PRIVACY VALUE NETWORKS

Project Reference TP/12/NS/P0502A

Version number: 2.0

11 August 2010

Anne-Marie Oostveen

Oxford Internet Institute

Contents

Figures and Tables index

1. Introduction

This longitudinal case study seeks to examine students' online disclosure and students' online privacy perception. In our research we focused on the use of personal websites, social networking sites, photo or video sharing websites and blogs. While the widespread use of social networks and blogs offer new opportunities for interaction and communication they also raise new privacy concerns. There are many potential negative consequences for individual students of online (self-) disclosure (e.g. legal or institutional disciplinary consequences, rejection from employment or internship opportunities). For instance, one-third of employers now use social networking sites to connect to potential recruits (The Guardian, 2009). Social networking sites create a central repository of personal information. These archives are persistent and cumulative (Barnes, 2006). Research by careerbuilder.co.uk found in a survey of 450 employers that more than four in ten employers discarded a job seekers resume after checking their Facebook page. Career Builder president Yasin said in a newspaper interview that job seekers can have all the skills needed for a job but will fail to secure their dream job because they had been sloppy about what they posted online (Telegraph, 11 jan 2010). Boasting about drinking and drugs, racist remarks, inappropriate photos, all of these things can have a negative impact on job opportunities. As Yasin states: "Job seekers are urged to be mindful of the information they post online. They are indirectly communicating with potential employers".

We will examine the extent of online disclosure among first year and final year students and will investigate whether and how students actively manage their reputation online. We hypothesize that students in their final year at university, who are about to enter the job market, might be more aware of (both the positive and negative) consequences of online disclosure and change their online behaviour accordingly.

2. Methods

The purpose of the student online disclosure case study is to inform the larger PVN project on issues of privacy and online disclosure. Our study aims at casting a light on the extent of online information revelation of college students in relation to their privacy attitudes and privacy behaviour. The first phase of our case-study is based on a survey administered to first year students and final year undergraduate students at the University of Oxford. This same survey will be repeated after 2 years among the first group of students to see if their behaviour/attitudes and opinions have changed over time.

2.1 Recruiting methods

There are over 20,000 students at Oxford, including 11,766 undergraduates. 53 per cent of these undergraduates are studying for degrees in the humanities and social sciences, and 44 per cent in the medical, mathematical, physical and life sciences. The remaining 3 per cent

are studying for undergraduate level diplomas and certificates offered by the Department for Continuing Education. Over a third of the total student body - more than 7,500 students - are citizens of foreign countries, including 15 per cent of undergraduate students[1].

Knowing that there are 11,766 undergraduates studying at the University of Oxford we expected to be able to get 200 first year students and 200 final year students to fill out the first questionnaire. Participants to the survey were recruited via Junior Common Room (JCR) mailing lists and also approached via the Access and Admissions Administrators of the 33 colleges with undergraduate students. However, despite being entered into a prize draw to be in with a chance of winning one of ten £20 Amazon gift vouchers the response rate was lower than anticipated and the survey was completed by 349 students. At the end of the survey we explained that the next part of the study will involve more qualitative research methods and we asked the respondents whether they are willing to participate in further research. 55 students indicated to be interested in being part of the follow-up study by entering their email address. These students will be approached later for our focus groups.

2.2 Survey design

The questionnaire is made up of some questions which have been developed by other researchers (Buchanan et al, 2006) as well as questions unique to this student online disclosure case. The questionnaire was piloted among 10 people and (after making some small adjustments) was put online for a month from 8 November till 4 December 2009. The survey questionnaire contained around 30 questions: an initial screening question; a set of demographic questions, a set of questions about the students' online disclosure; and more in-depth questions about the use of social networks and posting about others. Finally, the survey contained a set of questions about privacy behaviour and privacy concern. We analysed the survey results using SPSS Statistics 17.0 on Windows.

The privacy related questions are based on the work of Buchanan et al. (2006). Buchanan and colleagues developed and validated three scales, measuring privacy-related attitudes (Privacy Concern) and behaviours (General Caution and Technical Protection). After 3 studies to test these privacy measures the authors conclude that their scales are reliable and valid instruments suitable for administration via the internet and they encourage other researchers to use them in online privacy research. Our results will show that the scales also proved to be reliable in our study of online disclosure among students.

[1] See http://www.ox.ac.uk/about_the_university/facts_and_figures/index.html

3. Results

3.1 Participants

In absolute terms we had nearly the same number of male participants (181) as female participants (165). We classified participants depending on whether they were first year undergraduate students or final year undergraduate students. The percentage of first year students (55.3%) taking part in the survey was larger than that of final year students (44.7%). The average age of the students is 21 years (ranging between 18 and 54). The majority of the students are British (83%). In our sample 55 per cent of undergraduates are studying for degrees in the humanities and social sciences, and 45 per cent in the medical, mathematical, physical and life sciences (See Figure 1). This is almost identical to the overall 2009 figures for undergraduates given by the University (respectively 53% and 44%).

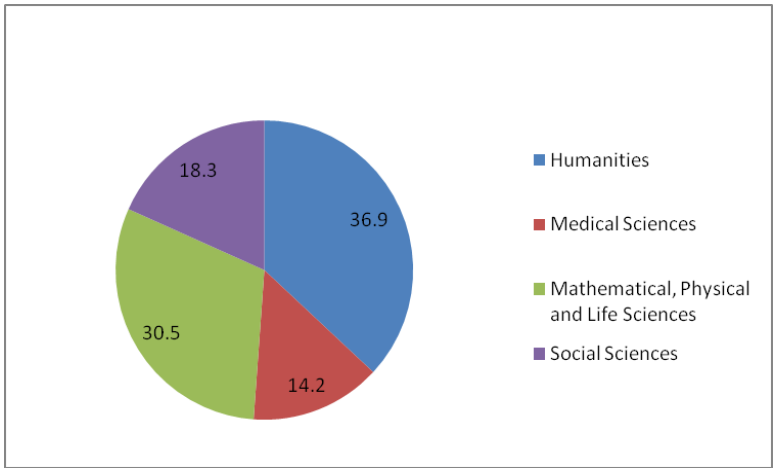

Figure 1: Academic division

3.2 Reported online disclosure

3.2.1 Where do students post personal information online?

We first tried to establish where students post information online. When we look at table 1 we see that Social Network Sites (SNS) are the most important venue to post personal information on the internet with well over 90% of both the first and final year students reporting to do this. In comparison, the OxIS survey found that nearly half (49%) of *all* British internet users updated or created a social network profile in 2009. According to Dutton, Helsper and Gerber (2009) this is a remarkable rise in social networking, up from 17% in 2007. Boyd and Ellison (2007) define social network sites as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by

others within the system". One of the most popular Social Network Sites is Facebook. Facebook has more than 400 million active users, with the average user creating 70 pieces of content each month. More than 25 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared each month[2].

Disclosure on other sites scores a lot lower with personal websites closing the ranks. While according to the 2009 OxIS study 22% of all British internet users write a (web) log our students are clearly less active bloggers (9%). An explanation for this could be that social network sites have taken over a lot of the functions that used to be provided by personal websites and blogs, becoming all-in-one platforms (Boyd and Ellison, 2007). This is also indicated by the fact that a relatively high percentage of both first year and final year students have used weblogs and personal websites in the past but have stopped providing personal information on these sites.

	Yes (users)		No (non-users)		Have done, but not anymore (ex-users)		No, but would like to	
	First year	Final year	First year	Final year	First year	Final year	First year	Final year
Social network site	92.5	92.5	5.2	1.5	2.3	6	0	0
Video sharing site	12.7	8.1	73.2	87	10.8	4.1	3.2	0.8
Micro-blogging site	12.3	9.9	81.5	84.3	4.1	3.3	2.1	2.5
Photo sharing site	9.3	11.6	80.1	83.5	8.6	3.3	2	1.7
Weblog	10.6	7.6	74.2	73.1	11.9	15.1	3.3	4.2
Personal website	5.6	2.6	79.9	83.3	13.2	12.3	1.4	1.8

Table 1: Where do first year and final year students post information? (First year N=144, Final year N=114)

Differences between first year students and final year students are only significant for the use of social network sites (0.064) and video sharing sites (0.032). Overall, first year students use more different outlets to disclose information than final year students. They only score lower on the use of photo sharing sites (e.g. Flickr, Photoblog), but indicate with a higher percentage that they have used them in the past. Again, photo sharing features have recently been incorporated in social network sites, making it very easy to upload and share photos. According to Besmer and Lipford (2008) social network site Facebook is the largest photo sharing site on the Internet with 14 million photos uploaded daily.

When we combine the users and ex-users, we see that most respondents use their real name when they disclose personal information on a SNS, although around 10% of first year students prefer to use a nickname, more often than final year students. The difference between the two groups on the use of nicknames versus real names on social network sites is the only statistically significant difference (0.035). Both first year and final year students are most likely to use a nickname on video sharing sites, while final year students also show a high proportion of using a nickname on weblogs and micro-blogging sites (Table 2). Although the differences

[2] http://www.facebook.com/press/info.php?statistics, accessed 12 June 2010.

between the two groups are large, they are not significant because of the small number of respondents.

	First year	N	Final year	N	Significance
Social network site	10.3	165	3.8	131	0.035
Video sharing site	59.5	37	73.3	15	0.749
Micro-blogging site	33.3	24	62.5	16	0.118
Photo sharing site	48.1	27	55.6	18	0.951
Weblog	41.2	34	66.7	27	0.129
Personal website	40.7	27	29.4	17	0.268

Table 2: Nickname usage on different sites for the combined users and ex-users (%)

3.2.2 What kind of personal information do students post online?

After establishing where students post information online, the next question is obviously what kind of information they disclose. Figure 2 shows for both the first year students and the final year students the type of personal information they post. The data can be split in two categories. First of all, there is the unique identifiable information. In social psychology personally identifiable information (PII) is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. Although the concept of PII is ancient, it has become much more important as information technology and the Internet have made it easier to collect PII, leading to a profitable market in collecting and reselling PII. Items which might be considered PII include, but are not limited to, a person's: full name (if not common), national identification number, telephone number, street address, email address, etc. Secondly, there is the information which is still quite personal but doesn't give uniquely identifying clues because many people such as gender, race, age, religious views, political views, relationship status, etc. Note that information can still be *private*, in the sense that a person may not wish for it to become publicly known, without being personally identifiable. Moreover, sometimes multiple pieces of information, none of which are PII, may uniquely identify a person when brought together. In our research, students are as forthcoming with providing personally identifiable information as they are with non-personally identifiable data (see Figure 2).

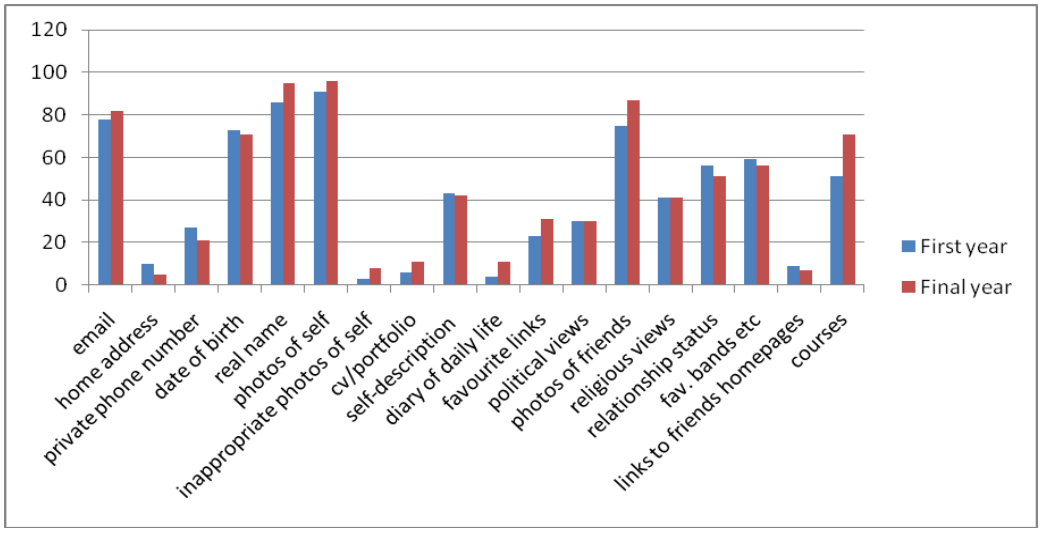

Figure 2: What kind of personal information do you post online? (first year N=177, final year N=133)

A recent study by Krishnamurthy and Wills (2010) shows that it is possible for third-parties to link personally identifiable information, which is leaked via social network sites, with user actions both within these social network sites and elsewhere on non-SNS sites. Third party servers are increasingly used to provide content and advertisements for web pages belonging to first-party servers. The authors refer to the ability to link personally identifiable information and combine it with other information as "leakage". Such leakage would imply that third parties would not just know the viewing habits of *some* user, but would be able to associate these viewing habits with a specific person. They point out the two immediate consequences of such leakage: "First, since tracking cookies have been gathered for several years from *non-OSN* sites[3] as well, it is now possible for third-party aggregators to associate identity with those *past* accesses. Second, since users on OSNs will continue to visit OSN *and* non-OSN sites, such actions in the *future* are also liable to be linked with their OSN identity" (Krishnamurthy & Wills, 2010: 112).

Overall, most of the students do not post personal information very frequently. 53% of both the first and final year students post once a month or less, about 12% post once a week, while about 15% post several times a week and about 6% post once or more often a day. There is no significant difference in the posting frequency of the 2 groups. However, when the students were asked how often they update their social network profiles, they showed a higher activity (see Figure 3). Apparently updating a SNS profile is not considered to fall under 'posting personal information online'.

[3] OSN stands for Online Social Network

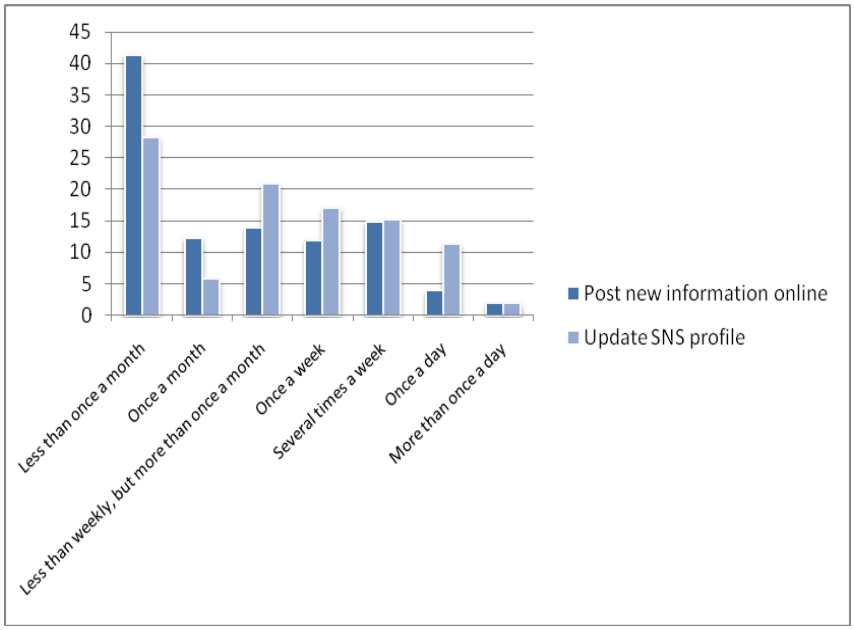

Figure 3: How often do you post personal information online / update your SNS profile?

3.2.3 Why do students post personal information online?

What are the motivations for students to post information about themselves online? Our survey shows that the main reason for online disclosure is to 1) keep (distant) family and friends informed, 2) self-expression, 3) re-acquiring lost contacts, 4) boredom and 5) because everybody else does it. Being creative, sharing ideas, beliefs and philosophies are moderately important, while getting new friends, self-promotion and search for recognition are not considered to be important motivations. Again there is very little difference when we compare the two groups. Not even with the motivations which, based on our hypothesis, would be expected to be more prevalent for first year students such as 'getting new friends', or more prevalent for final year students such as 'self-promotion'. The low importance of 'getting new friends' was also noted by Boyd and Ellison (2007): "On many of the large SNSs, participants are not necessarily "networking" or looking to meet new people; instead, they are primarily communicating with people who are already a part of their extended social network".

From the motivations of the students it makes sense to deduct that the key audiences they target are friends, family and fellow students and not so much future employers, tutors or total strangers. The result from the question 'Who are the key target audiences you have in mind when you post personal information online?' does indeed confirm this. Given the fact that the final year students will be entering the job market soon, one could expect them to include future employers more often as a key target audience. However, the data does not show this.

3.3 Posting about others

Students do not only disclose information about themselves online. While 46% of the students say that they never post *information or opinions* about friends, family, fellow students or lecturers, 45% of the respondents say they post such information sometimes and 3% does it often. However, it is far more common to post *photographs or videos* featuring other people**.** Here we find that 33% does this often, 43% sometimes and 20% never. These photos and videos are commonly tagged with the full names of the people featuring in them (see Figure 5).

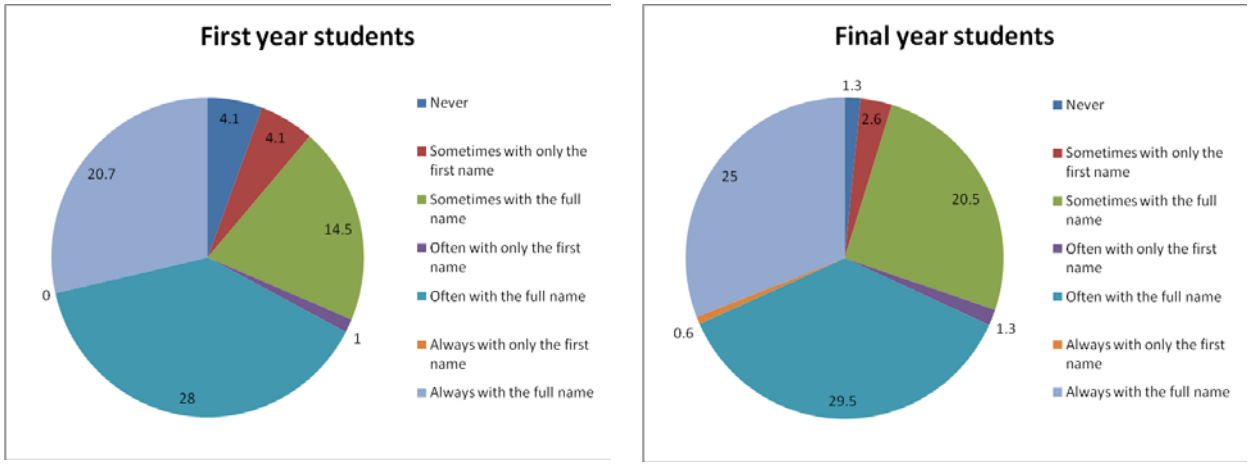

Figure 5: Do you tag your photos or videos with the real names of people? (first year N=193, final year N=156)

The next question we asked was whether before posting a photo or video online featuring other people, the students asked permission from these people to publish it. As we can see from the Figure 6, most students publish material about others without asking their consent. About 10% of the first year students always ask permission, compared to 7% of the final year students.

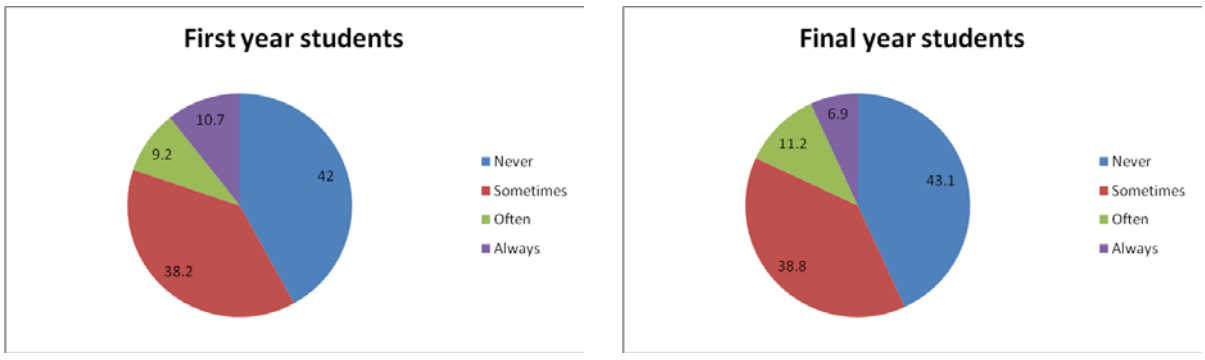

Figure 6: Asked permission on forehand (first year N=131, final year N=116)

Although slightly over 40% of the students never ask permission before posting material about others online, about 77% of the students have never been asked to remove information,

photos, videos or text from the internet by friends, family or others. From the 23% of respondents that have been asked to remove information the majority always obliges (Figure 7).

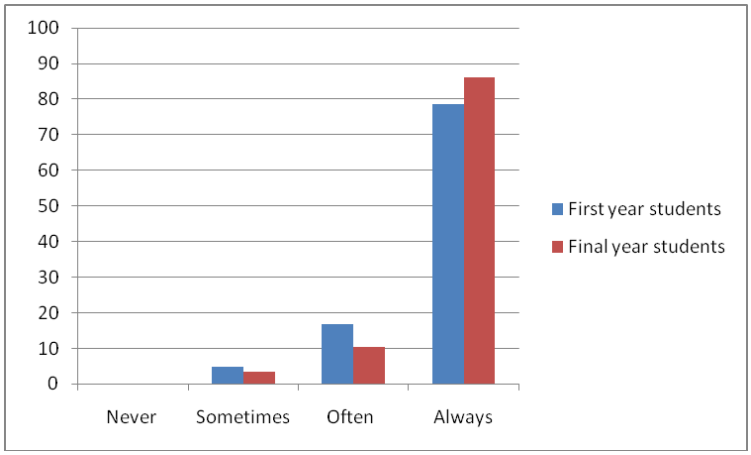

Figure 7: Do you oblige when you are asked to remove information? (first year N=42, final year N=29)

When the students were asked whether they themselves had ever asked a friend or relative to remove something that had been posted about them online we see a different picture emerge. While they indicate that they hardly ever get asked to remove information from the internet by friends or family, the results show that just over 40% of the respondents themselves have indeed requested 'once' or 'more than once' to have information about them removed (Figure 8). Anova shows that there is no significant difference between the two groups (0.390).

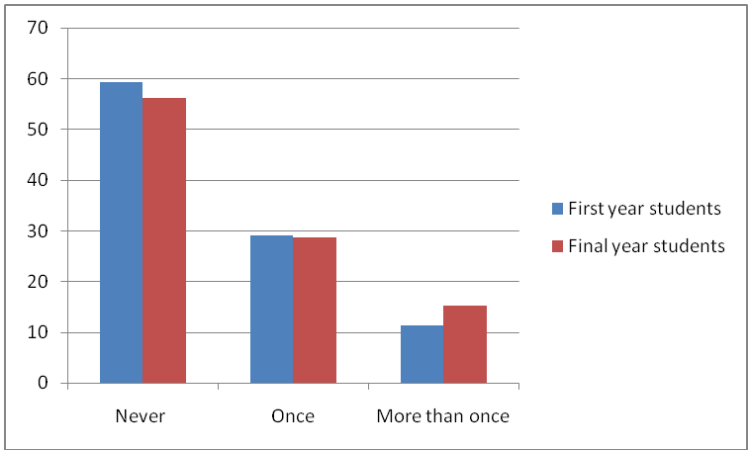

Figure 8: Have you asked others to remove information about you? (first year N=175, final year N=132)

Most students do not have their social network profiles set to be fully accessible to the public. This suggests that students are aware of potential privacy threats online and that many are proactive about taking steps to minimize potential risks. However, not having your profile visible to all internet users does not mean that all of the information posted on the social network is invisible unless one is part of the friend's network. With Facebook for example,

certain information is visible to everyone because it is essential to help people find and connect with people on Facebook. Name and profile picture are visible to everyone so that: 'real world friends can recognize you, and so we can display them when you write on someone's Wall'[4]. Gender is also public and networks are visible to everyone so people can see who else is part of someone's network (and will have access to their information if they accept a friend request). Other information such as hometown and interests, are visible by default to help friends and other people who have things in common to connect with each other, but can be changed by setting different privacy settings. Although most students have a certain amount of personal information floating about freely on the internet - partly posted by themselves on blogs, social networks and video or photo sharing sites, and partly posted by others and tagged with their real names – only a small percentage of our respondents had personal information misused by another person (as far as they are aware).

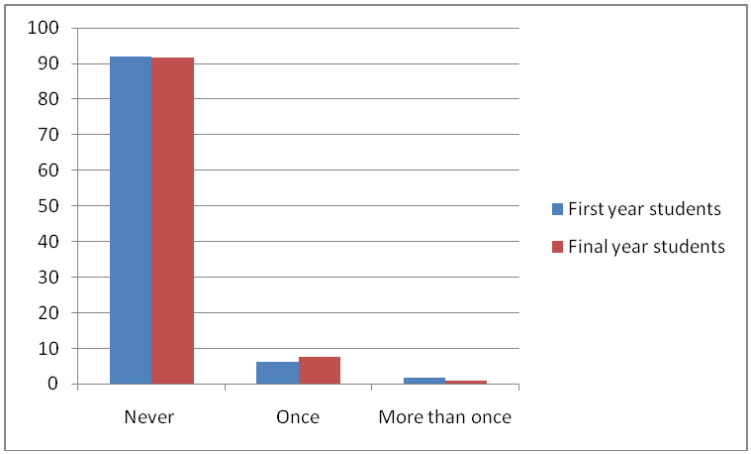

Figure 9: Have you had personal information you disclosed on the internet misused by another person? (first year N=175, final year N=132)

[4] http://www.facebook.com/privacy/explanation.php

3.4 Online reputation management

In our study both first and final year students agree that the internet increases their ability to obtain jobs (Figure 10). Whether this is because they are more visible for potential employers, or because it is now easier than ever to find and use job sites, online career tutorials and other job-hunting tools is not clear from our survey and we will have to examine this further in our follow-up focus groups. However, we have already seen in section 3.2.3 that 'self-promotion' is not an important motivation for the students to post information online and that future employers are not really seen as their key target audience. Again, there is no significant difference between the two groups of students (0.287).

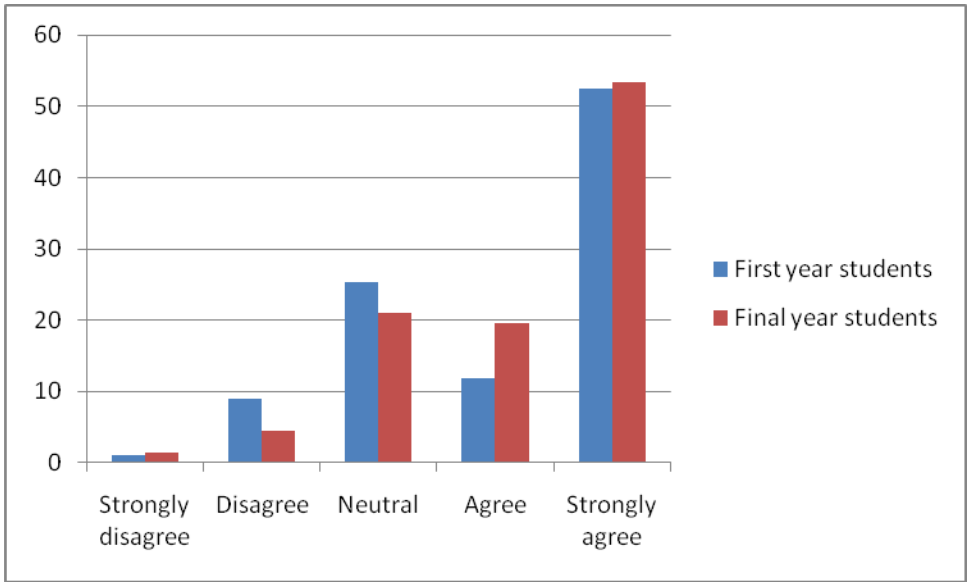

Figure 10: The internet increases my ability to obtain jobs (first year N=177, final year N=133)

A study commissioned by Microsoft found that 75% of US companies have formal policies in place that require hiring personnel to research job applicants online. In the UK slightly fewer than half of the companies surveyed had implemented similar policies (Microsoft, 2010). More shockingly, 70% of US employers and 41% of UK employers have rejected potential employees because of information found out about them online. The students in our survey seem to be aware that employers are using the internet to gather information about job applicants. Of the first year students 75% 'agree' or 'strongly agree' that employers will increasingly use online sources to check up on potential and current employees, of the final year students this is 88% and the difference between the two groups is significant at 0.049 (see Figure 11). When asked who they think is currently viewing their main social network profile, (future) employers score very low, but the results show that students do expect employers to be checking out their online profiles in the future.

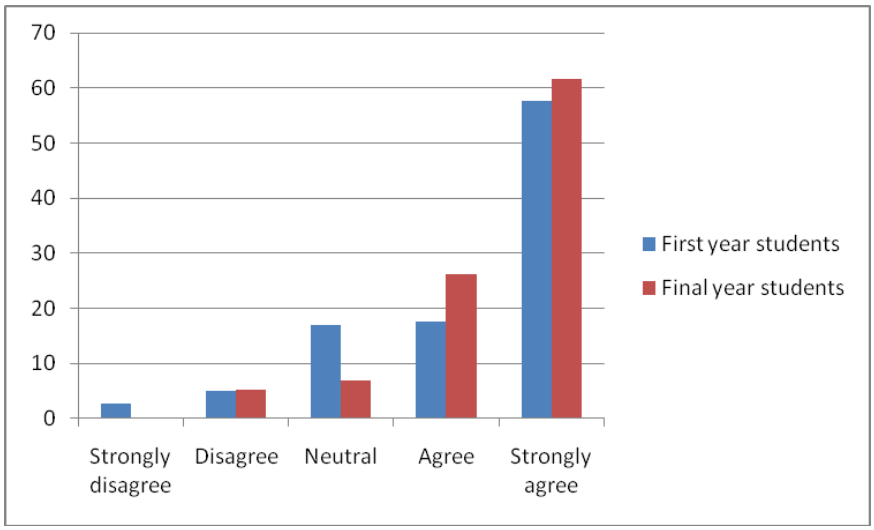

Figure 11: Employers will increasingly use Facebook (and other online sources) to check up on potential and current employers (first year N=177, final year N=133)

Recruiters, headhunters and HR managers encourage jobseekers to actively manage their online presence so that it will show them in a positive light for future employers. Cleaning up SNS profiles, limiting the amount of photos posted and deleting inappropriate photos, displaying achievements and detailing skills and qualitfications, all should contribute to better chances on a tough jobs market. According to a survey of 208 firms by recruitment consultant Harvey Nash and the Department for Work and Pensions, half of employers believe that if candidates invest time in developing a strong *online brand* using social and other networks, they are more likely to be hired (The Guardian, 2009). Because employers are increasingly searching the internet and are tracking social media content to find addditional information about candidates, one would expect prospective jobseekers to actively manage their online reputation. However, do we see this awareness of the importance of online reputation management among the final year students in our study?

A first step in online reputation management would be to explore what can be found about oneself online. Tarnowski (2009) suggests the following: "It is important that you look at your existing online brand and check for areas of concern. Start by Googling yourself and see what comes up. Try to remove content you feel could be a problem". However, an unexpected find from our survey is that a lot of students have never 'Googled' themselves and have therefore no idea of the kind of information that is out on the internet about them. When asked about their 'self-googling' the answers of the two student groups show a significant difference (0.031). First year students are less likely to 'Google' themselves (23%) than the final year students (15%). One would expect all final year students, who will be looking for jobs in the near future, to make sure that the information that can be found about them is accurate and not harmful. As already stated, more and more employers use the internet - and social networking sites in particular - as tools to double check on potential new workers and what they find online can affect their hiring decisions. It is therefore not just important for

prospective jobseekers to self-censor and clean up their own previously posted content, but also to make sure that others have not posted any 'digital dirt' about them. Luckily, 'only' 11 percent of the self-searching final year students discovered information that they would rather not see online. As we already saw from Figure 8 students do ask other people to remove information about them, also here we see that final year students do this slightly more frequently than first year students.

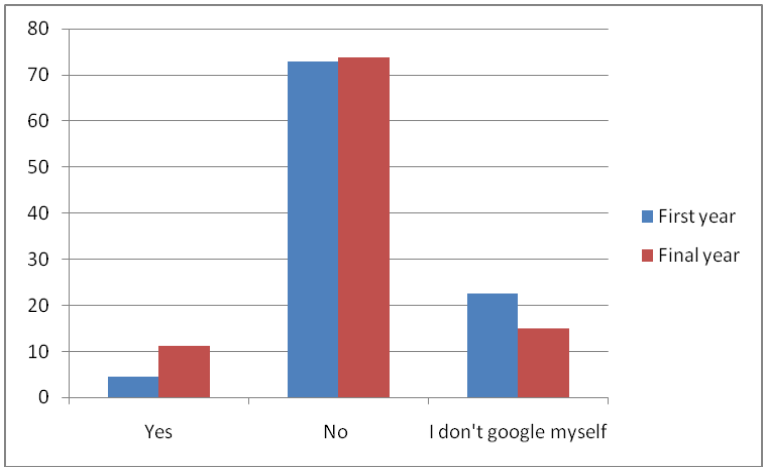

Figure 12: When you 'google' your own name, do you find information about yourself that you would rather not see online? (first year N=177, final year N=133)

Besides cleaning up possible harmful content, students can also create deliberate positive content. According to the recruiters this content should highlight specific accomplishments but without boosting up qualifications. Employers reported that one of the biggest mistakes that job seekers made was lying about their qualifications but having their real academic record available for all to see online. The majority of the students however feel that most people do probably boost their online profile to come across better (Figure 13). There is no significant statistical difference between first and final years (Anova 0.665).

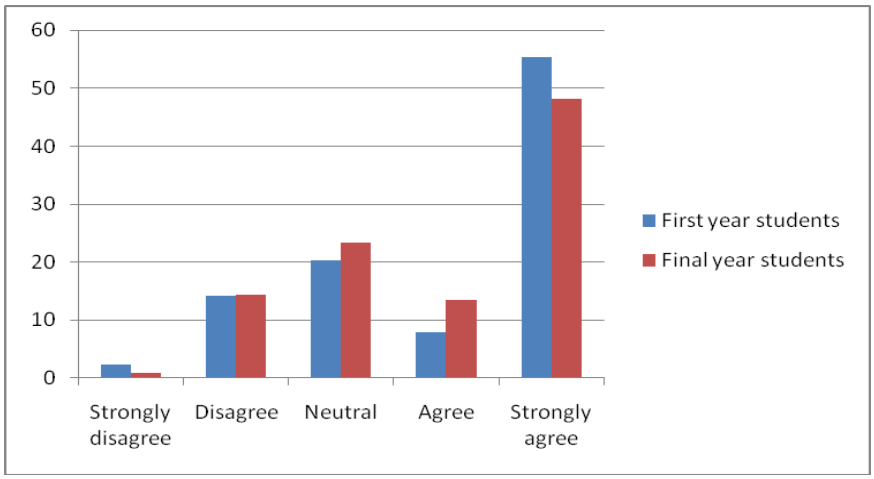

Figure 13: Most online profiles are exaggerated to make the person look more appealing (first year N=177, final year N=133)

While in general there were very little differences in the sort of information students post on the internet, we saw that about 11 per cent of the final year students post their CV or portfolio online compared to 6 per cent of the first year students. Furthermore final year students are far more likely (71%) to post information about the courses they are on than the first year students (51%). This is an indication that final year students are more aware of the importance of detailing their skills and qualifications online than the first year students. However, the survey also revealed that final year students are twice as likely to post inappropriate or suggestive photos of themselves (see Figure 2).

Although students are aware that employers might be checking their online profiles in the future, they do not seem overly concerned about actively managing their online reputation, and feel that their current online self-disclosure creates the right impression about them or have no opinion about it (Figure 14). Again there is no statistical significant difference between the answers of both groups of students (0.441).

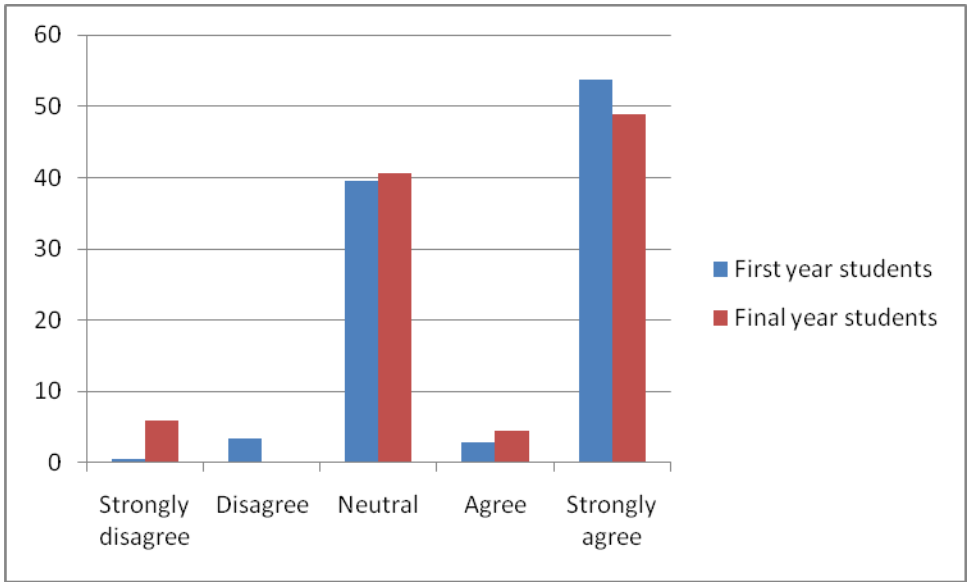

Figure 14: My online disclosure creates the right impression about me (first year N=177, final year N=133)

3.5 Privacy attitudes and behaviour

The questionnaire was designed to measure some theoretical constructs we expected to influence online (self) disclosure. Therefore we used blocks of items to measure (1) the positive nature of online disclosure, (2) the negative nature of online disclosure, (3) general caution, (4) technical protection, and (5) privacy concern.

As a first step, we used factor analysis to check whether the items indeed measured what they were expected to measure, and this proved the case. The analysis resulted in factors representing the theoretical constructs. In the next step, we used the items loading on the various factors to make a scale for the theoretical construct represented by the factor. A simple procedure was adopted for this: we take the average of the scores on the items. To test the internal consistency of the so obtained scales, we calculated Cronbach's Alpha for every scale. Cronbach's Alpha shows how closely related a set of items are as a group. This resulted in relatively high values above 0.7 for both the 'positive nature of online disclosure' dimension (.776) and the 'negative nature of online disclosure' dimension (.862).

	Item	Content
Positive nature	1	The information I can find about myself online makes me feel proud
	2	The information I can find about myself online makes me feel flattered
	3	The information I can find about myself online makes me feel respected
	4	The information I can find about myself online improves my feeling of self-worth
Negative nature	1	The information I can find about myself online makes me feel embarrassed
	2	The information I can find about myself online makes me angry
	3	The information I can find about myself online makes me feel foolish
	4	The information I can find about myself online makes me sad
	5	The information I can find about myself online makes me regret revealing certain things

Table 3: Positive and negative nature of online disclosure

Both the first year students and the final year students score higher on the positive nature of online disclosure items than on the negative ones, which is in line with the finding that they feel that their current online self-disclosure creates the right impression about them.

As already explained in the methods section our survey ascertained the privacy attitudes and behaviours of participants with questions modelled with minor modifications after Buchanan et al.'s (2006) study, as shown in table 4 and table 5. Participants responded to these questions using a 5-point Likert scale for each item ('never – always' for the privacy behaviour questions and 'not at all – very much' for the privacy attitudes questions).

	Item	Content
General caution	1	Do you shred/burn your personal documents when you are disposing of them?
	2	Do you hide your bank card PIN number when using cash machines/making purchases?
	3	Do you only register for websites that have a privacy policy?
	4	Do you read a website's privacy policy before you register your information?
	5	Do you look for a privacy certification on a website before you register your information?
	6	Do you read license agreements fully before you agree to them?
Technical protection	1	Do you watch for ways to control what organisations send you online (such as tick boxes that allow you to opt-in or opt-out of certain offers)?
	2	Do you remove cookies?
	3	Do you clear your browser history regularly?
	4	Do you block instant messages from someone you do not want to hear from?
	5	Do you block emails from someone you do not want to hear from?

Table 4: Privacy behaviour items

	Item	Content
Privacy concern	1	In general, how concerned are you about your privacy while you are using the internet?
	2	Are you concerned about online organisations not being who they claim they are?
	3	Are you concerned that you are asked for too much personal information when you register or make online purchases?
	4	Are you concerned about identity theft?
	5	Are you concerned about people online not being who they say they are?
	6	Are you concerned that information about you could be found on an old computer?
	7	Are you concerned who might access your medical records electronically?
	8	Are you concerned about people you don't know obtaining personal information about you from your online activities?
	9	Are you concerned that if you use your credit card to buy something on the internet your credit card number will be obtained/intercepted by someone else?
	10	Are you concerned that if you use your credit card to buy something on the internet your card will be mischarged?
	11	Are you concerned that an email you send may be read by someone else besides the person you sent it to?
	12	Are you concerned that an email you send someone may be inappropriately forwarded to others?
	13	Are you concerned that an email you send someone may be printed out in a place where others could see it?
	14	Are you concerned about emails you receive not being from whom they say they are?
	15	Are you concerned that an email containing a seemingly legitimate internet address may be fraudulent?

Table 5: Privacy attitude items

We also calculated Cronbach's Alpha for the privacy behaviour items and the privacy attitudes items. This resulted in high values above .8 for both 'Privacy Concern' (.905) and 'General Caution' (.806). However, the adjusted 'Technical Protection' scale showed a lower internal consistency of 0.639, below the acceptable reliability coefficient of 0.7.

From the privacy concern items we learn that the students are not very concerned about their privacy when they are online. On a scale from 1 (not at all concerned) to 5 (very much concerned), the first year students score on average 2.92, while the final year students score on average 2.97. Both groups of students are most concerned about 1) identity theft (average score 3.49), 2) organisations not being who they claim they are (3.43), 3) their credit cards being intercepted by someone else when they make online purchases (3.34), and 4) being asked too much personal information when buying something online (3.30). They are mildly concerned about an email containing a fraudulent internet address (3.18), people online not being who they claim to be (3.13), and their credit card being mischarged when buying something on the internet (3.02). The other items listed in table 5 did not raise much concern among both groups of students (averaging 2.65 or lower).

When we compare both groups of students we do not find a significant difference for general caution, technical protection or privacy concern. When we look at gender differences we see that there are significant differences between men and women with respect to general caution (0.101) and privacy concern (0.015). Women score higher on both the privacy attitude items and the general caution items. There is however no significant difference between the sexes with respect to the technical protection items (0.623). Finally when we look at the academic division of the students (Humanities; Medical Sciences; Mathematical, Physical & Life Sciences; and Social Sciences) we find no significant differences for general caution (0.131), technical protection (0.0403), nor privacy concern (0.967).

	General Caution	Privacy Concern	Technical Protection
Email address	0.335	0.750	0.559
Home address	0.108	0.790	0.650
Private phone number	0.074	0.075	0.716
Date of birth	0.041	0.283	0.289
Real name	0.315	0.063	0.781
Photos of self	0.365	0.089	0.482
Photos of friends/family	0.397	0.037	0.863
Self-description	0.019	0.058	0.270
Favourite links	0.219	0.489	0.022
Political views	0.922	0.155	0.001
CV/portfolio	0.985	0.671	0.065
Religious views	0.015	0.023	0.348
Relationship status	0.561	0.889	0.095
Favourite bands, pastimes, book , etc	0.152	0.264	0.134
Links to friends' homepages	0.957	0.275	0.962
Course you are on	0.015	0.054	0.078
Suggestive/inappropriate photos of self	0.293	0.023	0.993
Diary of your daily life	0.311	0.605	0.732

When we examine the correlations between our five theoretical constructs (the positive nature of online disclosure, the negative nature of online disclosure, general caution, technical protection, and privacy concern) we find that students who score high on the 'negative nature of online disclosure' show a higher privacy concern (0.172**). Also, students who score high on the 'negative nature of online disclosure' score low on the 'general caution' dimension (negative correlation of -.134*). This could mean that students who feel negative about their online disclosure take fewer precautions with regards to privacy issues (See Table 6).

Correlations

		Positive nature	Negative nature	General caution	Privacy concern	Technical protection
Positive nature	Pearson Correlation	1	-.143*	.021	.014	.025
	Sig. (2-tailed)		.024	.745	.828	.696
	N	250	250	240	238	240
Negative nature	Pearson Correlation	-.143*	1	-.134*	.172**	-.042
	Sig. (2-tailed)	.024		.038	.008	.518
	N	250	250	240	238	240
General caution	Pearson Correlation	.021	-.134*	1	.276**	.352**
	Sig. (2-tailed)	.745	.038		.000	.000
	N	240	240	299	294	299
Privacy concern	Pearson Correlation	.014	.172**	.276**	1	.108
	Sig. (2-tailed)	.828	.008	.000		.064
	N	238	238	294	294	294
Technical protection	Pearson Correlation	.025	-.042	.352**	.108	1
	Sig. (2-tailed)	.696	.518	.000	.064	
	N	240	240	299	294	299

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 6: Correlations between the five theoretical constructs

When we compare privacy attitudes with privacy behaviour we see that final year students score a little bit higher on general caution. On a scale from 1 (never) to 5 (always), the first year students score 3.07, while the final year students score 3.13. Figure 15 gives an overview of the 'Always' answers of the students (for the precise phrasing of the statements, please refer to table 4).

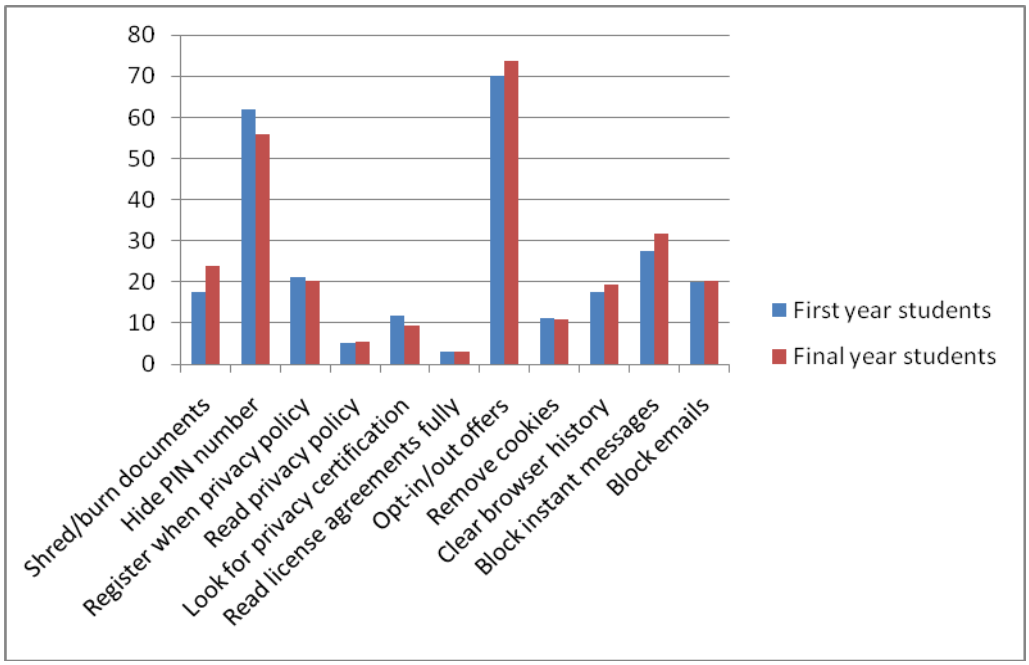

Figure 15: Privacy behaviour – 'always' answers (first year N=170, final year N=129)

A lot of studies have found that individuals' privacy attitudes seem inconsistent with their behaviour. According to Acquisti and Grossklags (2004) many surveys and experiments have uncovered a dichotomy between stated attitudes and actual behaviour of individuals facing decisions affecting their privacy and their personal information security: "Surveys report that most individuals are concerned about the security of their personal information and are willing to act to protect it. Experiments reveal that very few individuals actually take any action to protect their personal information, even when doing so involves limited costs" (Acquisti & Grossklags, 2004: 165).

As Buchanan et al. point out, there is likely to be a complex relationship between privacy attitude and privacy behaviour. Therefore, it is important to consider behaviours that people may adopt to safeguard their privacy. What we see in our study is that although students do not seem too concerned about their privacy, they do adopt behaviours to protect their privacy. They use pop-up window blockers (89%), firewalls (89%), anti-spy ware software (84%), browser privacy features (56%), and cookie controls (37%). Maybe the explanation is as Buchanan et al. suggest: "Concern prompts us to take preventive measures, but knowing that measures have been taken could reduce our level of concern" (Buchanan et al, 2007: 159).

4. Conclusions

In this report we examined students' online disclosure and students' online privacy perception. The results were based on a survey among 349 undergraduate students at the University of Oxford. In our analysis we made a distinction between first year and final year students. We hypothesized that students in their final year at university, who are about to enter the job market, might be more aware of (both the positive and negative) consequences of online disclosure and change their online behaviour accordingly.

Over 90% of the students post information on social network sites. The information they post on these social networks and on other sites such as blogs, photo and video sharing sites and personal websites is very similar among the two groups. The first year students use more different outlets to disclose information, but the evolution of social network sites into all-in-one platforms seems to have taken over many of the functions previously provided by personal websites and blogs, making the latter less popular among the respondents. Both the first and final year students generally use their real name when disclosing information on a SNS.

With regards to the type of information the students disclose there is little difference between the level of posting personally identifiable information and non-identifiable information. As already noted in the report this can lead to serious negative consequences (Krishnamurthy & Wills, 2010). In our focus groups we will ask more in-depth questions about the students' understanding of these consequences: How aware are students of the various potential negative consequences of disclosing information on the internet? Do they realize that a digital trail is forever?

Not only the type and the amount of information that students post online, but also the reason for disclosing information, is very similar among the two groups. Our survey shows that the main reason for online disclosure is 1) to keep (distant) family and friends informed, 2) self-expression, 3) re-acquiring lost contacts, 4) boredom and 5) because everybody else does it. Being creative, sharing ideas, beliefs and philosophies are moderately important, while getting new friends, self-promotion and search for recognition are not considered to be important motivations. The key audiences the students think are reading their profiles and blogs are friends, family and fellow students. One would have expected final year students to include future employers more often as a key target audience. However, the data does not show this. The students do however expect potential employers to read their online information in the future.

When students post photos or videos online of other people, they almost always tag these with the full names of the people featuring in them without asking for consent. When these people

ask them to remove information, text or photos and videos they will almost always oblige.

However, the students seldom get asked to remove content by others. Over 40% of the students themselves have asked others to remove information or photos about them (but there is no significant difference between first year and final year students in this respect). This can be seen as one method of online reputation management. Online reputation management is expected to become more important for those students who are closest to leaving university and having to find a job. We do indeed see this in our study. Final year students are significantly more likely to 'Google' themselves, they are significantly more aware of the fact that employers will use the internet to check up on potential job candidates, and they are more likely to post their CV or portfolio and course information online. In our follow-up research we will focus more in-depth on online reputation management. We will ask students how they feel about 'creating a strong online brand' and whether they think employers have a right to check their online profiles and use what they find to influence their hiring decisions. We will also pay more attention to the use of business-oriented social networking sites such as LinkedIn, Ecademy and Xing. On these professional social networks a user completes a professional profile and invites professional contacts to connect to the profile.

An interesting finding from our study is that our respondents seem to be more careful in their actual privacy behaviour than one would expect from their relatively low level of privacy concern. A lot of research has found that people claim to be worried about their privacy, but do not act this concern out in their privacy behaviour. In our study the students seem to take preventive measures to protect their privacy, which might explain their reduced level of concern.

The next step in our student online disclosure case-study is to organize focus groups with first and final year students to elicit more qualitative data. The survey as used for this report will be repeated in the final term of 2011 among the first group of students to see if their behaviour/attitudes and opinions have changed.

References

Acquisti, A. and J. Grossklags (2004) Privacy Attitudes and Privacy Behavior. In: J. Camp and R. Lewis (eds), *The Economics of Information Security (Advances in Information Security),* pp. 165 – 178, Springer: 2004.

Barnes, S. (2006) A privacy paradox: social networking in the United Sates, *First Monday* 11 (9), July 2006.

Besmer, A. and H.R. Lipford (2008) Privacy Perceptions of Photo Sharing in Facebook. 4th Symposium on Usable privacy and security 2008, Pittsburgh, Pennsylvania. July 23 - 25, 2008.

Boyd, D.M. and N.B. Ellison (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Buchanan, T., C. Paine, A. Joinson and U-D. Reips (2007) Development of Measures of Online Privacy Concern and Protection of Use on the Internet. *Journal of the American Society for Information Science and Technology*, 58 (2): 157-165.

Dutton, W., E. Helsper and M. Gerber (2009) The Internet in Britain: 2009. OxIS Oxford Internet Surveys. Oxford Internet Institute, University of Oxford.

Krishnamurthy, B. and C.Wills (2010) On the Leakage of Personally Identifiable Information Via Online Social Networks. ACM SIGCOMM *Computer Communication Review*, Volume 40, Number 1, pp. 112 – 117.

Microsoft (2010) Online Reputation in a Connected World. Report by Cross-Tab Marketing Services, commissioned by Microsoft. http://www.microsoft.com/privacy/dpd/research.aspx

Tarnowski, L. (2009) Social Media is the new way to secure some work. *The Daily Telegraph*, May 14, 2009.