Contextualised Concerns: The Online Privacy Attitudes of Young Adults

Michael Dowd

▶ **To cite this version:**

Michael Dowd. Contextualised Concerns: The Online Privacy Attitudes of Young Adults. 6th International Summer School (ISS), Aug 2010, Helsingborg, Sweden. pp.78-89, 10.1007/978-3-642-20769-3_7 . hal-01559464

HAL Id: hal-01559464
https://inria.hal.science/hal-01559464

Submitted on 10 Jul 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Contextualised Concerns: The Online Privacy Attitudes of Young Adults

Michael Dowd[1]

[1] School of ESPaCH, The University of Salford, Crescent House, Salford, Greater Manchester, M5 4WT.
m.s.dowd@edu.salford.ac.uk

Abstract. Existing research into online privacy attitudes, whilst useful, remains insufficient. This paper begins by outlining the shortcomings of this existing research before offering a fresh approach which is inspired by Solove's notion of "situated and dynamic" privacy. With reference to ongoing PhD research it is argued that the generation of rich, situated data can help us to understand privacy attitudes in context. In this research semi-structured interviews are being used in order to grasp how young adults understand, manage, and negotiate their privacy across online settings. The paper concludes with a call for further qualitative research into online privacy attitudes and suggests focusing on more niche online settings than Facebook.

Keywords: Online privacy. Young adults. Qualitative.

1 Introduction

As technological advancements are made, new means of both violating and protecting privacy may emerge and this is why technological developments are often met with concerns and questions relating to privacy. Indeed the most widely cited text in privacy literature, Warren and Brandeis' landmark 1890 publication: "The Right to Privacy" [1], was concerned with the "recent inventions" of instantaneous photographs and advanced printing technologies, which were described as threatening to: "…make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." [1]. It should come as little surprise then that the rapid evolution of the internet has been accompanied by increasing interest in its impact on privacy, as is illustrated both by the current focus of media attention on the topic [2, 3, 4] and also the growing body of academic research into a wide range of issues relating to online privacy.

The existing research into online privacy emanates from a broad range of disciplines including law, computer science, business, media and various others. It is important for any work in this area to explicate its disciplinary background because research from these diverse disciplines of course focuses on varying aspects of online privacy e.g. computer scientists tend to be concerned with the technical means of protecting privacy online, whilst business researchers are usually interested in the difficulties online privacy concerns can pose for e-marketing. This paper is written

from a sociological perspective and is concerned with people's attitudes, understandings, behaviours and concerns relating to online privacy. There is a useful body of existing research into online privacy attitudes but, as will be explained, it remains insufficient and so a fresh research approach will be offered here

This paper will present ongoing PhD research into the online privacy attitudes of young adults in support of the view that context is vitally important in understanding privacy attitudes. It will be shown that because of this it can be very fruitful for researchers to take an inductive research approach, generating situated data which can help us to understand privacy attitudes in particular contexts. It will be argued that generating data of this nature, and so offering insights beyond those offered by previous survey research, is the real value of social science in researching online privacy.

In order to achieve these aims the paper will be structured in the following way: firstly, the existing online privacy literature which has informed this research will be summarised and its influence clarified; secondly, the research methods being used here will be described and the rationale for their selection justified; and thirdly, interim findings from the PhD research will be cautiously presented in order to demonstrate both the significance of the research, and also the nature of the data being generated.

2 Existing Research

The existing literature relating to online privacy attitudes can be divided largely into two distinct categories with contrasting research approaches. Firstly, there is a significant body of quantitative, survey based research which comes generally from a business and marketing perspective. In the past this research had tended to focus on issues of consumer privacy [5, 6, 7, 8, 9] and so was concerned with commercial, rather than social, activities, the "instrumental", rather than the "expressive", internet [10]. This trend, however, has faded away in recent years with the publication of quantitative research into social networking sites [11]. Secondly, there is a growing amount of relevant qualitative research exploring the use of social networking sites. This research has developed in response to the rapid growth in popularity of such sites [12] and, whilst not always focused specifically on privacy, it does make important contributions to understanding the online privacy attitudes of social networking site users. Survey questionnaires have been by far the most popular method used for researching online privacy attitudes and so we will begin by summarising the key survey findings which have informed this research.

2.1 Survey Research

There are two prominent themes which have emerged from the existing survey literature and inform the PhD research presented here: the "privacy paradox", and "determinant factors". The "privacy paradox" is the apparent disconnect, or even contradiction, between reported privacy attitudes and actual behaviours. Surveys have

found that users, perhaps particularly young adults [13], report themselves to be very concerned about their online privacy and the flow of their personal information, yet upon examining their behaviour it seems they freely share personal information and either do not engage, or do not engage effectively, with privacy settings on social networking sites [14]. The "privacy paradox" has been evident in surveys of both social [13, 14] and commercial [15] aspects of internet use. A number of possible explanations for the "privacy paradox" have been suggested but none have been widely accepted. Stenger and Coutant have contended that users may indeed be concerned about their online privacy but lack the technical skills and understanding required to protect it [16]. Albrechtslund has outlined the "moral panic" perspective: that users actually have a complete lack of interest in personal privacy [17]. It has also been suggested that perhaps "optimistic bias" is at play, whereby users are concerned about privacy on a societal level but do not consider themselves to be vulnerable and so do not feel the need to actively protect their privacy [18].

"Determinant factors" are demographic variables which have been found to apparently influence online privacy attitudes. Survey research has identified a number of apparent "determinant factors" including: gender, age and level of education. Gender is perhaps the most prominent of these as women have repeatedly and consistently been found to be more concerned about their online privacy than men [6, 19, 20, 21, 22, 23]. These gendered findings have also been supported by studies focused on adolescents [7, 24]. Age too has been repeatedly identified as a significant factor, with older people found to be generally more concerned about their online privacy than younger people [5, 9, 20], although it is important to recognise that, despite these apparent patterns, levels of privacy concern vary considerably within age cohorts as well as across them [25]. Numerous studies have found that higher levels of education correspond with higher levels of online privacy concern [8, 26] and this is supported by research which has found that those with higher levels of education are more likely to adopt privacy protective behaviours [9].

The robustness of these findings has been demonstrated by the consistency with which they have been replicated; however there remains a need to further explore these "determinant factors" in order to understand how and why they have an apparent influence. This is particularly true in the case of gender because, despite the consistent survey findings, there has been no sustained exploration of why women may be more concerned about their online privacy than men. The explanations suggested in the literature have merely been weakly extrapolated from research in other areas. For instance, Moscardelli and Divine [7] have argued that women are more concerned about their online privacy than men because they have a greater fear of danger citing research into the fear of crime. Garbarino and Strahilevitz [6] have argued that women are more concerned because they are more risk averse generally, citing research from a variety of other domains to support this contention. These explanations do not have any empirical link to the research conducted and are completely unsatisfactory.

What is problematic about using survey research to further explore the "privacy paradox" and "determinant factors" is that the data generated is abstract and not rooted in the lived experiences of the research participants. Quantitative research is useful for identifying patterns but in order to insightfully explore these patterns, to understand how and why "determinant factors" such as gender might have an

influence on privacy attitudes, and to better grasp the "privacy paradox", we contend that a qualitative approach is required. By adopting a qualitative approach the research can be inductive: a weakness of this existing body of research is its 'top-down' approach, relying on predetermined definitions of privacy built into precoded surveys. This denies participants the opportunity to express their own understandings of privacy and so ignores individuals' ability to make, modify and define privacy in their own terms, in different ways across contexts. By working inductively, understandings can be allowed to emerge through the generation of situated, contextualised data so that credible explanations, rooted in the lived experiences of participants, can be offered.

2.2 Qualitative Research

The emerging body of qualitative research into social networking sites makes use of ethnographic methods [27, 28, 29, 30, 31] and, although the specific research focus is not necessarily on privacy issues, the rich and contextualised data generated in these studies offers valuable insights into how users understand and manage their privacy in these online spaces.

Perhaps the central finding of the existing qualitative literature is that for young people online: "…"privacy" is not a singular variable" [25], instead, different types of information are considered more or less private depending on who may have access to that information [30]. For instance, individuals may be content to share certain information with their friends but not with their parents, with potential romantic partners but not with employers and so on. The work of both Livingstone [29, 30] and boyd [27, 32] makes clear that online settings, such as social networking sites, are not conceptualised by young people as straightforwardly "public" or "private" in a binary way, but instead distinctions are made based upon their 'imagined audience' [27] and the affordances of the particular online setting [30]. What "privacy" means and what is "private" online is context dependent and so understandings and negotiations of privacy can vary across online settings. These findings demonstrate the need for research into online privacy attitudes to generate data which is situated rather than abstract because privacy attitudes are contextual.

These ethnographic studies have also illuminated a variety of the ways in which users manage their privacy in these online spaces. boyd describes a variety of privacy protective behaviours which users sometimes adopt in order to retain control of who has access to their social networking profiles, in an attempt to manage 'social convergence' [32]: falsifying identifying information such as age and location; engaging with privacy settings; and creating "mirror profiles" for instance [27]. More recent research into social networking sites has uncovered further means of managing privacy in these settings such as "wall cleaning" and creating aliases [28]. The point here is that the nature of the data generated by these qualitative studies enables researchers to develop more granular and sophisticated understandings of how privacy is conceptualised and managed by users in the social networking sites studied.

The shortcoming of the existing qualitative research into social networking sites is that thus far it has remained focused on specific online activities and sites as chosen by the researcher, largely Facebook. This means that the ways in which

understandings of privacy may alter, or remain constant, across online settings has not been explored and also that more niche online settings are being neglected. Nonetheless, the illuminating findings of this body of qualitative research and the nature of the data generated have, to some extent, inspired the methods employed in the PhD research presented here.

3 Conceptualising Privacy

Research into privacy attitudes is often presented with a lengthy discussion of the specific privacy definition being utilised in that particular paper. This research, however, does not rely on any predetermined, overarching conception of privacy but instead takes an approach which builds on the work of Solove [33] who proposed attempting to understand privacy contextually rather than in abstract.

Privacy is both historically and culturally contingent [34], and has been recognised as being an especially 'elastic' concept [35], as is apparent from the vast number of ways in which it has been conceptualised. Solove has argued that the bewildering array of existing privacy conceptions can be dealt with in six categories: the right to be let alone; limited access to the self; secrecy; control over personal information; personhood; and intimacy [33]. These categories are not mutually exclusive, as there is overlap between conceptions, but Solove uses them as a means of critically examining the overall discourse on conceptualising privacy. Solove concludes that existing conceptions, whilst illuminating in relation to certain aspects of privacy, are either too narrow or too broad due to their attempts to isolate the "core" characteristics, or abstract "essence" of privacy [33].

Solove advocates a new and pragmatic approach to conceptualising privacy inspired by Wittgenstein's notion of 'family resemblances'. Solove contends that it would be more useful to attempt to understand privacy as an aspect of everyday practices, by focusing on specific privacy problems, rather than attempting to isolate the "core" characteristics of privacy in order to understand it as an abstract, overarching concept. In doing this, privacy can be conceptualised: *"…from the bottom up rather than the top down, from particular contexts rather than in the abstract"* [33], so recognising the: *"…contextual and dynamic nature of privacy"* [33]. This conceptual approach is consistent with our contention that the data generated by research into privacy attitudes must be situated rather than abstract and underpins the methodological decisions outlined in the following section.

4 Method

4.1 Research Sample

The decision to focus on the online privacy attitudes of young adults was made for a number of reasons. Firstly, online privacy is considered to be an especially important issue for young people as they will be: *"…the first to experience the aggregated effect of living a digital mediated life."* [25]. Secondly, today's young adults are widely recognised as being part of the first generation to grow up immersed in digital technology [36, 37, 38] and so may be expected to have online experiences distinct from other demographic groups. Thirdly, much of the existing research into online privacy is focused on children [29, 30, 39] and is often motivated by the public's desire to protect the young and 'vulnerable' [39]. This research aims to recognise its participants not as "youth", "children" or "adolescents" in need of protection, but as young adults, responsible for themselves both online and offline.

"Young adults" have been defined as those born between 1990 and 1994 because the formative years of these people have coincided with the widespread integration of online communication and social media into everyday life: these young adults would have been aged between 5 and 9 when the instant messaging service "MSN" was launched in 1999; and between 8 and 12 when Friendster and MySpace heralded the arrival of mainstream social networking sites in 2002 [12]. In an English context this means that even before these people began studying at secondary school, aged 11, instant messaging had become everyday and widespread [40], with social networking sites not far behind. The experiences of these young adults then may be distinct even from those only slightly older.

The sampling is purposive: participants are being recruited in an attempt to access a diversity of experience and attitudes [41]. Sampling has been informed by the existing literature which suggests gender and levels of education influence online privacy attitudes. For this reason, both men and women from a variety of educational backgrounds are being recruited e.g. college students; university students; vocational apprentices; those in employment; those not in education, employment or training. An aim underpinning the work is to explore understandings of privacy across online settings, including those which have previously been under researched, and this is why participants are being recruited from diverse online settings such as Last.fm and Foursquare. Offline recruitment of research participants has taken place via contacts in educational institutions and community groups.

4.2 Research Method

Inspired by the rich, insightful data generated in ethnographic studies of social networking sites [27, 28] this research is using a qualitative approach to explore how young adults understand, manage and negotiate their privacy online. This approach is

suitable because the interest is in understanding the participants, their practices, and attitudes rather than in measuring or quantifying them [42]. Adopting a qualitative approach also allows us to work inductively: rather than limiting the research by imposing predefined, overarching definitions of privacy we instead allow understandings to emerge from the participants' own accounts. This enables us to conceptualise privacy contextually, as Solove has argued in favour of.

Semi-structured interviews are being conducted in order to generate situated and contextualised data: rather than asking all participants the same questions, participants are deliberately enabled to help shape discussions so ensuring that interviews focus on activities and issues which are familiar and relevant to them. This means that we do not limit the online settings which can be discussed: we focus on whichever online activities are most important to the participant. In exploring a variety of online settings the aim is to be able to make cross-contextual comparisons. This is important because as Jennifer Mason, a leading authority on qualitative research, has argued:

> *"…instead of asking abstract questions, or taking a 'one-size-fits-all' structured approach, you may want to give maximum opportunity for the construction of contextual knowledge by focusing on relevant specifics in each interview…The point really is that if what you are interested in, ontologically and epistemologically speaking, is for example a social process which operates situationally, then you will need to ask situational rather than abstract questions."* [43]

An interview guide is composed prior to interviews but its structure is not rigid: interviews are interpersonal events [44] in which both the interviewer and interviewee are active, co-constructing knowledge [41], and so each interview is inevitably and desirably different. Field notes are made after each interview noting both theoretical and methodological reflections. These field notes are later read in conjunction with the interview transcriptions in order to retain as much of the interview context as possible when coding and analysing the data. The environments in which interviews are conducted vary but it is always ensured that a laptop with internet access is available so that participants are able to illustrate points with online examples if they wish to do so.

At this point interviews have been conducted with 15 participants. Interviews with further participants are currently being scheduled with recruitment continuing both online and offline. There are also plans for follow up interviews with some of the existing participants in order to further pursue specific issues raised in their initial interviews.

5 Interim Findings

It must be stressed that the findings cautiously presented here are only preliminary: research is continuing and data analysis is iterative and ongoing. It is intended that these preliminary findings begin to demonstrate the value of taking an inductive

approach and generating rich, situated data when researching online privacy attitudes. The names of all participants are pseudonyms for reasons of confidentiality.

A broad range of online activities have been discussed in the interviews conducted so far, including: social networking, instant messaging, online gaming, blogging, online shopping, online banking, file sharing, and participation in interest driven online communities. The specific online settings which have been discussed in-depth have so far included: Last.fm, Facebook, MySpace, Bebo, Chat Roulette, "MSN", Mousebreaker, Amazon, eBay, YouTube, various dating websites and a number of chat forums.

Initial findings have indicated that all participants so far consider themselves to be techno-savvy internet users who are confident in their own abilities to manage their privacy online. Often participants have explicitly linked this confidence to technical skills, for example 'Frank' (Gender: male. Age: 17. Occupation: toolmaker) explained that: *"I got an 'A' in ICT so I know most stuff about computers and the internet"*. Of course, how well placed this self-confidence actually is remains open to question. Related to this self-confidence has been an advocacy for personal responsibility in managing privacy online: often breaches of privacy, and general negative online experiences, have been characterised as being at least partially the fault of the victim. Breaches of online privacy have been described as resulting from the victim's own reckless behaviour, immaturity or lack of technical knowledge, as 'Luke' (Gender: male. Age: 17. Occupation: apprentice maintenance technician) phrased it: *"It's just what you get yourself into"*.

The most prominent concerns expressed have been related to being deceived online, essentially the concern being that: "People online are not who they present themselves to be". Interestingly though this has not been in relation to e-commerce: concerns that online vendors are not reputable or genuine for instance, but instead it has been on a more social level. The kinds of deception which concern participants occur not during online transactions but through online interactions, whether that be via instant messaging, social networking sites or any other form of online communication. There has been a perceived distinction between being deceived by strangers, and being deceived by known parties. Being deceived by strangers has been associated with a physical threat from the "paedos", "creeps" and "weirdoes" ubiquitous in media reports [45, 46]. Whilst being deceived by known parties has been associated with the emotional threat of being embarrassed or humiliated, be it playfully by friends or maliciously by former partners seeking revenge for instance. Some participants explained that they were wary of deception as they themselves had deceived people online. For example, 'Kirsten' (Gender: female. Age: 16. Occupation: engineering student) explained how she had duped a female friend into believing an enamoured male had made contact with her: *"I said, 'This lad fancies you', so I made an email address"*.

Participants have also recognised 'identity theft' as a concern, but not in the sense of financial fraud as the term is commonly used. Instead, the participants have expressed concerns about being impersonated online, perhaps via a convincing social networking profile or instant messaging account, and having their social identity stolen and, subsequently, their reputation damaged. A number of participants explained that this was the main reason they engaged with the privacy settings on

social networking sites: to ensure that only those they trusted had access to photographs which could be used to convincingly impersonate them.

Some intriguing gender issues have also started to emerge. Male participants have expressed great enthusiasm for approaching "new girls" online, 'Frank' for instance explained that: *"Lads, I know for definite, go on with their mates to Facebook profiles and they go through their friends. If they see a good looking girl they're obviously going to add them and try to get to know them and see if they get anywhere, if you know what I mean…I mean I've done it before."* In stark contrast, female participants have consistently complained of the irritation of being approached by unfamiliar men. For example, 'Julie' (Gender: female. Age: 16. Occupation: engineering student) explained how she had grown tired of being approached by men through Bebo and so decided to move on to Facebook, although this migration from one social networking site to another did not actually solve the problem: *"Ah, all the men and stuff adding me all the time [laughs]…and in the end I got sick of it that much I just deleted my account…I get it sometimes on Facebook"*. It has also been interesting to note the widespread use of gender stereotypes in perceptions of other internet users with older men frequently cast as "dirty old men" and female users widely considered vulnerable targets.

Other themes which have emerged and which will be explored further as the research progresses include interesting perceptions of age and the media. Participants commonly expressed concern for the privacy of younger users and also voiced the view that older people may lack the technical knowledge to understand online activities and interactions. Participants have inconsistently criticised media portrayals of privacy online and yet also cited the media in support of their own opinions. It could be interesting to explore further how participants connect media reports with their own attitudes, experiences and practices.

5.1 Significance of Findings

Whilst these findings are, as previously stressed, only preliminary they do begin to demonstrate the usefulness of the research approach adopted and the nature of the data being generated. By working inductively, understandings are allowed to emerge from participants' own accounts and this can lead to the revelation of previously hidden meanings. In this case, a fresh perspective was gained on the taken for granted term "identity theft". "Identity theft" commonly refers to a form of financial fraud but for the participants in this research the term had a quite different meaning related to their social identity. This insight could not have been gained from, for instance, a survey which posed the question: "How concerned are you about identity theft?" This potential for revealing previously hidden meanings and understandings is a key advantage of working inductively.

Issues of online privacy are embedded in everyday life and so it is important to try and understand where these issues fit into the lives of the participants. This is why semi-structured interviews are useful: they enable us to focus on "relevant specifics" [43] in each interview in order to generate rich and contextualised data. The short data extracts presented here should have imparted a small flavour of the data

and briefly illustrated its richness. The importance of data being rich and contextualised is that theories generated from such data will be rooted in the lived experiences of the participants. This is a departure from previous theorising on the influence of "determinant factors" which has relied on abstract data and, at times, weak extrapolation [6, 7]. The fact that previous research has consistently identified women as more concerned about their online privacy than men without any sustained exploration of why this is the case means that the gender issues emerging from the data are theoretically significant.

It is significant that many of the diverse online settings discussed in interviews so far are under-researched. Websites such as Last.fm, Chat Roulette and LookBook have attracted only small amounts of interest from academic researchers despite having considerable numbers of users engaging in activities with significant privacy implications. This is, of course, partly as a result of internet research having to pursue a "moving target" [47], meaning that researchers may not always be able to keep pace with developments, but it is probably also to some extent due to the intense focus on Facebook. This indicates a need for research to focus on more diverse online settings.

6 Conclusion

This paper has emphasised the importance of context in understanding online privacy attitudes by providing an outline of ongoing PhD research and explaining its relationship with existing literature in the area. It has been contended that social scientists can make a significant contribution to research into online privacy attitudes by generating rich, situated data which can help us to understand privacy attitudes in context.

To conclude this paper it is appropriate to call for further qualitative research into online privacy attitudes. It could be especially fruitful for researchers to move their focus away from Facebook and to explore more niche online settings. The current trend of Facebook centered research is understandable, given its rapid growth in membership [48] and media attention on the sites, however, this does not justify neglecting other significant online settings. Last.fm for instance has a reported 30 million active members [49] engaging in a variety of social activities based around music. This considerable membership only seems diminutive in comparison with the phenomenon that is Facebook. If privacy concerns are influenced by the affordances and audiences of particular online settings [27, 29, 30] then settings such as Last.fm are important for research into online privacy attitudes, not only because of their substantial membership, but also because of their varying technical affordances and differing social contexts.

Acknowledgements.
This work forms part of the Visualisation and Other Methods of Expression (VOME) research project and was supported by the Technology Strategy Board; the Engineering and Physical Sciences Research Council and the Economic and Social Research Council [grant number EP/G00255/X]

References

1. Warren, S.D., Brandeis, L.D.: The Right to Privacy. Harvard Law Review. 4, 193-220 (1890)
2. Aaronovitch, D.: Online truth is more valuable than privacy. Times Online (2010), *http://www.timesonline.co.uk/tol/comment/columnists/david_aaronovitch/article7045915.ece*
3. Chakrabortty, A.: Facebook, Google and Twitter: custodians of our most intimate secrets. Guardian.co.uk (2010), *http://www.guardian.co.uk/commentisfree/2010/May/25/personal-secrets-to-internet-companies*
4. Keegan, V.: Where does privacy fit in the online video revolution? Guardian.co.uk (2010), *http://www.guardian.co.uk/technology/2010/mar/19/streaming-video-online-privacy*
5. Bellman, S., Johnson, E.J., Kobrin, S.J., Lohse, G.L.: International Differences in Information Privacy Concerns: a Global Survey of Consumers. The Information Society. 20, 313–24 (2004)
6. Garbarino, E., Strahilevitz, M.: Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. Journal of Business Research. 57, 768–775 (2004)
7. Moscardelli, D.M., Divine, R.: Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors. Family and Consumer Sciences Research Journal. 35, 232-252 (2007)
8. Milne, G.R., Gordon, M.E.: A Segmentation Study of Consumers' Attitudes Toward Direct Mail. Journal of Direct Marketing. 8, 45–52 (1994)
9. Nowak, G. J., Phelps, J.: Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs. Journal of Direct Marketing. 6, 28-39 (1992)
10. Tufekci, Z.: Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society. 28, 20-36 (2008)
11. Hoy, M. G., Milne, G.: Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. Journal of Interactive Advertising. 10, 28-45 (2010)
12. boyd, D., Ellison, N.: Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication. 13, 210-230 (2007)
13. Barnes, S.B.: A privacy paradox: Social networking in the United States. First Monday. 11, (2006), *http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1394/1312*
14. Gross, R., Acquisti, A.: Information Revelation and Privacy in Online Social Networks. In: WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71-80. ACM, New York (2005)
15. Norberg, P. A., Horne, D. R., Horne, D. A.: The privacy paradox: Personal information disclosure intentions versus behaviours. Journal of Consumer Affairs. 41, 100-126 (2007)
16. Stenger, T., Coutant, A.: How Teenagers Deal with their Privacy on Social Network Sites? Results from a National Survey in France. In: 2010 AAI Spring Symposium Series (2010)
17. Albrechtslund, A.: Online Social Networking as Participatory Surveillance. First Monday. 13 (2008), *http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949*
18. Cho, H., Lee, J.S., and Chung, S.: Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. Computers in Human Behavior. 26, 987-995 (2010)
19. Coles-Kemp, L., Lai, Y. L., Ford, M.: Privacy on the Internet: Attitudes and Behaviours. VOME (2010), *http://www.vome.org.uk/wp-content/uploads/2010/03/VOME-exploratorium-survey-summary-results.pdf*

20. Cho, H., Rivera-Sanchez, M., Lim, S.S.: A multinational study on online privacy: global concerns and local responses. New Media Society. 11, 395-416 (2009)
21. Fogel, J., Nehmad, E.: Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior. 25, 153–160 (2009)
22. O'Neil, D.: Analysis of Internet Users' Level of Online Privacy Concerns. Social Science Computer Review. 19, 17-31 (2001)
23. Sheehan, K.B.: An investigation of gender differences in online privacy concerns and resultant behaviors. Journal of Interactive Marketing. 13, 24–38 (1999)
24. Youn, S., Hall, K.: Gender and Online Privacy among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors. CyberPsychology & Behavior. 11, 763-765 (2008)
25. Marwick, A. E., Diaz, D. M., Palfrey, J.: Youth, Privacy and Reputation: Literature Review. The Berkman Center for Internet & Society at Harvard University (2010), *http://cyber.law.harvard.edu/publications*
26. Wang, P., Petrison, L.A.: Direct Marketing Activities and Personal Privacy: A Consumer Survey. Journal of Direct Marketing. 7, 7–19 (1993)
27. boyd, D.: Why Youth (Heart) Social Network Sites: The Role of Networked Publics. In: Buckingham, D. (ed.) Youth, Identity and Digital Media. MIT Press, Cambridge, MA, pp. 119–142 (2007)
28. Raynes-Goldie, K.: Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday. 15 (2010), *http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2775/2432*
29. Livingstone, S.: Mediating the public/private boundary at home. Journal of Media Practice. 6, 41-51 (2005)
30. Livingstone, S.: Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media Society. 10, 393-411 (2008)
31. West, A., Lewis, J., Currie, C.: Students' Facebook 'friends': public and private spheres. Journal of Youth Studies. 12, 615-627 (2009)
32. boyd, D.: Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. Convergence: The International Journal of Research into New Media Technologies. 14, 13-20 (2008)
33. Solove, D. J.: Conceptualizing Privacy. California Law Review. 90, 1087-1155 (2002)
34. Bezanson, R.P.: The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990. California Law Review, 80, 1133-1175 (1992)
35. Allen, A. L.: Uneasy Access: Privacy for Women in a Free Society. Rowman and Littlefield, New Jersey (1988)
36. Tapscott, D.: Growing Up Digital: The Rise of the Net Generation. McGraw-Hill, New York (1998)
37. Howe, N., Strauss, W.: Millennials Rising: The Next Great Generation. Vintage, New York (2000)
38. Prenksy, M.: Digital natives, digital immigrants. On the Horizon, 9, 1–6 (2001)
39. Byron, T.: Safer Children in a Digital World: The Report of the Byron Review. DCSF (2008), *http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf*
40. Lenhart, A., Rainie, L., Lewis, O.: Teenage Life Online: The Rise of the Instant Message Generation and the Internet's Impact on Friendships and Family Relationships (2001), *http://www.pewinternet.org/~/media//Files/Reports/2001/PIP_Teens_Report.pdf.pdf*
41. Holstein, J. A., Gubrium, J. F.: The Active Interview. Sage, Newbury Park, CA (1995)
42. Gilbert, N.: Research, Theory and Method. In: Gilbert, N. (ed.) Researching Social Life. Sage, London, pp. 21-40 (2008)
43. Mason, J.: Qualitative Researching. Sage, London (2002)
44. Kvale, S.: Interviews: An Introduction to Qualitative Interviewing. Sage, London (1996)

45. Minchin, R.: Postman jailed for child sex abuse. The Independent (2010), *http://www.independent.co.uk/news/uk/crime/postman-jailed-for-child-sex-abuse-2089104.html*
46. Savill, R.: Father frog-marches internet paedophile to police. Telegraph.co.uk (2010), *http://www.telegraph.co.uk/technology/news/8013649/Father-frog-marches-internet-paedophile-to-police.html*
47. Livingstone, S.: Critical debates in internet studies: reflections on an emerging field. LSE Research Online (2005), *http://eprints.lse.ac.uk/1011*
48. Facebook Statistics *http://www.facebook.com/press/info.php?statistics*
49. Jones, R.: Last.fm Radio Announcement. Last.fm Blog (2009), *http://blog.last.fm/2009/03/24/lastfm-radio-announcement*