Article

International Federation of
Library Associations and Institutions
2018, Vol. 44(3) 203–222
© The Author(s) 2018
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0340035218785389
journals.sagepub.com/home/ifl
SAGE

Information disclosure, privacy behaviours, and attitudes regarding employer surveillance of social networking sites

Deirdre McGuinness
William Fry Solicitors, Dublin, Ireland

Anoush Simon
Aberystwyth University, UK

Abstract

This paper explores the use of social networking sites amongst the student population of a Welsh university, with particular respect to information-sharing and privacy behaviours, and the potential impact of social networking site checks by employers on future use of these sites. A mixed-methods research design incorporating both quantitative and qualitative approaches was employed to investigate the research question. Results demonstrated that participants were concerned with maintaining privacy online, and were careful with regards to posting and protecting information on social networking sites; however, protective measures were imperfect due to human and system errors. Most respondents were aware of social networking site surveillance, with many noting that this would have an impact on their future use; however, users are active in protecting their privacy through a combination of use of privacy settings and varied levels of information disclosure dependent on context.

Keywords

Information and society/culture, Internet privacy, privacy, social media, social networking sites, surveillance

Submitted: 15 January 2018; Accepted: 9 May 2018.

Introduction

Over the past decade, with developments in social media, the Web has become increasingly social, with users actively creating their own content for dissemination across the internet. Social networking sites (SNSs) are one such means of sharing user-generated content, allowing users to disseminate content far beyond the borders of what was previously possible, and enabling them to 'become the stars of their own productions' (Pempek et al., 2009: 234).

SNSs have come under scrutiny regarding the security of online information. Changes to SNS infrastructure or security features have often been met with negative reactions from users concerned about losing control over personal information, but the behaviour of users has also attracted attention, with media reports indicating that people are disseminating information without thought of the possible consequences (Phipps et al., 2018).

In using SNSs, people are encouraged to share personal information with larger audiences and have grown accustomed to doing so. Research suggests that Internet users are comfortable sharing information within controlled environments, which is what makes SNSs (with password protection and privacy settings) attractive for information disclosure (Bateman et al., 2011). Many SNS users communicate in a manner that demonstrates their belief that these online communities are safe (Clemmitt, 2006). They post information with a specific audience in mind, and, with the

Corresponding author:
Anoush Simon, Information Studies, Aberystwyth University, Aberystwyth, Ceredigion, SY23 3AL, Wales, UK.
Email: ads@aber.ac.uk

availability of privacy settings, are able to define the parameters of their audience. However, online privacy is at risk when users underestimate the visibility of their profiles and fail to enforce adequate privacy measures, thereby leaving information open to unwanted viewers.

Employers take note of the wealth of information available on social media and may use them to gather information about current/prospective employees. Employers have always been able to conduct background checks on applicants but were rarely able to investigate the social aspects of a prospective employee's life. SNSs act as an additional source of personal data, enabling employers to conduct background checks at any stage of the hiring process and make decisions based on this information (Clark and Roberts, 2010).

SNS users are aware of possible privacy issues due to the frequent media reports on the topic. In particular, employer SNS checks are increasingly anticipated by prospective employees (Clark and Roberts, 2010). In recent years, various guidelines have been developed for and by employers (ACAS, n.d.) and upcoming, major changes to data protection (the General Data Protection Regulation (GPDR)) have also prompted further discussion and action (ICO, 2017).

It is possible that employer checks – even while limited and legitimate – could diminish the usefulness of social networking sites as a means of communication, as users fear judgement by current or prospective employers, and so alter their online behaviours (Clark and Roberts, 2010). Awareness of these risks may impact on how users employ SNSs. The practice of employer SNS checks, and its potential impact, was the focus of this study.

The aim of this research was to explore SNS use amongst students within a Welsh (UK) university, with regard to information-sharing and privacy behaviours, and to investigate the potential impact of employer scrutiny on their future SNS use.

The research was conducted in a medium sized university in Wales, United Kingdom. Both undergraduate and postgraduate students were included. The type of SNS studied was limited to a particular subset of social media websites. According to Keenan and Shiri (2009), there are two main types:

- people-focused, where social interaction involves the sharing of personal content centred on the user's profile/homepage (e.g. Facebook, Twitter, etc.);
- activity-focused, in which social interaction is based on site-specific content relating to a particular theme/subject (e.g. YouTube for video content, Flickr for photographs).

For this study, people-focused SNSs were the focus. Users of these sites may participate more actively and share more personal information with their online connection compared to users of activity-focused SNSs. Within this broad category, some sites are not primarily 'social' but more professionally-focused, e.g. LinkedIn. However, this site allows people to create networks (although professional rather than social) and generates a large volume of discussion, personal messaging and other content, therefore it was included in the broad 'people-focused' category. As will be seen later, participants were able to make a clear distinction between the aims of various sites and understood the need to adjust content and interactions accordingly.

The specific focus in this paper is a consideration of the results of the qualitative data (contextualised as appropriate with the findings of the quantitative element of the project), specifically perceptions, attitudes and reported behaviours in relation to privacy online, and particularly reactions to potential employer surveillance in this regard.

Literature

With the development of online communities, 'a more digital approach for maintaining and establishing relationships' (Madhusudhan, 2012: 100) has become the norm. Social media sites are possibly the most popular means of online communication, enabling users to share information to a selected online audience and allowing them to keep up to date with the lives of friends and family. While SNSs represent a popular and vibrant means of social communication, concerns have also been raised. The widespread practise of sharing personal information has stimulated debate about privacy online; when engaging with SNSs, users are encouraged to divulge personal details, and may do so without thought to maintaining privacy.

The debate regarding SNSs and privacy includes the professional environment. Employers are able to search profiles of potential job candidates and recruit those whose profiles demonstrate their suitability for the position (and indeed some sites, such as LinkedIn, exist for this purpose). However, the potential for employers to check non-professional SNS profiles has been the subject of contention, with job applicants arguing that this practise is an invasion of their privacy. SNS checks may have detrimental effects on future SNS usage, both from the perspective of its users and for the SNS itself (Clark and Roberts (2010).

Information disclosure

Sharing information is an important part of using SNSs and is actively encouraged, with sites providing a number of disclosure categories, allowing users to input personal information, as well posting information on their own profiles and their Friends' profiles.

SNS users prefer to provide accurate self-presentations, and 'users often respond honestly and in the majority of disclosure categories' (Strater and Lipford, 2008: 2). Reasons for self-disclosure in online communities include peer pressure, desire to be portrayed in a particular manner, trust in the network and other members, perceived benefits vs. costs of sharing information, SNS interface, and relaxed attitudes to privacy (De Souza and Dick, 2007). Chen and Michaels (2012) note the importance of the online community in information disclosure, stating that users wish to identify within the community and desire feedback affirming their membership from other users. A focus of attention to information sharing on SNSs is the posting of potentially sensitive/ controversial information. Users frequently update their profiles with highly personal information, using profiles 'as billboards about themselves while others use them as personal diary pages' (Clark and Roberts, 2010: 507). Included in this is information that could be construed as inappropriate. Foul language, sexist/ racist comments, evidence of intoxication, sexually explicit material, and professional indiscretions have all been noted on SNS profiles (Go et al., 2012; Morgan et al., 2010).

Sharing information publicly is common practice among SNS users: Pempek et al. (2009) note that students are twice as likely to post information on each others' walls as send messages privately. However, some studies have noted that although some adolescents are posting personal/identifying information, it is not to the extent assumed. Nosko et al. (2010: 408) found that users exercise 'some discretion regarding what kinds of revealing information they are willing to share', or judge their disclosures based on the social norms of their network, suggesting the influential role of the user's audience (Strater and Lipford, 2008).

Social networking and privacy

The control of personal information is paramount, with Clark and Roberts (2010: 511) noting '... a general belief that there is a natural right to have some information about oneself kept from others'. The right to privacy is protected under Article 12 of the Universal Declaration of Human Rights, and many countries recognise the individual's right to privacy; it is restated in the UK Human Rights Act 1998 Article 8. Most recently, changes to Data Protection legislation in 2018 (leading from the rolling out of the GPDR) are likely to have an impact on how personal data is used and re-used, and discussions and guidelines about organisations' use of employee (and indeed prospective employee) data is currently widespread (ACAS, n.d.; ICO, 2017; Robles, 2017; Stacey, 2017).

Legally, there is no clear consensus over online privacy. SNS users have the right to privacy; however, they must be aware that information shared online may go public (Smith and Kidder, 2010). It is argued that information shared online loses its claim to privacy as what is posted online (or indeed in the public sphere, as in Twitter) has a lower 'expectation of privacy' (Barnes et al., 2009: 32), due to the potentially large audience and difficulties in controlling access to information. Posting information on SNSs can be considered self-publication, and 'a person's right to privacy ceases once the individual publishes the information' (Clark and Roberts, 2010: 512); discussions in the literature indicate that the public/private boundaries may be blurring, and this impacts on employment relations (McDonald and Thompson, 2016; Sánchez Abril et al., 2012).

Maintaining privacy

Maintaining privacy on SNSs is important due to the presence of personal/sensitive information, which, if made publicly available, could harm the user. SNS users manage their online privacy by controlling the amount/type of uploaded information, or controlling access to information by using privacy settings. Most, if not all, SNSs provide multiple privacy settings enabling users to limit the information that can be viewed by strangers (i.e. individuals not accepted as Friends/Followers), and some sites (e.g. Google+ and Facebook) have also introduced settings allowing users to control the spread of information amongst accepted Friends. However, privacy maintenance may fail due to individual and system errors (Strater and Lipford, 2008). Particular faults include weak default privacy settings (Byrnside, 2008), the tendency for settings to change without prior notification (Landman et al, 2010), and the difficulty in designing privacy settings to cover all possible outcomes (Chen and Michael, 2012). SNS users frequently make little use of available privacy settings, possibly due to poor interface design, lack of understanding, conforming to social group expectations, and trust in the online community's security (Strater and Lipford, 2008). Users often underestimate their profiles' visibility (Acquisti and Gross, 2006; Byrnside, 2008) and vulnerability to risk (Cho et al., 2010). Although users are generally informed through privacy policies as to the visibility of their information, these are not always read (Arcand et al., 2007).

Employers and SNSs

Employers are gathering an increasing amount of information about job candidates 'to ensure the best fit between an applicant and the employer's organization' (Byrnside, 2008: 448), and now incorporate SNS checks into the decision-making process, viewing them as a convenient means of gathering information about prospective employees. Significant numbers of employers have reported that online information has influenced their decision, in most cases leading to the disqualification of the candidate over the presence of negative content (Clark and Roberts, 2010). Generally, employers will search for applicants using various SNSs and examine what information is made available. If applicants have privacy settings in place, HR managers may encourage them to join the company's SNSs as part of the recruitment process (Madera, 2012), or may add these applicants as Friends (Brandenburg, 2007). SNS profiles are attractive to employers in providing an easy and cost-effective way of gathering information about job applicants, compared to traditional background checks which were usually reserved for serious candidates (Branine, 2008). For employers, gathering information is necessary for making an informed decision regarding the right candidate (Brandenburg, 2007; Clark and Roberts, 2010). SNSs also serve as a useful means of confirming information given to employers by job applicants (Levashina, 2009).

UK recruitment has become increasingly person-orientated (Branine, 2008), and, although academic/professional achievements are still important for hiring decisions, 'non-academic qualities and "fit" are playing an increasingly significant role' (Go et al., 2012: 296). SNSs enable employers to gain a comprehensive view of the applicant, as well as providing insight into his/her standard behaviour. Traditional selection methods are frequently subject to bias; they 'include a certain element of self-presentation, reflecting "maximal" instead of "typical" work performance' (Kluemper and Rosen, 2009: 570). Personal profiles are less likely to highlight information aimed at employers, therefore possibly affording a more accurate insight into the applicant's personality/character. Applicants may argue that their personal/social life is no indication of their professional behaviour, but employers maintain that employees, in having access to sensitive company information, need to demonstrate careful judgement (Brandenburg, 2007). Decision making in sharing personal information may indicate how they might treat company data.

The accuracy of judgements based on SNS information has been questioned (Slovensky and Ross, 2012), and lack of objectivity in SNS checks may also be a problem. Decisions are based on subjective assessments of strangers' profiles in which little context is given, thereby easily leading to misinterpretation of posted content. Judgements made on this basis can be biased, especially without policies to guide this practice (Go et al., 2012; Clark and Roberts, 2010). SNS profile checks have the potential to invade the applicant's privacy, in accessing personal information without the owner's knowledge/consent (Byrnside, 2008), and impacting on 'the right to decide whether, and to whom, to disclose information in an atmosphere free from coercion' (Slovensky and Ross, 2012: 63).

The merits of employer SNS checks are discussed, justifying their use in selecting employees, whilst noting problems faced by profile owners and employers wishing to select the right applicant. Of interest were the potential implications of this practice. Employers must be aware that applicants may react negatively to the incorporation of SNS information into the decision-making process, which may perhaps lead to a negative perception of the organisation. SNSs themselves may also suffer as a result (Madera, 2012). Clark and Roberts (2010) argue that SNSs may be impacted adversely, with users modifying their online behaviour for fear of judgement or punishment by employers.

Themes identified in the literature have interesting implications for both employers and SNSs. In this context, this paper examines how students (a significant SNS user-group) react to the possibility of SNS checks in their future professional endeavours, and considers the possible impact employer surveillance will have on future SNS use.

Methodology

A mixed-methods approach was chosen as the most appropriate method for this study. While qualitative and quantitative research methods each offer numerous benefits, they are not without drawbacks. Both have underlying weaknesses, which may threaten the validity of the research. Quantitative methods are appropriate for describing what has happened, but 'they offer little insight into the social processes which actually account for the changes observed' (Clarke and Dawson, 1999: 55). They inform researchers about patterns of social interaction but fail to provide explanations as to how/why events have happened, and do not aid researchers in generating theory (Amaratunga et al., 2002).

Qualitative methods focus on 'lived experience' and seek to describe 'the meanings people place on the events, processes and structures of their lives' (Amaratunga et al., 2002: 22). They are useful for explorative research and for the development of hypotheses and can expand on quantitative data collected from the same setting (Amaratunga et al., 2002). However, there are important issues to be aware of (Pickard, 2007). Analysis of qualitative data is subjective, so results produced from such studies are dependent on the researcher's interpretation. Results are not readily applied to other similar situations, and there is difficulty in generalising data across the wider population. Questions of reliability and credibility are common with qualitative research.

The mixed-method approach involves utilising both qualitative and quantitative approaches in a single research study (Tashakkori and Creswell, 2007); this allows for methods triangulation, whereby the consistency of research findings can be checked by using different methods of data collection, potentially balancing or compensating for weaknesses in a single method. This may lead to increased validity and reliability of results. The mixed-method approach is also used in cases when a single approach fails to investigate the phenomenon thoroughly; results from one method are supported and enhanced by results of the other – researchers can seek explanations for quantitative results, or generalise qualitative results and test their validity (Fidel, 2008).

To gather both large-scale data and comprehensive insights, and to offset weaknesses in each method, a mixed-methods approach was chosen as the most appropriate method for this study. Participants were recruited online through a snowball sampling method.

The methods used included an online questionnaire consisting of 18 questions (including both open-ended and closed), and semi-structured interviews. Responses to closed questions were coded prior to the launch of the questionnaire and open-ended responses were coded manually. A series of semi-structured interviews (nine in total) were carried out to expand on some of the issues raised earlier in the research process. Interviews were recorded and transcribed for analysis, with codes assigned to the different themes established in each interview.

Participants were drawn from the student population of the university. Both undergraduate and postgraduate students were recruited for the survey to gain a more comprehensive view of online behaviour across the entire student population. For the interviews, the focus was exclusively on postgraduate students, to gain insight on views of privacy and employer surveillance amongst emerging professionals and to discuss changes in social media use and online behaviour throughout their university careers.

The sample gathered for this study compared to the entire student population is inevitably relatively small. As a result, the extent to which the findings of this research can be generalised to the wider population is limited. However, it does provide insights into student perceptions and responses to privacy online, which can contribute to our developing understanding of this area, and which is the focus of this paper.

Results

Questionnaire

The questionnaire response (n=108) consisted of 36 males (33.3%) and 72 females (66.7%). Respondents ranged in age from 18 to 61 years, with a mean age of 24.6 years. There were 64 undergraduates (59.3%) and 44 postgraduates (40.7%).

Most respondents identified themselves as frequent SNS users citing activity across a wide range of sites, including Facebook, Twitter and LinkedIn (Table 1), with 94 respondents (87%) visiting SNSs once a day or more (Table 1). Facebook, Twitter and LinkedIn were the most commonly used social networking sites amongst the participant base, and LinkedIn (being a professional-focused SNS) served as an interesting juxtaposition to the other sites, indicating how users are targeting employers with this information and so may be approaching it differently compared to more social, personal sites.

Participants reported multiple reasons when asked why they used SNSs. Frequently reported reasons were keeping in touch with people; including people met with only occasionally (92.6%), and people seen frequently (70.4%). SNSs were used to keep abreast with Friends' news (81.5%); however, only 38.9% of respondents reported using SNSs to keep their Friends up to date with *their* news. The disparity may indicate a preference amongst respondents to view others' information rather than posting their own.

Lesser reported reasons were meeting new people (12%) and self-promotion (12%). Social use of SNSs was predominant; only 24.1% used SNSs for professional networking. However, 55.6% reported

Table 1. Frequency of SNS use.

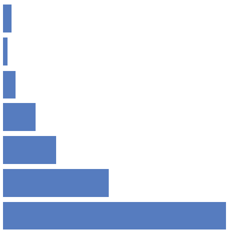
0	Answer		Response	%
1	Less than once a week		2	1.90
2	Once a week		1	0.90
3	A couple of times a week (2–3 days)		3	2.80
4	Most days during the week (4–6 days)		8	7.40
5	Once a day		13	12.00
6	More than once a day		26	24.10
7	Many times throughout the day		55	50.90
Total			108	100%

Table 2. Availability of information posted on SNS profile.

	General public	Friends and their friends only	Friends only	Myself only	Not certain who can view	Unavailable/unsure if available
Screen name/pseudonym/nickname	50	7	14	1	2	23
Full name	54	12	26	5	4	7
Date of birth	20	6	46	25	4	4
Hometown	30	11	39	12	4	8
Current address	7	3	27	33	1	32
Education history	15	15	59	5	6	6
Employment history	7	10	46	15	4	21
Family information	6	6	53	15	5	19
Friends list	28	19	42	9	5	4
Relationship status	14	7	44	18	4	17
Sexual orientation	13	8	31	20	3	27
Political views	7	6	35	15	3	37
Religious views	8	7	36	15	3	34
Email address	4	4	46	26	8	15
Contact number	1	1	24	36	4	36
Personal website	5	0	20	14	7	56
Full address	1	0	8	34	3	55
Interests	11	14	55	2	7	15
Posted photographs	6	16	74	2	5	1
Photographs in which you are tagged	7	25	61	5	5	2
Posted videos	5	11	63	3	5	15
Videos in which you are tagged	5	19	54	5	6	12
Wall posts on own wall	9	11	72	4	7	1
Notes/Blogs	8	8	46	1	4	32
Events you have created	4	12	61	2	6	16
Events you are attending	5	19	58	2	11	7
Communities/Networks/Groups	13	16	52	6	12	5

sharing university coursework information and/or employment-related information.

Information sharing on SNSs. Respondents were asked to identify the information posted on their profiles, and to indicate to whom it was available (Table 2).

Much of the information posted on SNS profiles was available to Friends only, excluding full name and screen name (pseudonym/nickname) with most respondents (50% and 46.3% respectively) making this public. Additionally, respondents' Friends lists were generally shared beyond the respondent.

Although 38% of respondents shared their hometown beyond their Friends, respondents were more cautious when sharing their full addresses, with many (50.9%) believing this information to be unavailable, and 31.5% reporting it as viewable only by the respondent himself/herself. Only one respondent

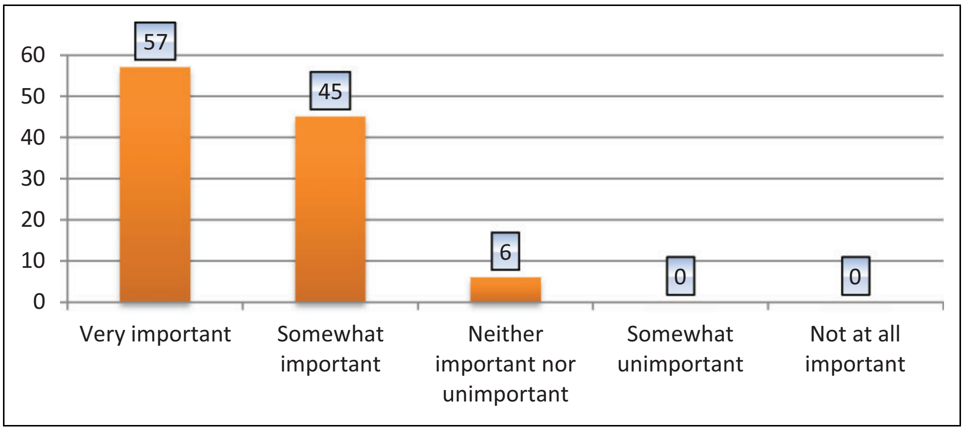


Figure 1. Importance of online privacy.

made their full address available to the public. Contact numbers were mostly omitted from profiles (33.3%) or made viewable to respondent only (33.3%). However, 22.2% made this information available to their friends. Very few (1.9%) made this information available to a wider audience.

Information regarding relationship status, political stance, religious views and sexual orientation were generally shared with Friends only, or were omitted altogether. Less than 20% of respondents reported sharing this information publicly. Information regarding employment history and education history was generally shared with Friends only (42.6% and 54.6% respectively); only a few respondents (6.5% and 13.9%) made this information public. Photographic/video media were generally restricted to Friends; however, media in which respondents were tagged were more often available to Friends of Friends. Created/attended events were also usually restricted to Friends, with low numbers reporting that this information was made available to the public. Respondents generally appeared to be aware of the audience for their online content, with a minority (11.1% and less) reporting uncertainty over who could view each piece of content.

Privacy. Survey respondents were asked about their attitudes to privacy online. The majority of respondents placed some importance in having privacy when using SNSs (Figure 1), reporting it as ‘somewhat important’ (41.6%) and ‘very important’ (52.8%).

An open-ended question asked respondents to note down privacy concerns experienced when using SNSs (Table 3). The 96 responses given were coded for analysis.

Table 3. Reported privacy concerns amongst respondents.

No response	12	11.1
No concerns	6	5.6
Damage to reputation	3	2.8
Lack of trust in SNS	1	0.9
Loss of privacy	7	6.5
Identity theft/Fraud	16	14.8
Cyber-bullying	1	0.9
Employers checking profiles	8	7.4
Monitoring of online activities	2	1.9
Data-mining	8	7.4
Understanding privacy settings and keeping up with policy changes	4	3.7
Strangers/Unwanted parties accessing personal information	20	18.5
Inappropriate/Unauthorised use/dissemination of personal information by other people	17	15.7
Hacking	11	10.2
Stalking	4	3.7

The most frequently reported concern was unwanted people/groups accessing personal information (18.5%) with possible consequences such as identity theft/identity fraud (14.8%), hacking (10.2%), cyber-bullying (0.9%) and stalking (3.7%) noted.

Several respondents were concerned over their information ‘getting into the wrong hands’ and being used without permission (15.7%), and the potential loss of privacy (6.5%) and damage to reputation (2.7%):

> Some information I might be tagged in might not be appropriate for others to see.

A small proportion of respondents (7.4%) reported concern over employers gaining access to online information not intended for their viewing, as ‘some activity that may jeopardise your career’.

Some respondents had problems with SNSs themselves, with one indicating that they did not trust their SNS, and another four reporting difficulty in keeping

Table 4. Reported methods of protecting personal information.

#	Answer	No.	%
1	Using strict privacy settings	74	68.5
2	Blocking content from members of the public (i.e. people you are not friends with)	84	77.8
3	Limiting the amount of information you upload to your profile	79	73.1
4	Only uploading information you deem appropriate for a wide audience	77	71.3
5	Limiting the amount and availability of important personal information (e.g. contact details, descriptive information such as date of birth, address, employment, etc.)	70	64.8
6	Using a pseudonym or nickname instead of your full name to make it more difficult for members of the public to find your profile.	19	17.6
7	Using private messaging to communicate information you do not want to make available to a wider audience	87	80.6
8	Controlling what content you are tagged in (e.g. requiring website to ask for confirmation before you are tagged in a photograph)	45	41.7
9	Keeping your password secret	99	91.7
10	Reading the privacy policy for information on how your information is used	28	25.9
11	Keeping your accounts across different social networking sites separate (i.e. not linked)	55	50.9
12	Only accepting friend/follower requests from people you already know	84	77.8
13	Other (please specify)	3	2.8

up to date with privacy changes. Also noted was the possible monitoring of online activities (1.9%) and data-mining (7.4%):

> Selling personal information to third parties without consent. My life should not be a commodity to be sold without my knowledge or approval.

Respondents selected from multiple choices their preferred methods of protecting their information (Table 4).

Controlling access to information was widely implemented: blocking content from the public (77.8%); granting access only to known Friends (77.8%); and using strict privacy settings (64.8%). The vast majority (91.7%) kept their password secret.

Most respondents also restricted what they shared: 73.1% limited the amount of information uploaded to their profile, with 64.8% limiting identifying information; 41.7% of respondents reported controlling information posted about themselves by their Friends; 71.3% only uploaded information appropriate for wide audiences, while 80.6% used private messaging to share information unsuitable for larger audiences; 50.9% reported keeping their different SNS accounts separate, thereby maintaining separate online identities.

Some privacy measures were less frequently employed. Only 17.6% employed a pseudonym to protect their identity or prevent strangers from finding them, and only 25.9% reported reading the Privacy Policy for information about controlling their content.

Most respondents were confident in protecting their information (Figure 2), reporting that they were ‘very confident’ (18.5%) and ‘somewhat confident’ (50%). Only 10.2% reported self-doubt in protecting their information.

Employer surveillance. Respondents were aware of the potential of SNS surveillance by employers (Figure 3), reporting that it was very likely (27.8%) and somewhat likely (42.6%). Very few respondents considered the likelihood of employer surveillance to be low, with only two respondents (1.9%) replying ‘probably not’.

Responses were mixed regarding the possible effects of SNS checks on future use (Figure 4). While 30.6% of the sample reported that their SNS use

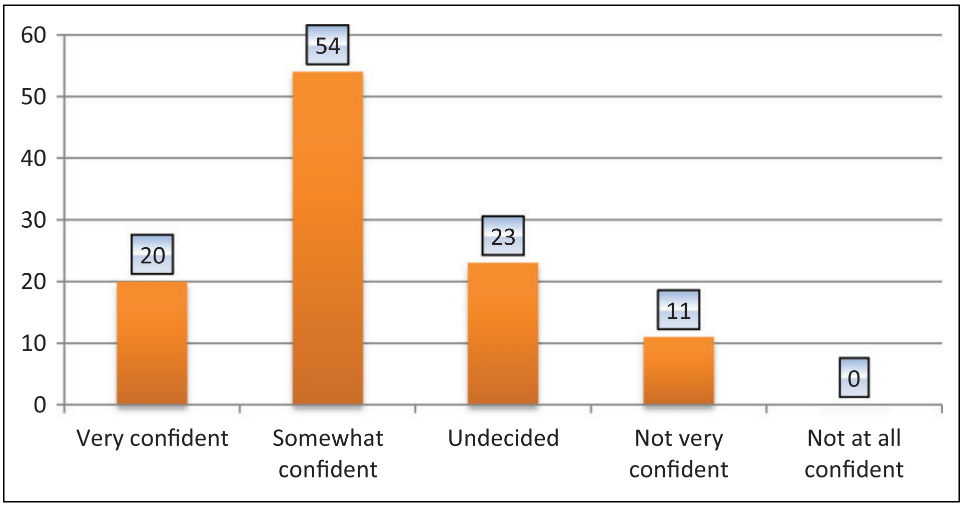


Figure 2. Reported confidence in ability to protect personal information.

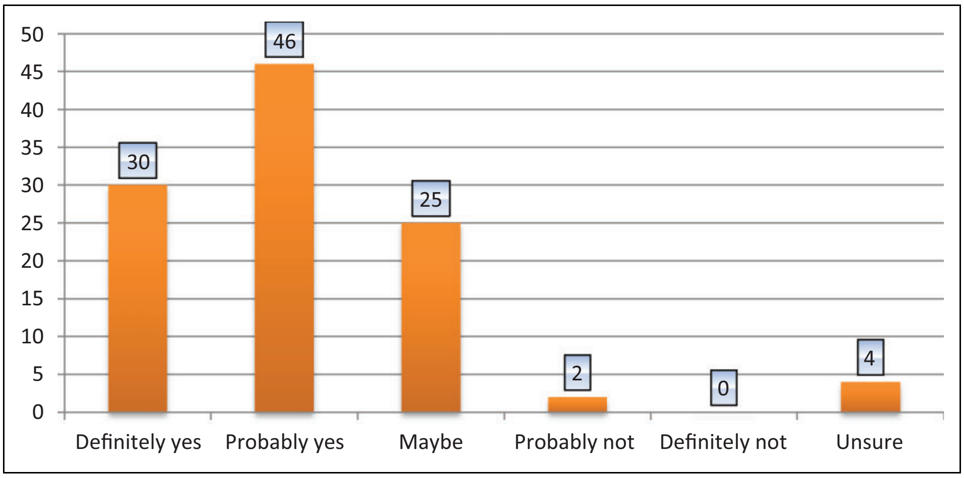


Figure 3. Perceived likelihood of SNS checks.

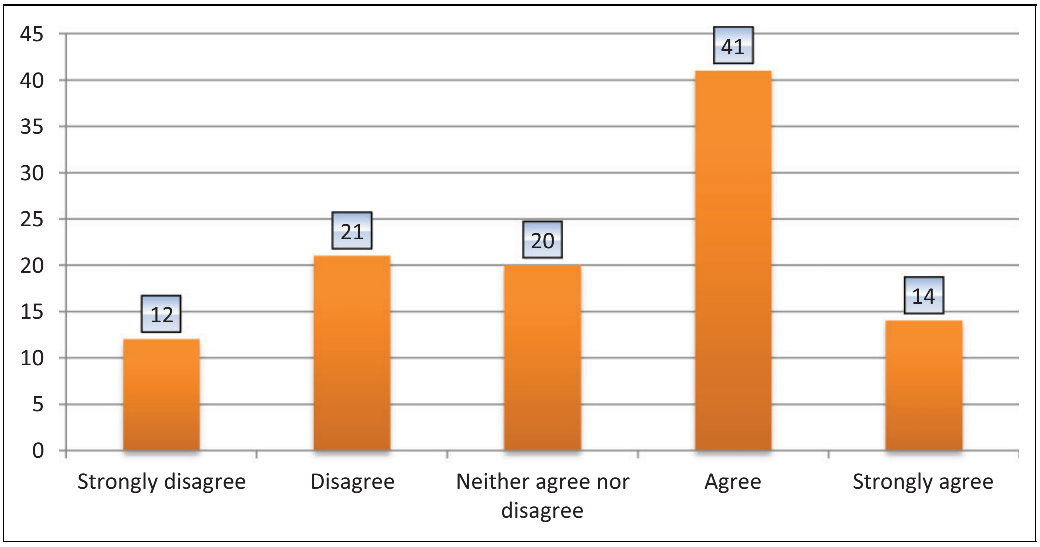


Figure 4. Perceived likelihood of employer surveillance affecting personal use of SNSs.

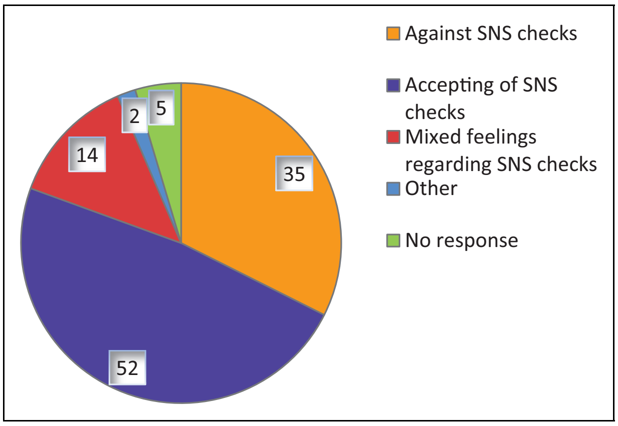


Figure 5. Respondent reactions to SNS checks.

would not change, a greater proportion (50.9%) reported that it would. 18.5% remained unsure.

An open-ended question was used to ascertain attitudes towards employer SNS checks (Figure 5). Out of the 108 respondents, 103 provided an answer, which were coded for analysis. Three groups were established; those against SNS checks (*n*=35, 32.4%), those accepting of the practice (*n*=52, 48.1%), and those with mixed feelings (*n*=14, 13%). Two respondents did not give a direct opinion.

Those against the idea claimed it to be 'invasive and unethical', 'inappropriate', and 'stalker-ish'. Many were concerned with information being misinterpreted, arguing that SNSs were not an accurate representation of their lives. They expressed concern over being judged on this information, particularly if it were to overshadow their educational/professional achievements:

> The true person is usually misconstrued on social networking sites
>
> I hope they'd see any information they found in context, and be tactful about how they used it.

Although satisfied with employers checking professionally-orientated profiles, respondents were unhappy with sharing information regarding their personal lives, questioning its relevance in hiring decisions. They preferred to keep separate their professional and personal lives:

> What I choose to do in my spare time doesn't indicate the type of individual I will be on the job.
>
> Work should be separate from personal life.

Other respondents reported mixed feelings, considering employer surveillance 'annoying but understandable'. Although some disliked their profiles being checked, they could understand the employer's decision to do so:

> I don't think it's right that they should do it, but then again if I was employing someone I'd find social networking sites a good way of gaining an idea of how the potential employee is.

A significant proportion (48.1%) reacted more positively. Several were unconcerned with profile checks due to privacy settings in place, while others ensured that their information was appropriate for employers. Also noted was the possibility of making a favourable impression:

> If people are just a little smart about it, they will use things like Twitter and LinkedIn to enhance their employable image . . . Therefore being checked online by employers can actually be an advantage.

Others argue that employers have the right to look at available online information, arguing that if a user fails to hide information from the public, they cannot expect privacy:

> If I'm stupid enough to place incriminating statuses or photos for all to see then it's my own fault.

Future use. An open-ended question required respondents to discuss their expected future SNS use: 95 responses were returned with mixed reactions (Figure 6).

Most respondents (*n*=47, 43.7%) indicated that their SNS use would remain unchanged, primarily for social interactions. Another 13.9% reported that they would use also SNSs for social purposes in the future; however, they did not indicate whether this differed from current use. A small number (*n*=7, 6.5%) anticipated using SNSs for professional reasons due to their potential for marketing themselves and networking with other professionals. Eight respondents (7.4%) indicated that their use of SNSs would likely decrease in the future, citing 'less time on my hands' and lack of interest. Only one participant (0.9%) claimed a possible increase, stating 'it's going to become even more important'.

Thirteen respondents (12.0%) predicted that they would be more cautious with what they make available online. Even users planning to continue using SNSs as they do now noted the necessity of caution when posting content, particularly to avoid jeopardising their professional endeavours:

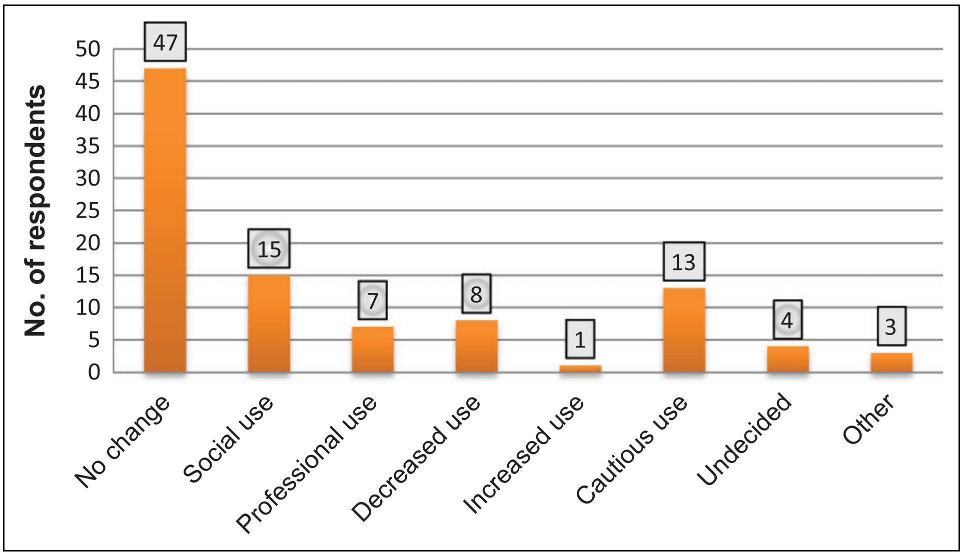


Figure 6. Expected future use of SNSs.

> I definitely feel that I couldn't vent about a bad day at work, even to friends, in case it would get back to my workplace somehow.

Employer surveillance will possibly affect SNS use amongst all respondents. Respondents indicated that they were willing to take measures to ensure that online content did not negatively affect their professional lives:

> Carry on the same, until I get a serious job, and then I'll recreate a new one, with appropriate pictures and stricter privacy settings.

The intention expressed here, to actively make use of the possibility of employer monitoring of SNS profiles to benefit the user, and indeed make them a more attractive potential employee, perhaps underscores a sense of being able to remain in control of personal information posted on SNS through a combination of privacy settings, experience, common sense and regular profile maintenance.

Interviews

Interviews were conducted with nine postgraduate students (7 females, 2 males, aged 22–32); four were UK residents and five international students, and were studying in different departments within the University. Interviewees used Facebook, Twitter, LinkedIn and YouTube, with Facebook being the most popular, and in all but one case, the most frequently used. Interviewees attributed specific purposes for different SNSs. Facebook was predominantly used for social interactions. Desire to stay in touch with people was a common reason for joining Facebook and was reported as its main benefit. Professional/educational use of Facebook was less common, though two interviewees used Facebook to share and gather information relating to their profession. The research did not specifically focus on differences between UK and international students. However, cultural background and context can have an impact – Kim et al. (2011) noted that although broad motivations for SNS use many be consistent, the weight placed on these, e.g. seeking entertainment or using social media for support, varies across countries.

Unlike Facebook, with its predominantly social focus, Twitter was not used for contacting friends. Instead, it was useful as a news feed, and for discussing and keeping informed about professional topics. Its value in allowing interviewees to promote themselves professionally and to network with other professionals was also highlighted:

> It's an easy way to show [employers] you are interested in issues to do with your future career, so it might just put you a little bit ahead.

LinkedIn was also employed by interviewees to facilitate professional networking and to seek information related to their future careers.

Information disclosure on SNSs. Different information was posted on interviewees' separate profiles, generally sharing day-to-day activities and pastimes on Facebook, while restricting LinkedIn and Twitter content to academic/professional achievements and interests. Although interviewees posted a wider variety of information on Facebook, they reported reluctance to share certain information, preferring to keep personal information (e.g. regarding family, relationships, etc.) amongst close friends:

> People who are in my actual circle will know that about me, but stuff I consider too personal to share online, I don't post.

Interviewees were also reluctant to share highly detailed identifying information, and in particular, information about their location or contact details for fear of stalking, identity theft or harassment. Some interviewees reported a preference not to discuss work-related matters on Facebook:

> I've never talked about my employment, or if I've had a bad day at work, I never say any of that.

Interviewees made conscious efforts to restrict information disclosure and reported that they were more cautious in online interactions, citing the potentially large audience and permanency of this content. Several interviewees tried not to post too much information about their lives:

> I don't want everyone to know what I'm doing everyday . . . it can be a bit intrusive in that way.

However, the trend of posting considerable amounts of information was noted, and participants considered that such information disclosure is, in part, influenced by the SNS itself. Users can share information that they would have no opportunity to do in real life, and many may be influenced to disclose information due to the website's culture of sharing:

> Before, it would just ask you a bunch of your general likes, so you would mention sport, films etc. But now they have them separated into different fields so it encourages you to expand on it.

In this context it is possible to think about user-generated but SMS-facilitated content, which may differ considerably between networks depending on aim and scope of SNS. Feedback regarding the extent to which one can learn about people from their profiles was mixed. Much can be learnt in some cases, 'because some people are inclined to post everything on Facebook'. However, people are selective with their disclosures, therefore it is difficult to determine what they are really like:

> I don't think you get to know everything about someone . . . they choose what they put up there . . . You can make yourself sound a certain way.

Posted information is selected to portray the user in a certain manner, something which may be largely influenced by their perceived audience. Awareness of the audience can cause Facebook users to be more selective when posting information:

> People judge you when you post something, so you tend to think first 'should I post this, is this appropriate?'

This links to findings in the survey highlighting an awareness of employer presence on SNS sites but also the possibility that information can be presented selectively to promote oneself to this perceived audience.

Privacy. In general, interviewees were aware of privacy issues, and employed stringent privacy measures to protect themselves on Facebook. However, they were happy for Twitter and LinkedIn profiles to be open to promote themselves professionally:

> I use it for career stuff, so I like people being able to find you randomly and think 'oh, that's the person we should employ'.

Privacy was very important on Facebook, and interviewees revealed that they would change their use of, or delete, their profile altogether if privacy settings were no longer available. This decision was conveyed even amongst interviewees who demonstrated heavy dependence on Facebook:

> It would kill me, but I think I would have to really revisit how I use Facebook . . . I would probably have to take a lot of stuff down.

With Facebook, privacy was protected by limiting information disclosure, and restricting access to information. Interviewees generally only allowed Friends to access their information. Some interviewees were careful in accepting Friend requests, with one deleting and reporting strangers who sent her Friend requests. Another regularly reviewed her Friends' list to ensure that only certain Friends could access her online information:

> I look at the person and ask myself 'do I really care about this person' and if no, I unfriend them.

Some interviewees employed additional measures to protect their information. One interviewee prevented strangers from finding her profile by removing it from Facebook's search results. Another employed a privacy feature separating Friends into groups based on intimacy/familiarity and allowing only close friends to access all information:

> People I don't really know, I've only met them at parties and stuff, I have them as 'acquaintances' so they're on a limited profile.

Although some interviewees believed that properly-used privacy settings should ensure the safety of posted information, others expressed doubt over this, stating:

> I don't think there is anywhere online that you can post information, and it'd be safe.

Even with privacy settings, interviewees highlighted the importance of only sharing information appropriate for wide audiences, as there were no guarantees over who could access profile information:

> If you wouldn't be happy with someone reading your comment in a magazine, don't put it on social networking sites, because it's the same difference at the end of the day. People can get hold of it, and you never know what they may use it for or judge you on.

Many interviewees reported that they were not entirely confident in maintaining privacy, blaming human error and system flaws. Two interviewees were uncertain if they were using appropriate privacy settings, while others reported that Facebook changed too often and did little to inform users as how best to protect themselves:

> It's difficult when the websites change ... it takes you a while to get around the grasp of it again.
>
> It's too complicated and I think that's on purpose ... so people get a bit confused and it's better for Facebook because they can control better what they want to do with the information.

Two interviewees were confident in protecting themselves online. For one, it was due to restricting information disclosure instead of relying on privacy settings. For the other, it was due to experience using these sites:

> I've used these sites from the very early days of them existing, so every time they've changed something, I've changed with it.

However, she had witnessed less experienced users struggling with privacy settings. Experience using SNSs appeared important in awareness/understanding of privacy issues and protection. The least experienced interviewee reported that she had difficulty with this and only through experimenting with the site was she beginning to understand Facebook privacy. Another interviewee reported that she had helped other users in setting up their profiles and explain how they could protect themselves:

> They would always come to me and ask me stuff; they were too scared and worried to put anything on there in case it all got out.

Many interviewees reported seeking information from friends and/or media reports regarding privacy issues. Several interviewees reported that SNSs failed to inform users, and that users themselves had to actively seek information and keep updated:

> You do have to keep aware of what's happening. If they have any changes of rules or if you need to update your privacy settings, you just have to keep on top of things really and just change with it.

Although several interviewees reported that they wished SNSs would better inform users, one interviewee noted that the SNSs' role in this is somewhat limited:

> If Facebook was to release information, would you actually pay attention to it? How many people read the terms and conditions?

Employer surveillance. Most interviewees were aware of employers checking SNS profiles, and some interviewees understood why employers used these sites, noting the opportunity for job applicants to take advantage of this trend:

> You can use things like Twitter to show that you're interested in the area you're trying to get a job in, so you're not just going to be someone who turns up at work, that you might have something extra that you can give to the job.

Interviewees were happy with sites such as LinkedIn and Twitter being checked, and some were unconcerned about Facebook checks as they had privacy setting in place and had ensured their information was appropriate. Others showed more reluctance, questioning the relevance/usefulness of Facebook information and arguing that employers should instead focus on information relating to their academic/career achievements. Interviewees were keen to maintain a separation between their work-life and their personal life, and that certain types of social media sites were appropriate in certain contexts:

> I'm one person outside of work, one person in work, and I will be professional and do my job when I'm there, but my downtime is my own.

This separation extended to their online activities, with interviewees creating separate SNS profiles in order to maintain 'several online identities instead of just the one'. This separation went as far as interviewees wishing to block managers and co-workers from their Facebook profiles, unless they were also friends socially. Interviewees argued that Facebook information provided only a limited view of their personality, and, as a result, may cause employers to make negative judgements regarding applicants who are otherwise suitable candidates:

> Seeing the person's social side doesn't really show what they're qualified for.
>
> You can party a lot, but still be a serious person at work, so it's not showing all of your personality.

However, conversely:

> sometimes your personal life can be an indication of what you'll do in your professional life.

Interviewees were concerned that they would be judged unfairly based on their information (particularly as several believed that employers were looking for negative information with which to disqualify candidates) and, as a result, be passed over for the position. Interviewees questioned the accuracy of judgements based on Facebook information, and were concerned about information being taken out of context. Facebook information demonstrated their social lifestyle to the exclusion of professional interests, and so, failed to inform employers about their educational/ professional achievements and interests:

> You can still have a very good social life and still be very hardworking.
>
> People take pictures only at certain events; I don't think it captures your entire life.

Several interviewees questioned whether employers looking at SNS information would be objective and **recognise** that information posted on socially-focused SNSs like Facebook would not necessarily conform to professional standards, as it is not employed for this purpose:

> You can't just pretend you're an upstanding citizen hiding behind a really smart profile.

This is a particularly pertinent issue for students who often post content about their university experiences- information which may differ significantly from what employers wish to see.

Evolving use of SNSs. Most interviewees wished to continue using SNSs, post-graduation, as they did currently. However, this depended on changes in SNSs and in their lives. Several reported that they might remove content from their current profiles or create new, professional ones. Those who reported that their profile would remain unchanged were already confident that their information was appropriate or were relying on privacy settings for protection.

While interviewees reported that they would continue to use LinkedIn and Twitter for professional reasons in the future, professional use of Facebook seemed unlikely, with interviewees stating they would be uncomfortable connecting with employers on what they deemed a personal site:

> I would never use Facebook for professional reasons ... [It] is more a site for friendship-based interactions.
>
> I don't think it's right to have employers mixed with friends.

Others disagreed, stating that although professional use may become more common, using Facebook socially was likely to continue, just perhaps more privately. One interviewee noted that the development of new features aimed at hiding information from unwanted viewers (e.g. different Friend groups) makes it easier and safer for users to continue sharing information freely. Enabling users to target disclosures towards specific audiences is beneficial as '[it will] give you the freedom to say what you want more' and help enhance communication between users while protecting their privacy.

Discussion

Results from the questionnaire and semi-structured interviews were largely consistent with earlier research, yet additional concepts emerged during analysis, particularly about the separation of personal and professional lives (online and offline), the active role played in restricting information disclosures, and the potential impact of employer surveillance.

SNSs may be 'blurring the boundaries between the personal and professional' (Donelan et al., 2009: 94). However, the data outlined in this paper indicates that SNS users take active measures to separate different aspects of their online lives. They strive to maintain boundaries between their social and professional online interactions (McDonald and Thompson, 2016). Smith and Kidder (2010) note that their online image may not be one which applicants wish to show employers. Participants in this research seem to be aware of this and are taking measures in order to ensure that employers only see their professional personas.

It was clear in the interviewee data that while Facebook was used for interacting with friends, Twitter and LinkedIn were deliberately employed for professional purposes. Professional use of SNSs was not as widely established amongst questionnaire respondents, possibly due to the partiality towards Facebook use (98% of respondents reported use), a site highly focused on social interactions. Many questionnaire respondents were against SNS checks simply because they wanted to maintain a separation between their private and professional lives, both online and offline. Questionnaire respondents reported using SNSs to gather/share information related to professional interests; however, very few engaged in active professional networking. In this regard, interviewees cited the availability of personal information and their discomfort with allowing managers/co-workers with whom they had no social relationship to access such information.

Information disclosure and privacy behaviours

Questionnaire respondents demonstrated caution when sharing personal information, with most posted information restricted to friends, or, as in the case of highly personal/sensitive information, hidden from view or omitted altogether. Overall, respondents treated different information in different ways, suggesting that they are utilising more comprehensive privacy settings allowing them to specify the audience for each piece of information. Respondents were also generally aware of who could access different pieces of information, suggesting that most of these users are, or believe they are, protecting their information. Earlier research noted the tendency for SNS users to allow access to information indiscriminately. This was not the case amongst current participants, with most respondents reporting that they allowed only known individuals to access their information, while some interviewees reported placing additional restrictions on accepted Friends. Students are much more active users of social network sites (across almost the whole range of activities such as posting or commenting) than employed or retired people. They are also more active in their use and checking of privacy settings. Young people overall are more likely to have acted to protect their privacy (Blank, 2014; Dutton et al., 2013).

Online privacy was considered important by participants; interviewees, in particular, reported that privacy maintenance was highly important on SNSs which contained personally-orientated information, therefore privacy settings were a necessity. In contrast to earlier research by (Christofides et al., 2009), interviewees reported restricting their information sharing online. However, they also noted that excessive information disclosure and careless privacy behaviours can be promoted by sites such as Facebook. As outlined below, interviews indicated adaption to these contexts by taking an active role in how and to whom information is made available.

Separate audiences and restricted information

As well as separate uses given to different SNS, interviewees also wished to separate the audience of their different profiles, restricting employers to their more professionally-orientated profiles while keeping their Facebook profiles amongst chosen friends. As a result, they kept Facebook profiles private, while leaving other profiles open to the public in order to extend the reach of professional information. LinkedIn, for example was clearly understood as a tool for professional networking that required a professional presence. Despite the opportunity for linking different SNS platforms, participants maintained a separation between SNS profiles, and, perhaps, as noted by interviewees, a separation between their professional and social identity. What was of most concern was the possibility of access/distribution of personal information by unknown/unauthorised parties, and the potential resulting harm to their safety/well-being. The possibility of employer scrutiny of SNSs was not widely reported amongst questionnaire respondents, with only 7.4% reporting this as a general concern, suggesting that, compared to other possible risks, it is not a high level of concern.

Privacy settings were widely used; however, most respondents restricted information sharing, indicating that they did not rely completely on the websites. They were aware that privacy settings were prone to failure, and instead preferred to rely on their own instincts to prevent leaks of personal/sensitive content. It was noted that privacy settings were often overly complicated and subject to frequent change, so it was difficult for users to completely ensure that posted information was secure.

The information made available by SNSs regarding privacy does not appear to be widely used, with only around one-quarter of questionnaire respondents reporting to read privacy policies. Additionally, only two interviewees reported reading the privacy policy.

This does not lead to a disregard for personal privacy, in fact a general awareness of privacy issues makes users more vigilant. Interviewees also prefer turning to friends for advice or seeking information from unrelated sources such as the media and research articles. Seeking advice from friends was particularly apparent amongst less experienced users, with one interviewee reporting that she was frequently approached by friends who were concerned over who could access their information. Although many interviewees complained about the lack of information provided by SNSs, one noted that the role played by these sites in informing users was small, as users choose to overlook the already available information.

All participants were aware of the possibility of SNS checks conducted by employers, with mixed responses regarding impact on future SNS use. For most respondents, this was reported as likely to have an impact, with some indicating that their future use of SNSs would be more cautious as a result of this. Others reported being prepared to make changes to online activities in the event of SNS checks. Interviewees preferred checks of more professionally-focused profiles but were satisfied with general checks of their Facebook profiles, as they believed that employers would be unable to access potentially damaging content. However, interviewees reacted negatively to more invasive checks of Facebook profiles, reporting that this would likely impact their opinion of the company in question. This may be considered an example of a 'chilling effect' in SNS use with a negative attitude towards the relevant company a manifestation of this effect in the external (offline) environment. The idea of a chilling-effect (that is, behaviour modification) can be evidenced in 'real life' behaviours but also is a focus of investigation in the online world and can lead to a resistance to using everyday technology (Sidhu, 2007), for example after the NSA/PRISM surveillance revelations in 2013 (Penney, 2016). However, this may be to some extent ameliorated by users' understanding of how to control social media to their advantage, e.g. in presenting a positive image of themselves to potential employers, as evidenced earlier, as well as a measured acceptance of the behaviour of organisations and SNS providers. The user has the power to control and indeed utilise these effects and current participants were conscious of this.

Participants also reported that employer checks of online profiles would cause them to be more cautious when using SNSs. Sites such as LinkedIn and Twitter are preferred for professional purposes, but users reported that they were prepared to make changes to their Facebook profiles, e.g. altering their current profiles or creating new ones in order to impress employers. Clark and Roberts (2010) identified this as a key problem with employer surveillance of SNS profiles, significantly effecting future use, and weakening SNSs as a medium of communication. However, this need not be the case – participants in this study noted that social communication would remain prominent on SNSs; it may just alter and evolve. Uses for different SNSs have already become established and are not likely to significantly change in the future, with a large proportion of the questionnaire respondents and interviewees reporting that their use of SNSs, though dependent on changes in SNSs and personal circumstances, would remain similar in the future.

Both user behaviour and SNS interface are likely to evolve in the face of employer surveillance, as it is in the interests of both to adapt to this practice. As noted by one interviewee, Facebook is has introduced new features that would prove beneficial for individuals seeking to continue using SNSs for social interaction while facing the possibility of SNS checks; and in the light of very recent negative publicity has rewritten its terms and conditions to make the language clearer (Kleinman, 2018).

Concerns with employer judgements of SNS information

Although research such as Morgan et al. (2010) and Strater and Lipford (2008) assert that SNS users post truthful information, interviewees noted that posted information, although generally accurate, is one-sided, and therefore, is not an accurate portrayal of the individual. Employers engaging in SNS checks may only be making judgements on an incomplete portrayal.

Employers planning to check SNSs as part of their hiring process should focus on job-related information (Madera, 2012). However, this may prove troublesome due to the unavailability of such information on certain profiles. While Twitter and LinkedIn contained information regarding an interviewee's professional experience and interests, Facebook information was related to social interactions, and did not include much reference to professional endeavours. The literature indicates that employers justify checking personal profiles to confirm information provided in applications, particularly education/employment history. However, as low numbers reported to reveal this information to the public, the usefulness of personal profiles for this purpose is questioned. Employers must take care when scanning SNS profiles for confirmatory information, as this information may not be accessible.

Self-presentation in SNS profiles was commented on by interviewees, who noted that 'you can make yourself sound a certain way'. SNSs users can employ personal profiles as a means of representing their public persona, something which may vary considerably depending on their perceived audience (Acquisti and Gross, 2006). Interviewees reported that they took their audience into consideration to avoid negative judgements, consistent with findings from Valkenburg et al. (2006; cited in Pempek et al., 2009) which noted that SNS users posted information aimed at deriving positive feedback from their audience. The possibility of innocent information being misinterpreted by employers was also noted and was a significant concern amongst both questionnaire respondents and interviewees.

Conclusion and recommendations

In response to earlier research predicting significant changes in SNS use because of privacy concerns, and the increasingly common practice of employer surveillance, this study aimed to investigate the potential impact of SNS checks on use of these sites, and to explore possible SNS use in the future.

Several key areas were examined: use of SNSs; information-sharing behaviours; privacy concerns and behaviours; awareness of, and reactions to employer surveillance; and potential impact of employer surveillance on future SNS use. The issues arising provide an insight into individuals' attitudes towards and perceptions of privacy online, and also indicates that users are thinking critically about social media use, if necessary taking action to protect their privacy either through use of relevant privacy settings or indeed how and to whom they disclose information.

Findings are consistent with earlier research demonstrating the importance of information sharing on these sites. However, SNS users face problems in protecting their information due to fallible privacy settings, human error and a lack of clarity regarding a legal right to privacy on SNSs. Participants were aware of issues, with many reporting that they relied on their own judgement when sharing information, as opposed to depending on the SNS to protect their content.

Participants were in general aware of the possibility of employer monitoring and were not dissatisfied if they were able to maintain some control over access to information. Earlier research, highlighted the potential impact of employer checks, proposing that this practice may damage the utility of SNSs as a medium of communication. However, the data described here indicates that, while SNS checks will likely impact communication, it is not to the extent predicted, as users and SNSs themselves are finding ways to adapt to this practice, and indeed increased awareness and the beginnings of change to legalisation and best practice guidelines will all have an impact on understandings and actions in relation to privacy online.

Although over one hundred students took part in the online questionnaire, this is of course a small proportion of the entire student population, and the use of a snowball sampling method resulted in a non-random sample. As Facebook was used as one means of recruiting participants in this way, a bias toward Facebook users may also be considered a limitation. This limits the generalisability of the results; however, they do give indications of possible trends in behaviour. Based on the literature and the findings of the current study, a series of recommendations were developed for SNS users, employers engaging in SNS checks, and the websites themselves.

1. Recommendations for users: What was most apparent was the need for SNS users to be careful with what they post. Current participants advised caution when making information available online and asserted that it was the responsibility of the user to ensure the safety of their content. Additionally, for users on the brink of entering the job market, it is worth taking into consideration the possibility of creating alternative profiles to showcase professional experience and interests, while maintaining old profiles for socialising.
2. Recommendations for employers: Employers should be aware of the fallibility of online information, and refrain from taking SNS content at face value. Information posted online may be incorrect, outdated, posted without knowledge/consent, or may not refer to the correct individual, leading to inaccuracies and possible misinterpretations of information. Available information may not be relevant for employment decisions, while relevant information may be omitted/hidden from view. Employers must avoid allowing personal biases to sway their judgements. Policies and training should be established to ensure standardisation of this practice, and employers should avoid overly invasive SNS checks. Employers should also consider openness regarding hiring procedures – prior knowledge of SNS checks may increase perceptions of fairness, allowing applicants to ensure

professional information is available on their profiles.

3. Recommendations for SNSs: It is important for SNSs to continue developing website features that will help users control the information they post. The sites should continue to educate users regarding available settings and ensure that policies/guidelines are not overly complicated. Sites could ensure that the default settings are higher to protect inexperienced users who may not be aware of the measures they must take to protect themselves.

A response from one international interviewee indicated possible cultural differences in this practice. While SNS checks may be expected in the US and Great Britain, they may be less common, and possibly less acceptable, in other countries. This could make for interesting comparisons internationally.

It has been noted that that attitudes do not always lead to expected changes in behaviour. Carrying out a longitudinal study will provide more information as to how information-sharing and privacy behaviours are changing over time, and to investigate more thoroughly the impact of employer surveillance. Finally, a more wide-scale analysis into how different SNSs are treated by users could be of interest: while responses from interviewees indicated that online behaviour varied from one site to the next, due to constraints in the scope of the current project it was not possible to investigate this among a larger population.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

ACAS (n.d.) Social media - recruitment and performance management. Available at: http://www.acas.org.uk/index.aspx? articleid=3377 (accessed 31 January 2018).

Acquisti A and Gross R (2006) Imagined communities: Awareness, information sharing and privacy on Facebook. In: Danezis G and Golle P (eds) *Privacy Enhancing Technologies*. Berlin/Heidelberg: Springer-Verlag, pp. 35–58.

Amaratunga D, Baldry D, Sarshar M, et al. (2002) Quantitative and qualitative research in the built environment: Application of 'mixed' research approach. *Work Study* 51(1): 17–31.

Arcand M, Nantel J, Arles-Dufour M, et al. (2007) The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review* 31(5): 661–681.

Barnes N (2009) Reaching the wired generation: How social media is changing college admission. National Association for College Admission Counselling. Available at: http://www.nacacnet.org/publicationsresources/marketplace/discussion/pages/socialmediadiscussionpaper.aspx (accessed 31 January 2018).

Barrick MR, Patton GK and Haugland SN (2000) Accuracy of interviewer judgements of job applicant personality traits. *Personnel Psychology* 53: 925–951.

Bateman PJ, Pike JC and Butler BS (2011) To disclose or not: Publicness in social networking sites. *Information Technology & People* 24(1): 78–100.

Blank G (2014) No, digital natives are not clueless about protecting their privacy online. *The Conversation*, 12 September. Available at: https://theconversation.com/no-digital-natives-are-not-clueless-about-protecting-their-privacy-online-31654 (accessed 30 April 2018).

Brandenburg C (2007) The newest way to screen job applicants: A social networker's nightmare. *Federal Communications Law Journal* 60(2): 597–626.

Branine M (2008) Graduate recruitment and selection in the UK: A study of the recent changes in methods and expectations. *Career Development International* 13(6): 497–513.

Byrnside I (2008) Six clicks of separation: The legal ramifications of employers using social networking sites to research applicants. *Vanderbilt Journal of Entertainment and Technology Law* 10(2): 445–477.

Chen X and Michael K (2012) Privacy issues and solutions in social network sites. *IEEE Technology and Society Magazine* 31(4): 43–53.

Cho H, Lee J and Chung S (2010) Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior* 26(5): 987–995.

Christofides E, Muise A and Desmarais S (2009) Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyber Psychology & Behavior* 12(3): 341–345.

Clark LA and Roberts SJ (2010) Employers' use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics* 95(4): 507–525.

Clemmitt M (2006) Cyber socializing. *CQ Researcher* 16(27): 627–648.

De Souza Z and Dick G (2007) What explains the MySpace phenomenon? Extending the Technology Acceptance Model to explain the use of social networking by schoolchildren. In: *Proceedings of the International Academy for Information Management 22nd international conference on informatics education & research*, Montreal, Canada. Available at: http://www.sig-ed.org/ICIER2007/proceedings/what_explains.pdf.

Donelan H, Herman C, Kear K, et al. (2009) Patterns of online networking for women's career development.

Gender in Management: An International Journal 24(2): 92–111.

Dutton W, Blank G and Groselj D (2013) *Cultures of the Internet: The Internet in Britain. Oxford Internet Survey 2013*. Oxford: Oxford Internet Institute, University of Oxford.

Fidel R (2008) Are we there yet? Mixed methods research in Library and Information Science. *Library & Information Science Research* 30(4): 265–272.

Go PH, Klaassen Z and Chamberlain RS (2012) Attitudes and practices of surgery residency program directors toward the use of social networking profiles to select residency candidates: A nationwide survey analysis. *Journal of Surgical Education* 69(3): 292–300.

ICO (2017) Guide to the General Data Protection Regulation. Available at: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (accessed 31 January 2018).

Keenan A and Shiri A (2009) Sociability and social interaction on social networking websites. *Library Review* 58(6): 438–450.

Kim Y, Sohn D and Choi SM (2011) Cultural difference in motivations for using social network sites: A comparative study of American and Korean college students. *Computers in Human Behavior* 27(1): 365–372.

Kleinman Z (2018) Facebook: Cambridge Analytica warning sent to users. *BBC News*, 9 April. Available at: http://www.bbc.co.uk/news/technology-43698733 (accessed 30 April 2018).

Kluemper D and Rosen P (2009) Future employment selection methods: Evaluating social networking web sites. *Journal of Managerial Psychology* 24(6): 567–580.

Landman MP, Shelton J, Kauffmann RM, et al. (2010) Guidelines for maintaining a professional compass in the era of social networking. *Journal of Surgical Education* 67(6): 381–386.

Levashina J (2009) Expected practices in background checking: Review of the human resource management literature. *Employee Responsibilities and Rights Journal* 21: 231–241.

McDonald P and Thompson P (2016) Social media(tion) and the reshaping of public/private boundaries in employment relations. *International Journal of Management Reviews* 18: 69–84.

Madera J (2012) Using social networking websites as a selection tool: The role of selection process fairness and job pursuit intentions. *International Journal of Hospitality Management* 31(4): 1276–1282.

Madhusudhan M (2012) Use of social networking sites by research scholars of the University of Delhi: A study. *International Information & Library Review* 44(2): 100–113.

Morgan EM, Snelson C and Elson-Bowers P (2010) Image and video disclosure of substance use on social media websites. *Computers in Human Behavior* 26(6): 1405–1411.

Nosko A, Wood E and Molema S (2010) All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior* 26(3): 406–418.

Pempek TA, Yermolayeva YA and Calvert SL (2009) College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology* 30(3): 227–238.

Penney JW (2016) Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal* 31(1): 117–182.

Phipps C, Rawlinson K and Mason R (2018) Toby Young resigns from the Office for Students after backlash. *The Guardian*, 9 January. Available at: https://www.theguardian.com/media/2018/jan/09/toby-young-resigns-office-for-students (accessed 21 June 2018).

Pickard AJ (2007) *Research Methods in Information*. London: Facet.

Robles MM (2017) The debate about using social media to screen job applicants. In: *Proceedings of the Appalachian research in business symposium*, pp. 140–145.

Boone NC, USA. Available at: https://encompass.eku.edu/fs_research/108/ (accessed 31 January 2018).

Sánchez Abril P, Levin A and Del Riego A (2012) Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal* 49(1): 63–124.

Sidhu DS (2007) The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans. *University of Maryland Law Journal of Race, Religion and Class* 2: 375–393.

Slovensky R and Ross WH (2012) Should human resource managers use social media to screen job applicants? Managerial and legal issues in the USA. *Info* 14(1): 55–69.

Smith WP and Kidder DL (2010) You've been tagged (then again, maybe not): Employers and Facebook. *Business Horizons* 53(5): 491–499.

Stacey E (2017) Facebook snooping on candidates? GDPR could put a stop to that. *Personnel Today*. Available at: https://www.personneltoday.com/hr/facebook-snooping-candidates-gdpr-put-stop/ (accessed 31 January 2018).

Strater K and Lipford H (2008) Strategies and struggles with privacy in an online social networking community. *Analysis* 1(10): 111–119.

Tashakkori A and Creswell JW (2007) Exploring the nature of research questions in mixed methods research. *Journal of Mixed Methods Research* 1(3): 207–211.

Valkenburg PM, Peter J and Schouten AP (2006) Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *CyberPsychology & Behavior* 9: 584–590.

Author biographies

Deirdre McGuinness is an Assistant Librarian at William Fry Solicitors in Dublin, Ireland. She graduated from Aberystwyth University in Wales in 2013 with a Master's in Information and Library Studies. She then went on to hold roles in the Oireachtas Library & Research Service (library and research service of the Irish Parliament), the Irish Hospice Foundation and Trinity College Dublin, before joining William Fry as their Library and Information Services Assistant in 2015. She is a member of the British and Irish Association of Law Librarians and won their Dissertation Award for her thesis – *Information disclosure, privacy behaviours, and attitudes regarding employer surveillance of social networking sites*, upon which this paper is based. She is a committee member of the Academic and Special Libraries Section of the Library Association of Ireland.

Anoush Simon is a Senior Lecturer in Information Studies at Aberystwyth University, Wales. Her research and teaching interests include the information society, social impacts of new technologies, digital and social inclusion, public libraries and social justice.