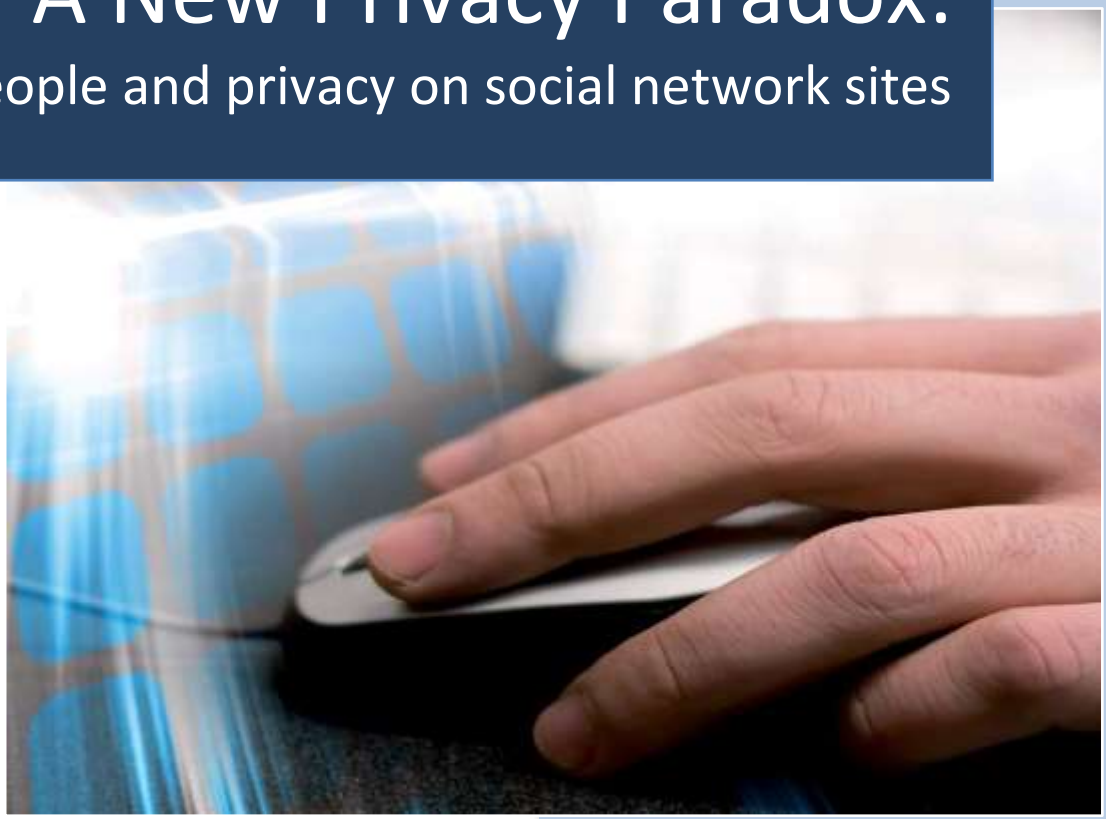
Global Cyber Security Capacity Centre

Oxford Internet Institute
University of Oxford

Global Cyber Security Capacity Centre: Draft Working Paper

A New Privacy Paradox:

Young people and privacy on social network sites



Grant Blank
Oxford Internet Institute and Global Cyber Security Capacity Centre, University of Oxford

Gillian Bolsover
Oxford Internet Institute, University of Oxford

Elizabeth Dubois
Oxford Internet Institute, University of Oxford

April 2014

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

A New Privacy Paradox:

Young people and privacy on social network sites

Grant Blank
Oxford Internet Institute and Global Cyber Security Capacity Centre, University of Oxford, grant.blank@oii.ox.ac.uk

Gillian Bolsover
Oxford Internet Institute, University of Oxford, gillian.bolsover@oii.ox.ac.uk

Elizabeth Dubois
Oxford Internet Institute, University of Oxford, elizabeth.dubois@oii.ox.ac.uk

Abstract: There is a widespread impression that younger people are less concerned with privacy than older people. For example, Facebook founder Mark Zuckerberg justified changing default privacy settings to allow everyone to see and search for names, gender, city and other information by saying "Privacy is no longer a social norm". We address this question and test it using a representative sample from Britain based on the Oxford Internet Survey (OxIS). Contrary to conventional wisdom, OxIS shows a negative relationship between age and privacy; young people are actually more likely to have taken action to protect their privacy than older people. Privacy online is a strong social norm. We develop a sociological theory that accounts for the fact of youth concern. The new privacy paradox is that these sites have become so embedded in the social lives of users that they must disclose information on them despite the fact that these sites do not provide adequate privacy controls.

Prepared for the Annual Meeting of the American Sociological Association, 16-19 August 2014, San Francisco, California. We thank the Oxford Internet Institute and the Global Cyber Security Capacity Centre at the University of Oxford for supporting this research. We thank William H. Dutton for valuable comments on an earlier draft.

A New Privacy Paradox:

Young people and privacy on social network sites

Standing on a stage in San Francisco in early 2010, Facebook founder Mark Zuckerberg, responding in part to the site's recent decision to change the privacy settings of its 350 million users, said that as Internet users had become more comfortable sharing more information online with more people privacy was no longer a social norm (Johnson & Vegas, 2010). Because information about the users of social media was being sold by Facebook to advertisers and other third parties for targeted advertisements at higher prices, Zuckerberg has a commercial interest in relaxing norms surrounding online privacy, but his attitude has been widely echoed in popular media.

The idea of a privacy paradox is commonly referenced in relation to SNSs; the idea that young people are sharing their private lives online, providing huge amounts of data for commercial and government entities, that older generations have fought and are fighting to keep private, because they do not fully understand the public nature of the Internet and its implications (Barnes, 2006). Some have gone so far as to assert that this practice may be the biggest generational split since the early days of rock and roll (Nussbaum, 2007).

There has been relatively little systematic research into privacy attitudes or actions among different age groups, or, for that matter, into most of the other major variables, such as race and gender, that may relate to how people present their private lives in online settings. Some evidence points to growing concern among Internet users about online privacy and increased concern over the ability of users to manage their information privacy online, for instance utilizing the privacy settings on popular SNSs (Marwick et al., 2010). A 2013 Pew study

found that 50 percent of Internet users were worried about the information available about them online, compared to 30 percent in 2009 (Rainie, Kiesler, Kang, & Madden, 2013). Following the revelations that the U.S. National Security Administration was collecting the telephone and Internet metadata of its citizens, a Washington Post-ABC poll found that 40 percent of U.S. respondents said that it was more important to protect citizens' privacy even if it limited the ability of the government to investigate terrorist threats (Cohen & Balz, 2013). So privacy concerns may be increasing at the same time as conventional wisdom holds onto the view that younger people are less likely to act to control the privacy of their personal information in the online setting.

With these issues in mind this paper addresses the question: how does age relate to online privacy and, in particular, do young people do less to protect their online privacy than older Internet users? The next section lays out a sociological theory of privacy grounded in an understanding of how people organize their social life. This is followed by a review of prior research and a discussion of our methods. The paper then presents data on actions taken to protect privacy and related variables. To conclude the paper discusses of these findings, their limitations, and the implications for future research.

Literature review

Privacy concerns an individual's ability to control what personal information is disclosed, to whom, when and under what circumstances. The unauthorized disclosure of personal information is normally considered a breach of privacy, although authorization and what is personal information are matters of dispute, particularly in an online context. Altman (1975, 18) describes privacy succinctly as "selective control of access to the self" although this might go

beyond legal definitions and hark back to related definitions of privacy focused on the right to be left alone, as framed by Warren and Brandeis (1890).

Many agree that disclosure and privacy are closely connected to fundamental characteristics of social life (Nissenbaum, 2011; Rule, 2009). Social life is powerfully structured by the context in which it takes place. People become acquainted based on many shared characteristics: some people you know from a local neighborhood—either current or past neighborhoods; others from sports clubs, church groups, hobby clubs, pubs or other leisure activities. Others are from current or prior education: school friends, university friends. Still others are based on common occupations or professions, or are people who work for the same company or organization. Almost everyone has family and relatives.

A variety of sociological theories suggest that privacy is part of the structure of social life. Rainie and Wellman, for example, describe how people who once experienced social life in relation to small and tight-knit communities are now becoming increasingly networked individuals with access to much larger and more loosely defined social connections (2012). With larger networks of looser ties, the practice of personal information sharing on a daily basis could become more challenging. Does information flow through the entirety of an individual's network or is it limited in some way?

Others focus more pointedly on specific realms where privacy expectations and values may be different. Nissenbaum describes the notion of 'context' in terms of roles, activities, norms, and values (2009, p. 133). She explains that a variety of factors represent, in an abstract sense, the social structures experienced in daily life. For example, Bourdieu's 'field theory' describes social systems wherein agents (individuals) are bounded by rules (norms) in specific fields (circumstances) (Martin, 2003). Nissenbaum argues that the different characteristics of

different fields are crucial for considering what is and what is not a violation of privacy (2009). Similarly Walzer describes a theory of justice in which context is crucial for deciding between right and wrong (1984) and Searle (and many others) explain how integral different social settings are to understanding social reality (1995).

Goffman explains the social psychology of these issues by describing how people act differently depending on who they are performing to. Individuals engage in "impression management" by presenting different versions of themselves to different audiences. The expectations and norms of the audience govern what personal information is presented and what is kept hidden (1959). Marwick and boyd extend this argument SNSs by looking at the "imagined audiences" of SNS users (2011).

The issue of audiences highlights a fundamental problem with privacy in some SNSs: Marwick and boyd (2011) describe 'context collapse', in which audiences that are separate offline collapse into a single unified online context. The management of this issue varies across social networking sites.[1] For example, Facebook started as a website restricted exclusively to university students at select elite US universities where it was bounded by the common norms of a small, self-selected population which was relatively homogeneous in terms of age, behavior and education. It has since diffused to become a transnational network with more than 1.15 billion active monthly users of all ages (Constine, 2013) where extreme heterogeneity is typical. SNS users often have difficulty conceptualizing the audiences that read their online posts and use the same account to address different audiences at different times (Marwick & boyd, 2011).

[1] Google+ seeks to avoid this problem with its concept of "groups". More specialized SNSs, like LinkedIn or dating sites, avoid the problem by focusing on a more limited social circle with a single set of norms, like employment in the case of LinkedIn. Facebook has begun to allow users to put people into categories called "groups", however, these are harder to use than Google+ groups. Google+ immediately prompts users to put people into a group; Facebook requires that users take the initiative to create groups and add people to them.

Heterogeneous contexts logically might lead to privacy problems: There are serious consequences when actions that are normatively appropriate in one context are revealed to members of another audience where norms are different; for example, a 24-year-old US high school teacher was forced to resign after a parent complained about a photo of her holding a glass of wine and a mug of beer while on holiday in Europe that was posted to her Facebook profile (Downey, 2011). Although the problem is particularly evident on Facebook, it appears on other SNSs as well. Twitter is primarily public and that can have serious consequences; for instance, Justine Sacco, a corporate communication specialist, was fired by her employer for what some saw as an insensitive tweet about AIDS in South Africa (Bercovici, 2013; Southall, 2013). Other examples abound. Even on Google+ there is nothing to prevent a naïve user from following the Facebook default that puts all their contacts into a single group.

This suggests that SNSs are a particularly good research site to investigate how people handle privacy. They create privacy problems that may make users more self-consciously concerned about privacy than in many other online situations.

There is a large body of literature that concerns online privacy; however, the number of published papers that use systematically collected data is very small. We were able to find only three peer-reviewed papers that addressed questions of privacy using a sample that could be generalized to a population: Taddicken (2013), who used an Internet panel to create a sample of 2,739 German adults, Turow and Hennessy (2007), who conducted a telephone survey of 1,200 US adults, and Milne and Culnan (2004), who constructed a sample of 2,468 US adults based on the Harris Poll Online panel. In addition, there are two Pew reports (Madden & Smith 2010; Raine et al., 2013), which use random digit dialing to construct a representative sample of US

adults, and a research report by Hoofnagle, King, Li, and Turow that used a similar methodology (2010).

However, the majority of research in relation to privacy on SNSs uses convenience samples, often of university students. Early research in this area was conducted during the period that Facebook was limited to a relatively homogeneous population of university students, concluding that "only a vanishingly small number of users change the (permissive) default privacy preferences" (Gross & Acquisti, 2005).[2] However the rapid increase in the heterogeneity of SNS users and high levels of media coverage of privacy-related issues may have persuaded Internet users to become more concerned controlling their online privacy. A more recent study using a convenience sample of 200 Facebook users recruited via Amazon Mechanical Turk found that only 36 percent of content was shared using the default privacy settings (Y. Liu, Gummadi, Krishnamurthy, & Mislove, 2011).

Demographic Characteristics

A great deal of research has examined how demographic variables are related to privacy. Gender, in particular, is frequently related to privacy perceptions and practices both on- and offline. In a study using a convenience sample of university students, males have been found to be more likely to post risqué pictures containing sexual content or alcohol to their Facebook profiles and were less concerned than female students about current or prospective employers seeing this type of photo online (Peluchette & Karl, 2008). Similarly, female university students were found to be more likely to have private profiles (Lewis, Kaufman, & Christakis, 2008).

[2] The world's largest social networking, Facebook, was limited to Harvard University students when initially launched in February 2004. It was expanded to other elite universities in March 2004, before opening enrolment to all university students, then high school students, and finally everyone aged over 13 in late 2006.

However, a more recent study of undergraduate students' Facebook use noted few gender differences related to self-reported use, skills and privacy practices (boyd & Hargittai, 2010). They considered it noteworthy because "it is rare for women and men to report the same level of comfort with online tasks".

Possibly because of the widespread use of college student samples, the relation between education and privacy has been largely neglected. An email survey of 889 Internet users, found that users with less education tended to be less concerned with online privacy (Sheehan, 2002).[3] Milne and Culnan (2004) found that education level was negatively related to the likelihood of reporting reading online privacy policies. Similar results were found by O'Neil (2001), who analyzed online survey data collected via solicitation. A Pew report found that those who had a college or graduate degree were more likely to have utilized privacy protection measures online, such as clearing their browser and cookie histories, or encrypting their Emails (Rainie, Kiesler, Kang & Madden, 2013). However none of these studies examine how educational level may affect an individual's likelihood of acting to protect their privacy in social networking sites.

Another understudied area is that of income. One of the only studies to include income as an independent variable, Sheehan (2002) found that income had no significant effect; however, higher income brackets were overrepresented in the sample, with almost half of respondents earning more than $60,000 per year. In contrast, O'Neil (2001) found that Internet users with higher incomes were less concerned with online privacy. However, again these studies generally focus more on concern than action, and do not specifically address privacy on SNSs.

[3] Sheehan's (2002) data are from a random sample of email addresses available from the Four11 directory search engine. At the time of the search Sheehan reports that Four11 contained about 15 million addresses.

Results for age have been mixed. Sheehan (2002) found that older Internet users were more polarized in their attitudes to online privacy than younger users, and that the respondents most concerned about privacy tended to between ages 25 and 54. However, based on an online survey of German Internet users, Taddicken (2013) found that age had little relationship to SNS information disclosure, privacy concerns or the number of sites used. Similarly based on a representative US sample, Hofnagle et al (2010) found no significant differences by age across a range of privacy variables. However two Pew telephone surveys of representative samples of the US population both found that older users were less likely to have changed their privacy settings, deleted unwanted comments, removed their name from photos or taken steps to limit the information about them on SNSs; young adults were also less trusting of the sites that host their online content (Madden & Smith, 2010, Raine et al. 2013). These ambiguities surrounding age make it fertile ground for additional research.

Non-demographic characteristics

Research into the non-demographic characteristics that may affect online privacy practices can be broken into five main areas: concern about privacy, computer skills, bad experiences, the number of SNS sites used and individual psychological characteristics. Individual psychological characteristics are often seen as an explanation for these other non-demographic factors.

Concern about privacy has consistently been found to have little or no association with online information disclosure (Taddicken, 2013). Furthermore, a psychological study of 343 undergraduate students found that, contrary to the expectations of the authors the propensity to disclose information online and the propensity to control information disclosed online were not significantly negatively correlated, and were associated with different underlying personality

traits: the need for popularity significantly predicted disclosure while levels of trust and self-esteem predicted information control (Christofides, Muise, & Desmarais, 2009).

In another study of the personality traits related to information disclosure on SNSs, C. Liu, Ang, and Lwin (2013) found, based on a survey of 780 adolescent Facebook users, that narcissism increased personal information disclosure and social anxiety decreased it. In contrast to previous studies (e.g., Taddicken, 2013), the authors found that privacy concerns reduced information disclosure and suggested that it may be a moderating factor between personality traits and information disclosure. General general levels of willingness to self-disclose, both of which can be considered as personality traits, have also been found to be related to online information disclosure (Christofides et al., 2009; Taddicken, 2013).

Computer skills and ability is also often hypothesized to be related to online privacy perceptions and practices, and the allegedly better skills of the educated and the young are often advanced as an explanation for the effects of these variables. Turow and Hennessy (2007), found that respondents with higher online skills had a lower fear of information disclosure online but had a reduced trust in online institutions to protect their personal information. Based on a convenience sample of undergraduate students, boyd and Hargittai (2010) found that, controlling for the frequency of use, Facebook users with higher self-rated skills were more likely to have modified their privacy settings. However, care must also be taken when evaluating skills. Interviewing young people about their use of SNSs, Livingstone (2008) reports that “a fair proportion of those interviewed hesitated when asked to show me how to change their privacy

settings, often clicking on the wrong options before managing this task, and showing some nervousness about unintended consequences of changing settings."[4]

Dutton and Shepherd (2006) found that trust in the Internet rose with increasing experience; however, they concluded that "with experience can come bad experiences… which can undermine trust and use of the technology (Dutton & Shepherd, 2006, p. 446). However, further work found that the number of bad experiences a user had experienced had little effect on trust and online content creation (Blank & Dutton, 2012; Blank & Reisdorf, 2012; Blank, 2013). In contrast, looking specifically at SNSs Debatin, Lovejoy, Horn, and Hughes (2009), based on a survey of 119 undergraduate students and eight open-ended, follow-up interviews, found that users who reported having experienced personal privacy invasions (unwanted advances, stalking, or harassment; damaging gossip or rumors; and having personal data stolen or abused by others) were more likely to have changed their privacy settings than those who had heard about others who had experienced these violations. However, the size of this sample is very small (23 students who had experienced violations of privacy and 41 who had heard about others who had experienced these violations), so more work is needed to examine how bad experienced online might affect SNS users approached to online privacy.

A fifth non-demographic factor, the number of SNS sites used, has been found to be related to privacy concerns. Taddicken (2013), asking about the frequency of use of six different social media applications, found that individuals with higher privacy concerns used fewer applications but that those who used fewer applications disclosed more information. This finding

[4] Research has also shown that users privacy settings often do not match their expectations, with Liu et al. (2011) finding, based on a convenience sample of 200 Facebook users, that user's privacy settings only matched their expectations 37 percent of the time, almost always exposing more content than the user intended.

raises additional questions such as do those who use fewer applications tend to have lower computer skills or do they only use the sites that they trust to protect their privacy?

Psychological factors are often put forward as an explanation for the non-demographic variables that are found to affect information disclosure and control on SNSs. This approach focuses on information discourse and control as a result of conscious or unconscious choices rather than as a result of low skills or a lack of understanding of online privacy. For instance, Chang and Heo (2014), based on a survey of 192 university students, found that those who used Facebook for socializing (as opposed to hedonic, utilitarian or social investigation motives) were more likely to disclose information online.

To summarize, this survey of the literature finds three main areas of investigation with relation to privacy on SNSs: concern about privacy, information disclosure, and actions taken to protect privacy. This research often uses convenience samples of college students, which means it is unable to adequately address age effects (as well as potentially related variables such as education and income). This then leads to the question does a generation gap exist? However, given that previous research has come to different conclusions concerning the effects of age (as well as gender, education and income) on information disclosure and control online, it is important to establish, based on strong, representative data, the effects of these variables on privacy related practices on SNSs.

Methodology

The Oxford Internet Surveys (OxIS) collect data on British Internet users and non-users. Conducted biennially since 2003, the surveys are nationally representative random samples of more than 2,000 individuals aged 14 and older in England, Scotland, and Wales. Interviews are conducted face-to-face by an independent survey research company. The analyses below are

restricted to the 61% of the British population who were current SNS users in 2013, N = 1,629, or the 48% who were SNS users in 2011.

Our measure of privacy is an item asking respondents who have a profile on any SNS when they have checked or changed their privacy settings on any SNS. It is a 6-category Likert scale with response ranging from Never to More than Daily; below we usually dichotomize it to Never versus all other categories.

Among the demographic variables, race is coded into three categories: white, Asian and black. Place is coded as urban versus rural. Lifestage is a four-category variable: students, employed, unemployed and retired. Marital status has five categories: single, married, living with partner, divorced, widowed. We also include gender, education, age and income measured as total household income before tax.

The extent to which people see revealing personal information as risky may influence their privacy efforts. Five items ask about comfort revealing specific items of personal information: Comfort revealing an email address, a postal address, a phone number, a date of birth or a name. A PCA indicated that these formed a single factor with a Cronbach's alpha of 0.88 so we used the factor scores to create a measure called "Comfort revealing personal data".

Bad experiences on the Internet could influence attention to privacy. OxIS asks about six possible bad experiences on the Internet: SPAM, viruses, misrepresented purchases, stolen identity, requests for bank details, and accidentally reaching a porn web site. Each variable is a yes-or-no, dichotomous variable. We summed these variables to produce a "bad experiences" index, with values ranging from 0-6.

Concern with negative experiences was measured by creating an index from three variables: concern with spam, viruses, or obscene or annoying email. Each was measured on a

four-category likert scale where 0 meant No Concern at All and 3 meaning Very Concerned. These three variables were summed to produce an index ranging from 0 to 9.

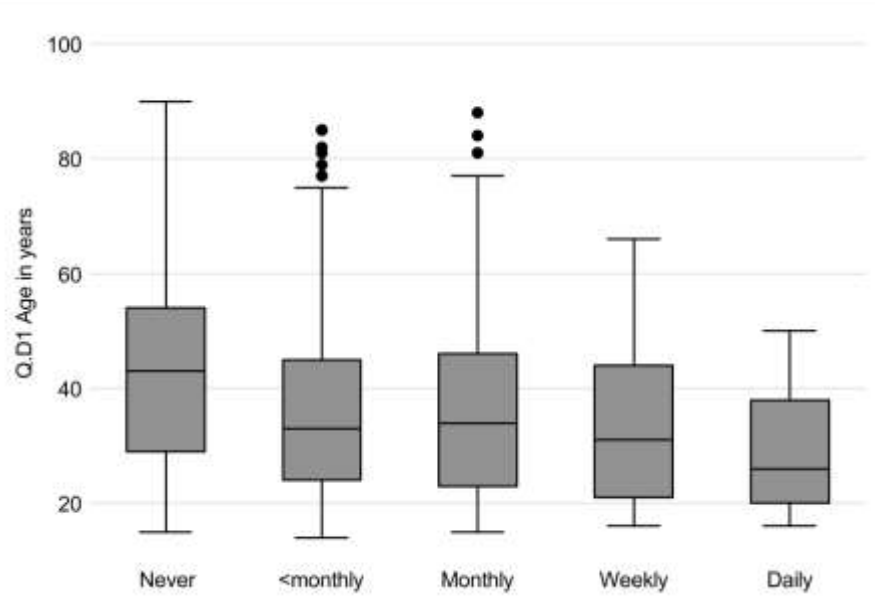
OxIS asks respondent whether they use each of 10 SNSs: Bebo, Facebook, an online dating site, Google+, Instagram, LinkedIn, MySpace, Pinterest, Twitter or any other SNS. These sites were chosen because other research indicated that each was used by at least 5% of the British population. The sum of these variables was used to measure "number of SNSs used", with a range of 0-10.

Finally, self-reported ability using the Internet is measured in OxIS using a five-point scale. Respondents are asked if they would rate their ability as bad, poor, fair, good or excellent.

Results

Since our primary interest is in the relationship between privacy and age, we begin with the grouped box plot in Figure 1. There is a clear inverse relationship. The median age of respondents who never check their privacy settings is 43 compared to a median age of 26 for respondents who check privacy settings daily. Immediately this suggests that the common assumptions that youth do not care and will not act on privacy concerns is potentially wrong.

Figure 1: Age versus Frequency of checking or changing privacy settings



OxIS 2013 N = 1,321 SNS users. The categories Daily and More than Daily have been combined since only 2 respondents reported checking privacy settings More than Daily.

Table 1 shows the zero-order relationships between privacy and seven demographic variables. For comparison, the first row of the table gives the totals for all SNS users. Overall about two-thirds of SNS users have checked or changed their privacy settings.

The age results are the most interesting in this table as they contradict previous studies which suggest age and privacy have little to no relation (Taddicken 2013; Hofnagle et al. 2010). Almost 95% of 14-17-year-olds have checked or changed their privacy settings. From there the percentage who have taken action to protect their privacy drops almost monotonically to the 32.5% of respondents age 65 and over. The strength of this effect is remarkable: between the oldest and youngest the difference is over 62 percentage points. Young people are the most likely of any age group to report having taken action to protect their privacy on social networking sites.

Table 1: Demographics of SNS use and privacy settings

	SNS users who have checked or changed their privacy settings	
	%	N
Total	65.0	871
Age		
14-17	94.9	67
18-24	77.4	193
25-34	67.1	207
35-44	71.3	187
45-54	54.8	123
55-64	52.7	71
65+	32.5	23
Education		
No qualification	52.2	80
Secondary	64.0	326
Further education	70.7	176
Higher education	70.9	289
Income		
<=£12,500	58.8	199
>£12.5-£20,000	66.1	204
>£20-£30,000	69.1	167
>£30-£40,000	75.0	122
>£40-£50,000	74.9	59
>£50-£80,000	66.2	67
Lifestage		
Student	90.4	152
Employed	66.1	517
Retired	43.1	43
Unemployed	57.5	148
Marital status		
Single	75.2	349
Married	58.5	319
Living with partner	67.8	146
Divorced/Separated	69.2	50
Widowed	42.3	6
Gender		
Male	64.3	413
Female	68.0	458
Urban/rural		
Rural	72.7	109
Urban	65.0	761

Table 1: Demographics of SNS use and privacy settings

	SNS users who have checked or changed their privacy settings	
	%	N
Ethnicity		
Asian	54.6	56
Black	73.2	44
White	67.2	757

Educated people are the more likely they are to have changed their privacy settings, consistent with Pew (Raine et al., 2013). The difference between the highest and lowest percentage is 18 points, so the apparent effect is smaller than age.

In the literature the effect of income is uncertain with some claiming no effect exists (Sheehan, 2002) and others suggesting those with a higher income will be less concerned with privacy (O'Neil, 2001). When considering actual action we see people with higher incomes are more likely to have changed their privacy settings. There is a slight drop in the highest income category, £50-80,000 per year, but the Ns are small and the drop may be sampling error.

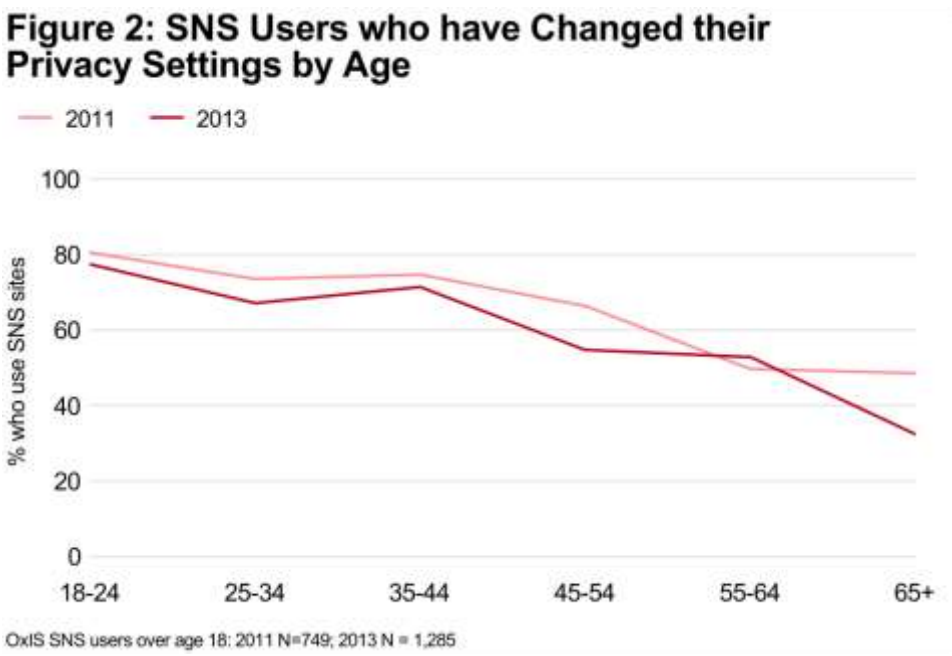
Students are most likely to have changed their privacy settings, followed by employed, unemployed and retired people. Since most students are young while retired people are old this may indirectly reflect age.

Singles are most likely to have changed their privacy settings, followed by people living with a partner. Married and divorced/separated respondents are similar, and widowed individuals are the least likely to have changed their privacy settings. However, again this pattern suggests that these variables may be proxies for age.

The differences in the percentages of SNS users who have changed their privacy settings in the remaining variables are not large. Women are slightly more likely than males to report

having checked or changed their SNS privacy settings: 68 percent of females compared to 64 percent of males, a four percentage point difference. Rural respondents are 7.7 percentage points more likely to have checked or changed their privacy settings than urban respondents, again not a large difference. Finally, Asians were the least likely to have changed their privacy settings, and blacks were the most likely.

Finding the strong age effects in Table 1, we can look back to ask if this pattern is present in earlier surveys. Figure 2 compares 2011 and 2013, showing that there has been little change in this pattern of age effects over the past two years. If anything, the percentage of users who have checked or changed their privacy settings fell somewhat between 2011 and 2013.

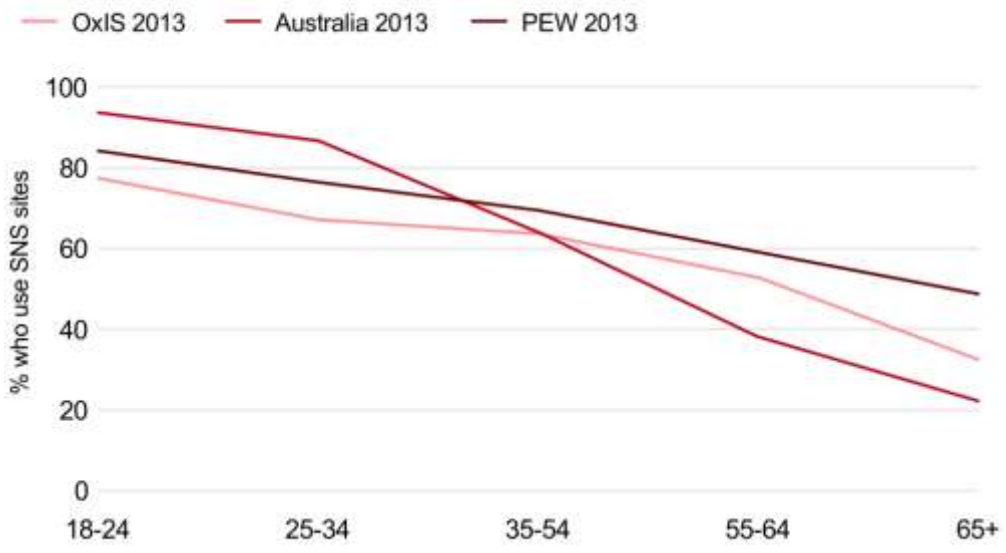


Recent nationally representative surveys in Australia (OAIC 2013) and the USA (Pew 2013)[5]. Since the Australian dataset only reported age as a 6-category variable, we constructed age categories for Pew and OxIS to make the results directly comparable. Figure 3 shows that three nations share an amazing similarity. The lines are usually within the margin of sampling

[5] Pew Research Center and OAIC, though sources of this data, bear no responsibility for the interpretations presented or conclusions reached based on that data.

error of the surveys (3-4 percentage points). The only difference is that Australian young people report protecting their personal information more frequently than in the USA and UK, with only 6 percent of Australian 18 to 24 year olds reporting having never adjusted their privacy settings, compared to 16-20 percent in the US and UK. The age effect is even stronger in Australia, however the trend remains the same: young people are more, not less, likely to have taken action to protect the privacy of their personal information on social networking sites.

Figure 3: SNS Users who have Changed their Privacy Settings by Age (UK, US, Australia)



OxIS SNS users 2013: N = 1,321; Australian SNS users 2013: N = 822; PEW SNS users 2013: N = 432

Multivariate models

We can compare the relative importance of these variables with multivariate models. Table 2 shows odds ratios from hierarchical logistic regression models, using two categories of variables: demographic variables and non-demographic variables. The dependent variable is whether or not the respondent reported checking or changing their privacy settings. Model 1 contains all the demographic variables in OxIS but it is somewhat misleading since it has

collinearity problems. The largest condition index is 21.1. Auxiliary regressions showed that the problem was collinearity between age and lifestage. This is not surprising since students are disproportionately more likely to be young people while older people are more likely to be retired. Since lifestage appears to be distorting the other coefficients, we elected to drop it from further models. Model 2 shows the demographic-only model without lifestage.

The results from Model 2 show that after controlling for other demographic variables, all the age coefficients remain significant: younger people are more likely to have checked or changed their privacy settings. [6] For education, only respondents with higher education degrees are significantly different from people with no educational qualifications. They are over twice as likely to have changed privacy settings. Respondents living in rural areas are more likely to have changed privacy settings. Income is generally not significant and neither gender nor marital status are ever significant. The core takeaway from this model is that the respondents who have checked or changed their privacy settings are disproportionately young and well-educated. As so often on the Internet, young, educated elites dominate.

[6] There are various ways to specify these models. In general, the major difference is whether include income or lifestage, and whether to include age as a categorical variable or a continuous variable. We explored all of these. The specification of age does not change the pattern of collinearities: age and lifestage remain collinear, so both cannot be included. We include age as a categorical variable because that matches the presentation in the tables. Using the continuous version of age does not change the substantive results.

Table 2: Logistic regression models reporting odds ratios

Variable	Model 1	Model 2	Model 3
Age			
18-24	0.378	0.166*	0.161*
25-34	0.354	0.116**	0.127**
35-44	0.348	0.122**	0.168*
45-54	0.192	0.066***	0.094**
55-64	0.145	0.057***	0.088**
65-74	0.043**	0.027***	0.042***
75+	0.047**	0.030***	0.051***
Education			
Secondary school	1.361	1.410	0.950
Further education	1.552	1.753	1.159
Higher education	1.910*	2.127**	1.157
Urban	0.552**	0.557**	0.445***
Female	1.216	1.219	1.412*
Income			
£12.5-£20,000	1.408	1.426	1.275
£20-£30,000	1.332	1.270	1.118
£30-£40,000	1.430	1.399	0.917
£40-£50,000	2.159*	2.178*	1.311
£50-£80,000	2.089	1.990	1.026
Lifestage			
Employed	0.284		
Retired	0.557		
Unemployed	0.259		
Marital status			
Married	0.794	0.780	1.062
Living with person	0.956	0.905	1.165
Divorced/separated	1.761	1.709	1.826
Widowed	1.060	1.068	1.171
Non-demographic variables			
Comfort revealing information			1.127***
Ability to use the Internet			1.520***
Number of bad experiences			1.240**
Number of SNS sites used			1.448***
Concern with bad experiences			1.104**
Constant	19.627***	15.629***	0.360
N	1,220	1,230	1,210
McFadden's R^2	9.7%	8.9%	19.0%
BIC	1878.7	1882.6	1696.9

Notes: * p < .05; ** p < .01; *** p < .001

Omitted categories are age 14-17, no educational qualifications, rural, male, income <= £12,500/year, student, and single.

Model 3 explores the effects of the non-demographic variables. All five of these variables are statistically significant. These additional variables roughly double the R^2 and they reduce BIC by about 188 points. The effect of the number of social network sites used is particularly strong. Of those with only one SNS profile 49% have changed their privacy settings compared to 81% of those with 4 profiles. The effect of users' self-reported ability using the Internet is also strong. Ability is measured on a five-point scale ranging from "bad" to "excellent." Of those with who report only poor ability 32% have changed their privacy settings compared to 79% of those who rate their ability as excellent.[7] This finding is consistent with boyd and Hargittai, which examined the practices of 18-19 year old Facebook users (2010). They find that those ranked more highly in terms of skill tended to change their privacy settings more frequently. The coefficients of the demographic variables do not change very much. Age remains significant and strong; urban-rural and education are also significant. However, now that some non-demographic characteristics are controlled, gender becomes significant. In this model, women are more likely to have changed their privacy settings.

Discussion

Contrary to the prevailing discourse, we do not find a privacy paradox in which young people are apathetic toward online privacy. In fact, and contrary to Zuckerberg's opinion, people who check or change their privacy settings tend to be young. This is not solely a British phenomenon. We see this in multiple datasets from three countries. It is also not a completely new finding; for example, in a Pew report from 2010 (Madden & Smith, 2010), but it seems to have been overlooked in the rhetoric surrounding youth and privacy.

[7] These are marginal effects, holding all other variables at their means.

We noted in the literature review that two authors had found no age effect (Taddicken, 2013; Hoofnagle et al., 2010). It is important to consider how these results can be reconciled with our finding of a strong age effect. Taddicken's anomalous results about age could stem from several possibilities. One is that Germany is different from Britain, the US or Australia. It is tempting, however, to look at possible methodological issues: the Internet panel was matched on three observable characteristics: age, gender and German state. What is missing is any measure of social status, like income or education. In fact, in Table 1 Taddicken (2013, p 10) reports education levels for her survey that are almost 20 percentage points different from the population of German Internet users. This bias could easily account for the lack of an age effect. Hoofnagle et al. (2010) do not ask explicit questions about SNSs, so this may account for lack of an age effect in their findings.

Several alternative explanations could explain our strong age result. Young people may be more skilled at using the Internet, so they know how to change privacy settings. Boyd and Hargittai (2010) report that, among students, more highly skilled Facebook users are more likely to have changed their privacy settings. We control for skills in Table 2 and we find that they are significant but there is no change in the age effect. Age and skills are independent. Another explanation is that youth are more comfort using the Internet and thus they are more likely to investigate and change privacy settings. Again, in Table 2, when we control for comfort level it is significant but the age effect does not change. Age and comfort are independent. Yet another explanation is that young people have responded to the media attention focused on SNSs and this has made them more aware. When we control for concern with negative effects in Table 2 we find it is statistically significant but that the age effect does not change. Finally, when we control for negative experiences in Table 2 we also find it to be statistically significant but it has

no effect on age. None of these alternative explanations changes the fact that the proportion of individuals who have taken action to protect their privacy on SNSs still declines consistently by age. The age effect appears to be real.

These findings lead us to conclude that there is a new "privacy paradox". Barnes outlined the original privacy paradox in a 2006 article arguing that "adults are concerned about invasion of privacy, while teens freely give up personal information… (and) this occurs because often teens are not aware of the public nature of the Internet." While this may have been true in 2006, this is no longer the case in 2013. Young people are much more likely than older people to have taken action to protect their privacy on SNSs.

We suggest that these findings may be a result of the conscious choices of the individuals who use SNSs, rather than a result of a lack of skill, a lack of understanding of privacy issues or other similar variables. This perspective finds some support in the previous literature, Taddicken (2013) explains that those who saw the social web as more important disclosed more information online and disclosed more personal facts online. Chang and Heo (2014) found that the perceived benefits of using Facebook were related to disclosure of basic and sensitive (but not what they categorized as "highly sensitive") information but that the perceived risks of using Facebook were not related to information disclosure.

If information sharing on SNSs is approached from the perspective of a risk-benefit analysis, it is possible that young people view the risks and benefits of information disclosure and control online differently than older adults. For instance, based on a survey of 119 undergraduate students, Debatin, Lovejoy, Horn and Hughes (2009) found that respondents believed that the benefits of using Facebook outweighed the risks; would the same be true for older respondents?

The new privacy paradox, therefore, is not about young people over-sharing online with little understanding of the risks, but that social life is now conducted online and that SNSs do not provide users with the tools that would adequately enable them to manage their privacy in a way that is appropriate for them. Based on this perspective, a new theory of online privacy is necessary to start to explain how individual users approach the task of managing their online information.

A Sociological Theory of Privacy

We argue that privacy has its roots in broad, fundamental characteristics of social life. This extends the prior discussions of context and imagined audiences to explain how privacy originates and why it is fundamental. We argue that it is social structure that creates context: people know each other based around shared life stages, experiences and purposes. In this sense any person is the center of many social circles composed of people they know from different parts of their life.[8] We use the word "circle" because we do not wish to imply that these are self-conscious entities like a small group and we do not use the word "network" because this is related to technical issues such as network positions and the boundaries of various clusters, which are outside of the scope of this paper.

The circles of a typical individual are mostly independent and often unaware of each other. Some circles are actively growing, like local friends when we move to a new community, while others may be stable for years or decades, such as university friends. These examples imply that we often have very different relationships with each of these collections of people. We are closer to some circles than others, and closer to some people in each circle than others. Within each circle there may be strong ties and weak ties; there may be people we have known

[8] This view of social life originates with Georg Simmel, particularly his essay "The metropolis and the mental life" (Levine, 1971).

for decades or brand new acquaintances. Offline these circles generally do not conflict because different parts of our lives are not usually exposed to each other, although some circles overlap and some people may be part of multiple circles.

Information that is well-known and freely available in one circle (say a family) could be embarrassing or damaging if it were to become known in another setting (such as an employer). For example, individuals who have said their privacy has been violated are most likely to blame their family and friends for revealing information about them – not government or business (Dutton & Meadow, 1987). For instance, information about health, medications or pregnancy may be shared within a family but not with work colleagues or employers. Incidents from a vacation with friends may not be shared with professional colleagues. Different circles have different norms for what is acceptable and non-acceptable behavior and thus for what is made public and what is kept private. They also have different norms for what is expected to be disclosed and what is thought to be private. For example, certain opinions about one's job or boss that are kept to one's self in the office but may be expected to be shared later at the bar. Privacy, then, depends on the circle, the social context out of which the circle arises and its normative expectations. What is or should be private cannot be judged by a single standard; instead it is highly dependent on the social context and social networking sites need to provide users with the ability to manage their privacy in a way that meet these complex needs. This is the personal (or interpersonal) aspect of privacy.

Privacy is further complicated because of its relationship to different institutional domains, such as privacy with respect to corporations and to governments. Corporations make googling job candidates and examining their social network websites a common practice. A 2013 survey of more than 2000 hiring managers and human resource professionals found that 39

percent use SNSs to research job candidates and that of those who researched candidates online 43 percent found information that caused them not to hire a candidate (CareerBuilder, 2013). We can expect social media to be routinely monitored by employers. People who represent themselves in ways that could have a negative impact on employers may not be hired or may be terminated; the Justine Sacco example, described earlier, is a case in point (Bercovici 2013; Southall 2013). In one sense corporations could be seen as just another circle. However, this circle is closely monitored and violations of the norms of this circle could have financial and employment consequences.

Government is another institutional domain in which privacy is a key issue tied to civil liberties. Concern over government access to personal information has been central to the US Supreme Court deriving a right to privacy on the basis of the First and Fourth Amendment to the US Constitution. Government surveillance and access to personal information does not require electronic media or the Internet, but new media enable personal information to be collected more easily and in vastly larger quantities. Furthermore, different information is easily collected: information on who you communicate with and how often is available from easily stored and analyzed phone and email records without necessarily inspecting the actual content of the phone call or the email. From one perspective, governments are yet another circle with the norms defined by laws, but the power and resources wielded by governments really puts them in a different category than any other circle. Government privacy issues are a different in kind from other privacy concerns.

Privacy is uncertain in part because different social circles have different norms. This is consistent with Nissenbaum's focus on contextual integrity when considering legal aspects of privacy (2011). From this perspective privacy is a special kind of social norm. Violations to privacy

can arise because of deviations from the norms of a particular social circle, but also as a result of a difference of norms across multiple social circles. In this sense privacy is a sort of meta-norm that arises between groups rather than within groups. It provides a way to smooth out some of the inevitable conflicts of the varied contexts of modern social life.

If we apply this theory to young people it predicts that they would be more concerned about privacy than their elders. At a lifestage when they are leaving their families of origin and establishing their own identities, it is often the case that young people will be doing activities in one circle (e.g. friends) that they do not want known in other circles (e.g. potential employers or parents) leading them to be more concerned with privacy issues. Further, children and adolescents are likely to engage in a very limited number of social circles (for example family, friends, school), but as an individual enters the work force, starts to pay taxes, and develops friendships and romantic relationships farther away from the home, their number of social circles increases (e.g. work, government, relationships in new geographic locations) increasing the potential for conflicting privacy norms.[9] For instance, in a survey of undergraduate students, Peluchette and Karl found that 20 percent of respondents would not be comfortable with current or perspective employers seeing their Facebook profile (2008). This suggests a reason why young people with rapidly expanding social circles could be more sensitive to privacy issues than their elders.

This theory of privacy as a social construct relative to the norms of a particular circle has several implications for research. First, issues of privacy can extend beyond legal definitions of

[9] The fact that young people may join multiple new circles in a short time compounds the possibility of privacy violations due to inexperience or misunderstanding of the unfamiliar norms of the circles. It could be that the anecdotes we hear are only about youths who make mistakes and that the majority of young people are successfully navigating the contradictory norms of multiple circles with due attention to their privacy.

privacy and data protection, and have relevance within and between any specific social circles. Since norms vary from circle to circle, separate circles could be studied separately. In particular, government privacy issues are formal and legal issues that are distinct from the social norms that govern more personal social circles. They need to be studied separately. However, we should remember that an individual's perception of privacy online is a mixture of their perspectives across all social circles, ranging from government and corporate to one's individual social circles.

This leads to some issues concerning research sites. One point of the theory of circles is that privacy is related to conflicting norms of different circles from which social life is constructed. SNSs are a valuable research site because of their tendency to collapse these circles, which may heighten privacy concerns. However, other research sites could include places where conflicting circles are not collapsed, including friends or neighbors. This would probably require key informant interviews or ethnographic methods. Privacy with respect to corporations or government is a separate issue. As we write this in early January 2014 the theft of 4.6M SnapChat user accounts was just announced. What makes this particularly serious is that it includes both usernames and matched phone numbers (Blue 2014), making it much easier to personally identify people. The database may be sold to spam and phishing operations. The question is what are the consequences for the people whose personal details were stolen? Are they more serious than just additional spam? We really don't know much about the relationship between theft of usernames and financial loss, personal embarrassment, lost productivity or other potential problems. We don't know what the actual harm is. This would be a great research topic.

Privacy may still be a strong social norm, but is often not in the interest of SNSs providers to cater to the differentiated nature of the norm. Instead, companies such as Facebook stand to

gain commercial benefit from the use of personal data uploaded on these sites. The real paradox is that these sites have become so embedded in the social lives of users that to maintain their social lives they must disclose information on them despite the fact that there is a significant privacy risk in disclosing this information and that these sites do not provide adequate privacy controls to enable users to make them meet their diverse privacy needs.

REFERENCES

Altman, I. (1975). The environment and social behavior: privacy, personal space, territory, crowding. Brooks/Cole Pub. Co.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday,11(9). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394

Bercovici, J. (2013, 23 Dec.). Justine Sacco And The Self-Inflicted Perils Of Twitter. Forbes. Retrieved January 8, 2014, from http://www.forbes.com/sites/jeffbercovici/2013/12/23/justine-sacco-and-the-self-inflicted-perils-of-twitter/

Blank, G. (2013). Who Creates Content? Information, Communication & Society, 16(4), 590–612. doi:10.1080/1369118X.2013.777758

Blank, G., & Dutton, W. H. (2012). Age and Trust in the Internet: The Centrality of Experience and Attitudes Toward Technology in Britain. Social Science Computer Review, 30(2), 135–151. doi:10.1177/0894439310396186

Blank, G., & Reisdorf, B. C. (2012). The Participatory Web. Information, Communication & Society, 15(4), 537–554. doi:10.1080/1369118X.2012.665935

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? First Monday, 15(8). Retrieved from http://journals.uic.edu/ojs/index.php/fm/article/view/3086

Chang, C.-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. Computers in Human Behavior, 30, 79–86. doi:10.1016/j.chb.2013.07.059

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? CyberPsychology & Behavior, 12(3), 341–345. doi:10.1089/cpb.2008.0226

Cohen, J., & Balz, D. (2013). Poll: Privacy concerns rise after NSA leaks. Washington Post. Retrieved December 16, 2013, from http://articles.washingtonpost.com/2013-07-23/politics/40862490_1_edward-snowden-nsa-programs-privacy

Constine, J. (2013, July 24). Facebook's Q2: Monthly Users Up 21% YOY To 1.15B, Dailies Up 27% To 699M, Mobile Monthlies Up 51% To 819M. TechCrunch. Retrieved December 16, 2013, from http://techcrunch.com/2013/07/24/facebook-growth-2/

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication, 15(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Downey, M. (2011, October 10). Court rules against Ashley Payne in Facebook case. But more to come. Atlanta Journal Constitution: Get Schooled Blog. Retrieved from http://blogs.ajc.com/get-schooled-blog/2011/10/10/court-rules-against-ashley-payne-in-facebook-case/

Dutton, W. H., & Meadow, R. G. (1987). A tolerance for surveillance: American public opinion concerning privacy and civil liberties. In K. B. Levitan (Ed.) Government infrastructures. Connecticut: Greenwood Press.

Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology. Information, Communication & Society, 9(4), 433–451.

Goffman. (1959). The presentation of the self. Harmondsworth: Penguin.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71–80).

Retrieved from http://dl.acm.org/citation.cfm?id=1102214

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? (SSRN Scholarly Paper No. ID 1589864). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1589864

Johnson, B., & Vegas, L. (2010, January 11). Privacy no longer a social norm, says Facebook founder. The Guardian. Retrieved 8 Jan, 2014 from http://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Levine, D. (1971). (Ed.) On Individuality and Social Forms. Chicago: University of Chicago Press.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication, 14(1), 79–100.

Liu, C., Ang, R. P., & Lwin, M. O. (2013). Cognitive, personality, and social factors associated with adolescents' online personal information disclosure. Journal of Adolescence, 36(4), 629–638. doi:10.1016/j.adolescence.2013.03.016

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference (pp. 61–70). Retrieved from http://dl.acm.org/citation.cfm?id=2068823

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media & Society, 10(3), 393–411.

Madden, M., & Smith, A. (2010). Reputation management and social media. PEW Research Center. Retrieved from http://ictlogy.net/bibciter/reports/projects.php?idp=1650

Martin, J. (2003). What is Field Theory? American Journal of Sociology. 109(1): 1-49.

Marwick, A. E., Murgia-Diaz, D., & Palfrey, J. G. (2010). Youth, Privacy and Reputation (Literature Review) (SSRN Scholarly Paper No. ID 1588163). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1588163

Marwick, A. E., & Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media & Society, 13(1), 114–133. doi:10.1177/1461444810365313

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15–29. doi:10.1002/dir.20009

Nissenbaum, H. (2009). Privacy in context: technology, policy, and the integrity of social life. Stanford: Stanford UP.

Nissenbaum, H. (2011). A contextual approach to privacy online. Daedalus. 140(4): 32-48.Nussbaum, E. (2007). Say everything. New York Magazine, 12, 24–29.

O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. Social Science Computer Review, 19(1), 17–31. doi:10.1177/089443930101900103

Peluchette, J., & Karl, K. (2008). Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content. CyberPsychology & Behavior, 11(1), 95–97. doi:10.1089/cpb.2007.9927

Rainie, L., Kiesler, S., Kang, R., & Madden, H. (2013). Anonymity, Privacy, and Security Online. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_AnonymityOnline_09051

3.pdf
Rainie, L. & Wellman, B. (2012). Networked: the new social operating system. Cambridge, Mass.: MIT press.Rule, J. (2007). Privacy in peril. Oxford: Oxford UP.
Searle, J. (1995). The construction of social reality. London: Allen Lane.
Southhall, A. (2013, December 20). A Twitter message about AIDS, followed by a firing and an apology. The New York Times. Retrieved from: http://thelede.blogs.nytimes.com/2013/12/20/a-twitter-message-about-aids-africa-and-race/?_r=0
Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. The Information Society, 18(1), 21–32. doi:10.1080/01972240252818207
Taddicken, M. (2013). The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure1. Journal of Computer-Mediated Communication, n/a–n/a. doi:10.1111/jcc4.12052
Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust insights from a national survey. New Media & Society, 9(2), 300–318. doi:10.1177/1461444807072219
Walzer, M. (1983). Spheres of justice: a defense of pluralism and equality. New York: Basic Books.
Warren, S. & Brandeis, L. (1980). Right to Privacy. Harvard Law Review. 4, 193.