour (Table 6). Over half of all Facebook users have a high level of awareness of issues or activities relating to privacy on the social networking site (Table 6).

However, there appears to be a level of uncertainty relating to information being accessible to third parties (34.7 per cent) and also the risk to information from using applications and games on the social networking site (24.7 per cent). In relation to behaviour influenced by privacy, 77.4 per cent of users say they are cautious in what they say and do online. When presented with the statement 'I don't think about privacy issues when online',

Table 6: Privacy Statements and Privacy Settings

N=261	Changed Privacy Settings %	Unchanged Privacy Settings %	Total %
Privacy Awareness Statements			
Your name and profile picture on Facebook are not protected under the privacy settings (TRUE)	Agree 61.2	Agree 42.3	Agree 57.4
Whenever you share information on Facebook you can control exactly who can see it (TRUE)	Agree 53.9	Agree 50.0	Agree 53.1
Information set to 'everyone' on Facebook in the privacy settings is available to everyone on the internet not just Facebook users (TRUE)	Agree 64.1	Agree 54.7	Agree 62.2
Using the games and applications means you are making your information available to someone other than Facebook (TRUE)	Agree 52.9	Agree 37.7	Agree 49.8
Your friends' activities on Facebook can result in your information being made available to other companies and websites (TRUE)	Agree 57.0	Agree 57.4	Agree 57.1
Facebook does not share information with third parties (FALSE)	Disagree 46.1	Disagree 26.4	Disagree 42.1
Privacy Behaviour Statements			
I am cautious in what I say and do on Facebook	Agree 79.0	Agree 73.6	Agree 77.4
I don't think about privacy issues when online	Disagree 52.7	Disagree 25.9	Disagree 47.1

34 per cent agree with the statement while 47.1 per cent of Facebook users disagree (in other words they do think about privacy when online).

The older age groups (26–29 and 30+) are more aware of activities relating to privacy on the social networking site in comparisons to the younger age groups (18–21 and 22–25). The older age groups are also more cautious in what they say and do on the social networking site, in comparison to the younger age groups (84 per cent and 92.3 per cent versus 66.1 per cent and 78.8 per cent). The 18–21 age group are least likely to be concerned with privacy issues when online (28.1 per cent).

Facebook users who have changed their settings are more aware of activities in comparison to those users who have not changed their settings (Table 6). In terms of privacy behaviour, Facebook users who have changed their settings are more cautious in what

they say and do on the social networking site (79 per cent). However, a high proportion (73.6 per cent) of Facebook users who have not changed their settings also report to being cautious in what they say and do on Facebook.

Facebook users who have read the privacy policy appear to be more informed about activities concerning privacy on Facebook. However, almost half of respondents who have not read the policy also reported high levels of awareness. Respondents who have read the policy are likely to be more cautious on Facebook (86.1 per cent), but it is important to note that a high proportion (76.6 per cent) of users who have not read the policy are also likely to demonstrate caution in their behaviour on Facebook. A higher proportion (57.1 per cent) of Facebook users who have read the policy disagree with the statement 'I don't think about privacy issues when online'; compared with 45.5 per cent of respondents who have not read the policy.

Trust Statements

Study participants were presented with a number of statements relating to attitudes towards trust on Facebook and behaviours influenced by trust on Facebook (Table 7).

Table 7: Trust Statements by Privacy Settings

N=261	Changed Privacy Settings %	Unchanged Privacy Settings %	Total %
Attitudes			
I trust Facebook with my information	Agree 23.7	Agree 31.5	Agree 25.3
I trust my Facebook friends with my information	Agree 47.3	Agree 55.6	Agree 49.0
I trust friends of friends with my information	Agree 13.2	Agree 21.2	Agree 14.8
I trust other Facebook users with my information	Agree 3.4	Agree 7.4	Agree 4.2
Behaviour			
Trust issues are likely to cause Facebook users to question what they say and do on Facebook	Agree 73.7	Agree 68.5	Agree 72.6
Trust issues are likely to cause Facebook users to change what they say and do on Facebook	Agree 72.3	Agree 83.3	Agree 74.6
It is my responsibility to protect my information on Facebook	Agree 78.6	Agree 83.3	Agree 79.6
It is Facebook's responsibility to protect my information on Facebook	Agree 77.2	Agree 69.8	Agree 75.7

A quarter of respondents (25.3 per cent) trust Facebook. Almost half of the respondents (49 per cent) trust their Facebook friends. Only 14.8 per cent trust friends of friends. The majority of Facebook users (71.5 per cent) do not trust other Facebook users. It is important to note a proportion of respondents remain neutral on the trust statements (Table 7). In terms of behaviour influenced by trust, 79.6 per cent of survey respondents believe it is their own responsibility to protect their information on Facebook and 75.7 per cent of respondents believe it is Facebook's responsibility to protect users' information.

The youngest age group (18–21) trust Facebook the most (29.8 per cent say they trust Facebook). The oldest age group (30+) trust Facebook the least (55.6 per cent say they do not trust Facebook). The 26–29 age group appear to be the most trusting when it comes to Facebook friends (58.3 per cent) and friends of friends (29.2 per cent) in comparison to the other age groups. The younger age groups (18–21 and 22–29) believe it is more their responsibility to protect their information on Facebook when compared with the older age groups (26–29 and 30+) (82.5 per cent and 80.1 per cent versus 76 per cent and 74.1 per cent), while the older age groups believe it is more Facebook's responsibility (88 per cent and 88.9 per cent versus 63.2 per cent and 76 per cent).

Facebook users who have not changed their settings, in comparison to those who have changed their settings, are more likely to trust Facebook the company (31.5 per cent versus 23.7 per cent), Facebook friends (55.6 per cent versus 47.3 per cent), friends of friends (21.2 per cent versus 13.2 per cent) and other Facebook users (7.4 per cent versus 3.4 per cent) (Table 7). Facebook users who have changed their settings believe Facebook the company has a greater duty to protect users' information when compared to Facebook users who have left their settings unchanged (77.2 per cent versus 69.8 per cent).

Facebook users who have not read the privacy policy are less likely to trust the website compared with Facebook users who have read the policy. Respondents who have not read the policy in comparison to users who have read the privacy policy reported proportionately lower responses when asked if they trust Facebook the company (23.6 per cent versus 36.1 per cent), Facebook friends (45.7 per cent versus 70.6 per cent), friends of friends (13.6 per cent versus 22.9 per cent) and other Facebook users (3.1 per cent versus 11.4 per cent).

Table 8 provides a summary of Facebook users' awareness of privacy issues and attitudes to trust on the social networking site.

DISCUSSION

This study examines Facebook users' perceptions of online privacy by means of information disclosure and activity on the social networking site, awareness of and behaviour influenced by privacy issues, and attitudes to trust.

A high proportion of Facebook users disclose personal information, putting Facebook users at high risk of e-threats such as identity theft, fraud and stalking. Findings from the survey show the youngest age group (18–21) are the most active Facebook members, in terms of information disclosure, Facebook activities and frequency of use. The main privacy concern perceived by Facebook users in this study is information being accessible by and sold to third parties, also identified by Debatin et al. (2009). While concern is

Table 8: Summary of Attitudes and Awareness to Privacy and Trust across Age Groups

Age Groups % of Respondents	18-21 21.8%	22-25 56.8%	26-29 11.6%	30+ 9.8%
Attitudes and Awareness				
<i>Leading concerns</i>	<ul style="list-style-type: none"> • Information accessible to third parties • Risk to employment prospects • Information sold to third parties 	<ul style="list-style-type: none"> • Risk to employment prospects • Information accessible to third parties • Information sold to third parties 	<ul style="list-style-type: none"> • Information accessible to third parties • Information sold to third parties • Viruses 	<ul style="list-style-type: none"> • Information accessible to third parties • Information sold to third parties • Identity theft
<i>Privacy awareness and behaviour</i>	<ul style="list-style-type: none"> • Less informed about activities concerning privacy (what information is protected, how information is shared and accessed) • Relatively cautious in what they say/do online • Least likely to think about privacy issues when on FB 	<ul style="list-style-type: none"> • Less informed about activities concerning privacy • Relatively cautious in what they say/do online • Think about privacy issues when on FB 	<ul style="list-style-type: none"> • Most informed about activities concerning privacy • Most cautious in what they say/do online • Think about privacy issues when on FB 	<ul style="list-style-type: none"> • Most informed about activities concerning privacy • Most cautious in what they say/do online • Think about privacy issues when on FB
<i>Trust and attitudes</i>	<ul style="list-style-type: none"> • Most trusting of FB • Overall low trust levels • High levels believe FB and the user both have responsibility to protect users' information • Believe it is more the user's responsibility 	<ul style="list-style-type: none"> • Overall low trust levels • High levels believe FB and the user both have responsibility to protect users' information • Believe it is more the user's responsibility 	<ul style="list-style-type: none"> • Most trusting of FB friends and friends of friends • Overall low trust levels • High levels believe FB and the user both have responsibility to protect users' information • Believe it is more FB's responsibility 	<ul style="list-style-type: none"> • Least trusting of FB • Overall low trust levels • High levels believe FB and the user both have responsibility to protect users' information • Believe it is more FB's responsibility

Note: FB = Facebook

evident about information being accessible by third parties, only one-quarter of respondents believe third parties have access to their information, suggesting misunderstanding or uncertainty by Facebook users (Acquisti and Gross, 2006).

Privacy

The majority of Facebook users have changed their privacy settings, reflecting an increase in users changing their settings when compared with previous studies (Madden and Smith, 2010; Debatin et al. 2009; Gross and Acquisti, 2005; Govani and Pashley, 2005; Jones and Soltren, 2005). The second half of 2009 and throughout 2010 are the two most active periods for change to one's privacy settings, prompted mainly by privacy concerns. A possible explanation for the surge in Facebook users adjusting their privacy settings during this time is the controversy surrounding Facebook and its privacy settings (Rothery, 2010). Facebook users' information becoming publicly available (in late 2009) by default may explain why many Facebook users adjusted their settings in the early 2010 period. The activity from May 2010 onwards may be a result of Facebook's provision of new simple and easy-to-use privacy settings control.

While most respondents use the 'friends only' privacy option on Facebook, one of the tightest control options on the social networking site, the majority of respondents still have between 200 and 300 Facebook friends, which is above the average Facebook user's 130 friends (Facebook, 2010). Facebook users also have many different classifications of 'friends' on Facebook. These findings suggest Facebook users are concerned with privacy and are using strict settings yet still disclose information to, as Debatin et al. (2009: 102) describe, 'a loosely defined group'. While over half of Facebook users are confident their current settings meet their desired protection, over one-quarter remain unsure, showing a level of misunderstanding or confusion relating to the privacy controls which exist on the social networking site (Acquisti and Gross, 2006). A proportion of Facebook users (over one-fifth) have not changed their privacy settings, because they do not see the need to change their settings; the majority of these users are aged 18–21. This finding concurs with Barnes (2006), who claims younger users are more willing to disclose information on social networking sites and are often oblivious to potential risks.

There is a high level of awareness of activities concerning information privacy (what information is protected, how information is shared and who has access) among Facebook users. The vast majority of respondents (77.4 per cent) believe they are cautious in what they say and do on the social networking site, reflecting high security consciousness. This result contrasts with Rosenblum (2007), who reports that social networking users openly and freely live their lives online. However, the finding is more in line with a recent study conducted by Madden and Smith (2010), showing growing vigilance and consciousness of one's behaviour on social networking websites. The results of this study shows older Facebook users are more likely to be cautious in what they say and do on Facebook in comparison to younger Facebook users. Previous research shows older individuals tend to be less tech savvy, causing them to be more cautious in their online behaviour. Older Facebook users will generally look for more information and reassurance before they engage in

online activity and become more aware in the process (Chaffey et al., 2009). Facebook users who have changed their privacy settings are more aware of activities concerning privacy on Facebook in comparison to those who have not changed their settings. However, both those who have changed and those who have not changed their settings are cautious in what they say and do online. This finding implies an awareness of privacy risks on the social networking site by those who have not changed their privacy settings, but also suggests these Facebook users are not concerned enough to actually change their settings, resembling the privacy paradox (Barnes, 2006).

This study shows the majority of Facebook users have not read the privacy policy, which is consistent with previous studies (Govani and Pashley, 2005; Jones and Soltren, 2005). Facebook users who have not read the privacy policy believe it is too long and uninteresting. Bilton (2010) recognises the length of the privacy policy as a major barrier for Facebook users understanding Facebook's position on privacy. If Facebook creates a more concise and straightforward privacy policy Facebook users might be more willing to read the policy. However, Facebook users may simply have no interest in reading the privacy policy and their attitudes to privacy may not be strong enough to warrant action. Despite a high number of Facebook users voicing concerns and taking action to protect themselves by adjusting their privacy settings, the vast majority of respondents still have not read the policy. Unsurprisingly, Facebook users who have read the privacy policy are more aware of activities relating to privacy than those users who have not read the policy. However, a high proportion of those users who have not read the policy also demonstrate high levels of privacy awareness. This finding suggests Facebook users who have not read the policy are being informed about privacy activities on Facebook from other sources, which may include other Facebook users, the media or privacy advocacy groups, and may imply the controversy surrounding Facebook is being discussed and noticed by users. Overall, the study shows Facebook users perceive it is more important to change privacy settings than to read the privacy policy.

The theory of the privacy paradox in an online environment states that internet users are concerned about privacy yet do little to safeguard it (Barnes, 2006). This study reveals Facebook users are taking protective action to ensure their online privacy and are demonstrating caution in their online behaviour. However, the study also shows Facebook users are willing to part with personal information and interact with a broad definition of online 'friends'. Arguably, Facebook users' desire for social interaction overcomes privacy anxieties. A theoretical implication from this research is that the term 'privacy paradox' may be too strong in the social networking environment and perhaps 'privacy trade-off' would be a more appropriate term. Protective action is being taken in social networking sites but users still willingly trade privacy for the social factor of social networking sites.

The literature highlights that privacy is often considered the number one obstacle to online growth. This argument may hold true within an e-commerce setting; however, within social networking, while privacy concerns exist and are prompting protective action, the rate of adoption to social networking sites continues to accelerate. The level of activity documented in this study on Facebook, despite a high level of privacy concerns and risk

awareness, shows privacy is not a prime obstacle to social networking sites because the majority of users are actively protecting themselves by changing their privacy settings.

Trust

A small proportion of Facebook users (25.3 per cent) trust Facebook. This result is worrying for Facebook the company, as trust is considered vital in getting customers to trade on one's website, to revisit a website and to engage in positive word-of-mouth (Liu et al., 2005). While a certain level of trust is evident between direct friends on the social networking site, the overall level of trust on the website is low. It is important to highlight that an equal number of respondents (25 per cent) also remain neutral on statements relating to attitudes to trust, which might suggest Facebook users have no preference for trust on the social networking site or have never thought of the need to trust. This possible explanation would appear to contradict the substantial body of literature that highlights trust as one of the most important determinants for online activity (Metzger, 2004; Gefen, 2002). Facebook's continued adjustments to its features and in turn privacy settings and policy have caused privacy concerns to increase (Rothery, 2010; Debatin et al., 2009); however Facebook's membership also continues to rise (Fletcher, 2010). The literature suggests privacy violations damage privacy perceptions and in turn lower trust and stall online activity. From this study it would appear the desire for social interaction by social networking users outweighs their concerns for privacy, as noted by Debatin et al. (2009), and might explain why trust is less important in the social networking context. Facebook users are willing to sacrifice control over their personal information (thus sacrificing privacy) in exchange for social interaction, which they class as valuable, rather than searching for trust (Olivero and Lunt, 2004). Another explanation is Facebook users are actively engaged in adjusting their privacy settings and may perceive trust to be less of a concern. Alternatively, Brustein (2010) suggests Facebook is increasingly seen as a 'social utility' and is satisficing customers (Hesseldahl, 2010), which may explain why trust is less important in a social networking context.

This study reveals older Facebook users (30+) are the least trusting group on Facebook, which is in contrast with Madden and Smith (2010) who found the 18–29 age group is the least trusting group on social networking sites. The younger Facebook users (18–25) believe it is more their responsibility to protect their information on Facebook, while older Facebook users (26+) believe the obligation to protect users' information rests more with Facebook the company. This finding is interesting because while the younger age groups believe they have a greater responsibility to protect their information, they are the users who disclose the most information, engage in most Facebook activities, log in more regularly and also refrain from reading the privacy policy. Arguably the younger age groups, while the most active Facebook users, may indeed be the most vulnerable.

The survey results reveal users who have not changed their privacy settings and users who have read the privacy policy have higher trust levels on Facebook, although both of these groups represent the minority of Facebook users surveyed. It seems logical that Facebook users who have read the policy would place more trust in the social networking

site as they are acquiring more information from reading the policy and arguably gaining more control, in turn reducing privacy concerns and raising trust levels as outlined in the literature (Hoadley et al., 2010; Van Dyke et al., 2007; Metzger, 2004; Seigneur and Jensen, 2004; Sheehan and Hoy, 2000). However, it appears illogical that Facebook users who have not changed their settings would trust Facebook more. It was expected that Facebook users who have changed their privacy settings would have higher levels of trust on the social networking site because by adjusting their privacy settings they are assuming greater control over their information. A possible explanation for this contradiction is Facebook users are adjusting their settings in response to the controversy surrounding Facebook's approach to privacy and, while they are assuming control over their information, the factor that prompted them to change their settings could have severely dented or prevented trust developing.

Overall, this study reveals the vast majority of Facebook users believe both Facebook the company and the user have an almost equal obligation to protect users' information on Facebook. This finding shows users expect Facebook to protect their information. However they do not trust them with their information. Trust's traditional orientation as focusing on an 'expectation of goodwill' (Koehn, 2003: 7) is therefore not reflective in a social networking context. Facebook users do not believe Facebook the company has their best interests at heart but believe they have a duty to provide control mechanisms to protect online users to a certain extent. This view is supported by Hoadley et al. (2010) who found that by providing protective controls to Facebook users their privacy concerns relating to new features were largely alleviated. Facebook users equally have a duty to fully utilise these control mechanisms. Perhaps trust is less likely to be a deciding factor within a social networking context, thus supporting Wang and Emurian (2005) who believe trust is context specific, and what may exist instead is the need for a partnership with shared responsibility.

Facebook's introduction of clear and easy-to-use controls to activate and manage privacy settings is a positive development for Facebook and shows the social networking site is fulfilling some obligations to the user. However, the social networking site continues to develop new features and services at an astonishing rate and, based on its history of fast-paced developments coupled with lapses in privacy (Fletcher, 2010), concerns and problems are likely to remain. While retaliation against Facebook's unethical activities concerning privacy have remained largely minimal to date (Debatin et al., 2009) and Brustein (2010) suggests Facebook is increasingly becoming a 'social utility', problems will persist should Facebook fail to demonstrate it is consistently taking sufficient measures and providing adequate and easy-to-use controls to its customers, to ensure their information is protected and not exploited. Unless Facebook acknowledges the concerns expressed by Facebook users and meets their privacy needs consumer upset is likely to continue and may eventually damage Facebook's strong membership base or stall online activity. Facebook users may keep a Facebook profile but inactivity may increase in response to privacy anxieties. A slowdown in online activity on the social networking site will upset the core concept of Facebook: openness and sharing of information.

CONCLUSIONS

This study shows Facebook users are alert and cautious when using the social networking site. However, Facebook users are not completely informed or aware of all activities concerning privacy on the social networking site. In terms of behaviour, protective action (changing privacy settings) is being taken and a greater attentive persona appears to be assumed by most Facebook users. However, while Facebook users believe they are more cautious in what they say and do on the social networking site some activities in terms of information disclosure and number of Facebook 'friends' appear to still be driven by the desire for social acceptance on the social networking site and not by privacy concerns. Thus a 'privacy trade off' in a social networking circumstance is deemed a more appropriate approach to privacy than the term 'privacy paradox' used in the wider online environment. The study also reports low levels of trust exist on Facebook. The search for social acceptance and popularity appears to be a more important driver for online activity rather than trust in the company or trust in other users. The controversy surrounding Facebook and its lapses in privacy could also explain the low levels of trust in the social networking site. However, low trust levels to date have not hindered activity on Facebook and membership continues to rise. Facebook users seem willing to push aside trust issues to achieve social interaction. The importance of trust in a social networking context is clearly questionable and perhaps different determinants for online activity exist in different online environments.

Recommendations for Facebook the Company

Firstly, Facebook need to address its current privacy policy. The overwhelming amount of information presented in the privacy policy needs to be condensed and presented in a more readable and user-friendly document. Although some Facebook users may still refrain from reading the policy, it is important that Facebook clearly communicates its privacy practices in order to appear reliable and honest. The current policy is cluttered, confusing and long. Confusion and misunderstanding reported on the social networking site could be overcome if the privacy policy was more inviting to users. Secondly, Facebook's short history has shown continued development and commercialisation of the website has brought subsequent privacy concerns. Users have been tolerant of lapses in privacy to date and membership continues to grow, however discontent may accelerate further unless Facebook addresses its overall approach to privacy. Facebook has taken an important first step in addressing its questionable stance on privacy by redesigning its privacy settings in May 2010. It is important that Facebook continues to take measures to reassure users it is taking responsibility for its customers' information and to show it is also providing users with the necessary controls to protect their information. New features and services must be adequately accompanied by suitable protective measures. Facebook users must consistently be provided with control mechanisms.

Recommendations for Facebook Users

The study also shows important implications for the average Facebook user. The study highlights the reality that protecting one's privacy is the joint responsibility of both

Facebook the company and the Facebook user. It is all well and good if Facebook provide privacy and control mechanisms to users to protect their online privacy but Facebook users must actively employ these tools in order to alleviate the risk of a violation of privacy on the social networking site. Facebook users must recognise the dangers of actively socialising in the online vacuum and must either take steps to protect their online activity or actively take responsibility for their online actions.

Future Research

It is recommended this research be conducted on a larger scale, incorporating a balanced mix of all age groups. A larger-scale research, availing of random sampling, would enhance the generalisability of the results. This study found trust is considered less important in a social networking context compared with an e-commerce environment. An interesting study to pursue would be to measure the importance of trust in a social networking site relative to e-commerce websites. Another possible research area would be to examine the importance of trust in social networking sites relative to other drivers of social networking activity. The study conducted is relevant and timely given the controversy surrounding Facebook and its privacy stance and the recent changes made to its privacy settings. In order to progress the research further, a longitudinal study monitoring continued changes to Facebook (new features, services and privacy settings/policy) would be interesting to observe going forward. Reactions to these changes by Facebook users should be closely examined to enable a more in-depth look at their perceptions of privacy.

REFERENCES

- Acquisti, A. and Gross, R. (2006) 'Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook', *Lecture Notes in Computer Science*, 4258, pp. 36–48.
- Barnes, S.B. (2006) 'A Privacy Paradox: Social Networking in the United States', *First Monday*, 11(9), available from: <<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312>>, accessed 4 June 2010.
- Bart, Y., Shankar, V., Sultan, F. and Urban, G.L. (2005) 'Are the Drivers and Role of Online Trust the Same for all Websites and Consumers? A Large-Scale Exploratory Empirical Study', *Journal of Marketing*, 69, pp. 133–52.
- Bilton, N. (2010) 'Price of Facebook Privacy? Start Clicking', *New York Times*, 12 May, available from: <<http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html>>, accessed 18 May 2010.
- Boyd, D.M. and Ellison, N.B. (2008) 'Social Network Sites: Definition, History and Scholarship', *Journal of Computer-Mediated Communication*, 13, pp. 210–30.
- Brustein, J. (2010) 'Facebook Is to Power Company as ...', *New York Times*, 24 July, available from: <<http://www.nytimes.com/2010/07/25/weekinreview/25brustein.html?scp=2&sq=facebook&st=cse>>, accessed 26 July 2010.
- Bryman, A. and Bell, E. (2007) *Business Research Methods*, second edition, New York: Oxford University Press.

- Caudill, E.M. and Murphy, P.E. (2000) 'Consumer Online Privacy: Legal and Ethical Issues', *Journal of Public Policy and Marketing*, 19, pp. 7–19.
- Chaffey, D., Ellis-Chadwick, F., Mayer, R. and Johnston, K. (2009) *Internet Marketing: Strategy, Implementation and Practice*, fourth edition, Essex: Pearson Education Limited.
- Debatin, B., Lovejoy, J.P., Horn, A.K. and Hughes, B.N. (2009) 'Facebook and Online Privacy: Attitudes, Behaviours and Unintended Consequences', *Journal of Computer-Mediated Communications*, 15, pp. 83–108.
- Domegan, C. and Fleming, D. (2007) *Marketing Research in Ireland: Theory and Practice*, Dublin: Gill & Macmillan.
- Dwyer, C., Hitzl, S.R. and Passerini, K. (2007) 'Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace', paper presented at proceedings of the 13th Americas Conference of Information Systems, Keystone, Colorado, 9–12 August, available from: <<http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf>>, accessed 3 June 2010.
- Facebook (2010) *Statistics*, available from: <<http://www.facebook.com/press/info.php?statistics>>, accessed 7 June 2010.
- Felt, A. and Evans, D. (2008) 'Privacy Protection for Social Networking Platforms', *Web 2.0 Security and Privacy (W2SP)*, May, available from: <<http://w2spconf.com/2008/papers/s3p1.pdf>>, accessed 7 June 2010.
- Fletcher, D. (2010) 'Facebook without Borders', *Time*, 31 May, pp. 22–8.
- Gefen, D. (2002) 'Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers', *ACM SIGMIS Database*, 33, pp. 38–53.
- Gefen, D., Karahanna, E. and Straub, D.W. (2003) 'Trust and TAM in Online Shopping: An Integrated Model', *MIS Quarterly*, 27, pp. 51–90.
- Ghuari, P. and Grønhaug, K. (2002) *Research Methods in Business Studies: A Practical Guide*, second edition, Harlow: FT Prentice Hall.
- Govani, T. and Pashley, H. (2005) 'Student Awareness of the Privacy Implications when Using Facebook', *Carnegie Mellon*, available from: <<http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>>, accessed 4 June 2010.
- Gross, R. and Acquisti, A. (2005) 'Information Revelation and Privacy in Online Social Networks (the Facebook Case)', *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, Alexandria, Virginia, 7 November, ACM, available from: <<http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>>, accessed 3 June 2010.
- Hann, I., Hui, K., Tom Lee, S. and Png, I. (2007) 'Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach', *Journal of Management Information Systems*, 24, pp. 13–42.
- Hesseldahl, A. (2010) 'Facebook Popularly Unpopular', *Bloomberg Business Week*, 12 August, available from: <http://www.businessweek.com/magazine/content/10_34/b4192086028904.htm>, accessed 18 August 2010.
- Hoadley, M., Xu, H., Lee, J.J. and Rosson, M.B. (2010) 'Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry', *Electronic Commerce Research and Applications*, 9, pp. 50–60.

- Jones, H. and Soltren, J.H. (2005) 'Facebook: Threats to Privacy', *Social Science Research*, December, pp. 1-76, available from: <http://www.mendeley.com/research/facebook-threats-to-privacy/?mrr_wp=0.1#>, accessed 12 June 2010.
- Kirk, J. (2010) 'European Officials Chastise Facebook Privacy Settings', *Computer World*, 13 May, available from: <http://www.computerworld.com/s/article/9176698/European_officials_chastise_Facebook_privacy_settings>, accessed 8 June 2010.
- Koehn, D. (2003) 'The Nature of and Conditions of Online Trust', *Journal of Business Ethics*, 43, pp. 3-19.
- Lee, M.K.O. and Turban, E. (2001) 'A Trust Model for Consumer Internet Shopping', *International Journal of Electronic Commerce*, 6, pp. 75-91.
- Leenes, R., Schallabock, J. and Hansen, M. (2008) *PRIME White Paper*, third and final version, PRIME (Privacy and Identity Management for Europe), available from: <<http://www.mendeley.com/research/prime-white-paper-v2/>>, accessed 21 January 2012.
- Liu, C., Marchewka, J.T., Lu, J. and Yu, C.S. (2005) 'Beyond Concern: A Privacy-Trust-Behavioural Model of Electronic Commerce', *Information and Management*, 42, pp. 289-304.
- Madden, M. and Smith, A. (2010) 'Reputation Management and Social Media: How People Monitor their Identity and Search for Others Online', report of the Pew Research Center, Washington DC: Pew Research Center, available from: <http://www.pewinternet.org/~media/Files/Reports/2010/PIP_Reputation_Management.pdf>, accessed 29 June 2010.
- Mannan, M. and van Oorschot, P.C. (2008) 'Privacy-Enhanced Sharing of Personal Content on the Web', paper presented at the World Wide Web Conference, Beijing, 21-25 April, ACM, available from: <<http://delivery.acm.org/10.1145/1370000/1367564/p487mannan.pdf?key1=1367564&key2=9756747721&coll=GUIDE&dl=GUIDE&CFID=94900663&CFTOKEN=37030123>>, accessed 3 June 2010.
- Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995) 'An Integrative Model of Organizational Trust', *Academy of Management Review*, 20, pp. 709-31.
- Metzger, M.J. (2004) 'Privacy, Trust and Disclosure: Exploring Barriers to Electronic Commerce', *Journal of Computer-Mediated Communications*, 9(4), available from: <<http://jcmc.indiana.edu/vol9/issue4/metzger.html>>, accessed 8 June 2010.
- Mills, J.L. (2008) *Privacy: The Lost Right*, New York: Oxford University Press.
- Nielsen (2009) 'Global Faces and Networked Places: A Nielsen Report on Social Networking's New Global Footprint', *Nielsen*, available from: <http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf>, accessed 2 July 2010.
- Olivero, N. and Lunt, P. (2004) 'Privacy versus Willingness to Disclose in e-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control', *Journal of Economic Psychology*, 25, pp. 242-62.
- O'Neill, N. (2009) 'This Week in Facebook: September 20, 2009', *All Facebook*, 20 September, available from: <<http://www.allfacebook.com/2009/09/this-week-in-facebook-september-20-2009/>>, accessed 16 June 2010.

- Patton, M.A. and Josang, A. (2004) 'Technologies for Trust in Election Commerce', *Electronic Commerce Research*, 4, pp. 9–21.
- Robson, C. (2002) *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*, second edition, Oxford: Blackwell.
- Rosenblum, D. (2007) 'What Anyone can Know: The Privacy Risks of Social Networking Sites', *IEEE Security and Privacy*, 5, pp. 40–9.
- Rothery, G. (2010) 'About Face', *Marketing Age: Business & Leadership*, 4(2), pp. 22–5, available from: <<http://content.yudu.com/A1o0rt/mavol4iss2/resources/index.htm?referrerUrl=>>>, accessed 16 June 2010.
- Rousseau, D.M., Bitkin, S.M., Burt, R.S. and Camerer, C. (1998) 'Not so Different after all: A Cross-Discipline View of Trust', *Academy of Management Review*, 23, pp. 393–404.
- Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research Methods for Business Students*, fifth edition, Harlow: FT Prentice Hall.
- Seigneur, J.M. and Jensen, C.D. (2004) 'Trading Privacy for Trust', *Lecture Notes in Computer Science*, 2995, pp. 39–107.
- Sheehan, K.B. and Hoy, M.G. (2000) 'Dimensions of Privacy Concern among Online Consumers', *Journal of Public Policy and Marketing*, 19, pp. 62–73.
- Sudman, S. and Blair, E. (1998) *Marketing Research: A Problem-Solving Approach*, Singapore: McGraw Hill.
- Survey Monkey (2010) 'What Are Filters?', *SurveyMonkey.com*, available from: <http://help.surveymonkey.com/app/answers/detail/a_id/260>, accessed 2 July 2010.
- Tavani, H.T. (2011) *Ethics and Technology: Controversies, Questions and Strategies for Ethical Computing*, third edition, Hoboken, NJ: Wiley & Sons Inc.
- Van Dyke, T.P., Midha, V. and Nemat, H. (2007) 'The Effects of Consumer Privacy Empowerment on Trust and Privacy Concerns in e-Commerce', *Electronic Markets*, 17, pp. 68–81.
- Wang, Y.D. and Emurian, H.H. (2005) 'An Overview of Online Trust: Concepts, Elements and Implications', *Computers in Human Behaviour*, 21, pp. 105–25.
- Wortham, J. (2010) 'Facebook Tops 500 Million Users', *New York Times*, 21 July, available from: <<http://www.nytimes.com/2010/07/22/technology/22facebook.html>>, accessed 26 July 2010.

Copyright of Irish Journal of Management is the property of Irish Journal of Management and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.