Annotated Bibliography:
Digitally mediated surveillance, privacy and social network sites

February, 2011

Prepared for Cyber-surveillance in Everyday Life: An International Workshop
May 12-15, 2011
University of Toronto, Canada

Kate Raynes-Goldie
kate@theedgelab.ca
Department of Internet Studies, Curtin University/EDGELab, Ryerson University

Aims

Drawing on the existing body of primarily youth-focused research, combined with two newer studies examining adults (Brandtzæg, Lüders, & Skjetne, 2010; Lenhart, 2009), this bibliography provides an examination of user understandings of digitally mediated surveillance (DMS) and privacy practices on social network sites (SNS). Some emergent research on the activities, goals and beliefs of the companies behind SNS will also be examined. The three broad, guiding questions that will be answered are:

- What are the key works, themes and debates in the area of SNS, privacy and DMS?
- What should regulators, policy-makers and law makers know about user understandings and behaviours related to privacy and risk in light of DMS and the ubiquity of SNS?
- What should regulators, policy-makers and law makers know about the activities, goals and ideologies of the companies who make SNS?

Within these broader goals, this bibliography aims to contribute to exploring the following questions:

- How do users understand privacy and DMS on SNS? What are their attitudes towards potential risks?
- What motivates the users of social network users to participate and share information (despite concerns about risk, if any)? What are the costs and benefits?
- How do users manage their privacy? What strategies do they employ?
- What are the key properties of SNS with respect to privacy and how do they facilitate DMS?

Introduction

In both the mainstream media and academia alike, much has been written about DMS, SNS, online privacy and everyday life. There has been a particular research focus on younger users, especially North American teens. To varying degrees, much of this research focuses on a perceived change in attitudes and behaviours with respect to disclosure and privacy among youth relative to adults (Acquisti & Gross, 2006). This contrast has been called the privacy paradox (Barnes, 2006). The youth focus in SNS research likely resulted from a number of factors, including the fact that young people were essentially the early adopters of social media and thus were the first group that could be studied. However, as social media becomes ubiqtuious, so too do the risks, and potentially, the new attitudes and behaviours. As more recent studies in the emerging body of work on adults suggest, adults too face privacy threats on SNS, but more as a result of less familiarity with SNS technology (Brandtzæg et al., 2010). Along with an emerging focus on adult users comes a much needed examination of the companies behind SNS and the ideologies which drive them (Stumpel, 2010). Indeed, this sort of examination is not new (see Bigge (2006), for example), but it seems to be increasingly common. Another key research theme is the definition of privacy itself in the context of networked sociality, with many researchers proposing revisions that go beyond the public/private or privacy as 'freedom from surveillance' paradigms (Solove, 2007; Nissenbaum, 2010; Stumpel, 2010; Tufekci, 2008). Indeed, an inadequate notion of privacy in the context of SNS may be responsible for the perceived privacy paradox, or it may simply be that the landscape has drastically changed since 2006, when the concept was first conceived (Utz & Krämer, 2009). Finally, and most importantly for surveillance research, SNS can be seen as a new mode of surveillance in the form of lateral or peer surveillance. It has been argued that this mode of surveillance can be beneficial (Albrechtslund, 2008) as well as harmful (Andrejevic, 2005; Bigge, 2006).

Annotated Bibliography (in chronological order)

Palen, L., & Dourish, P. (2003). ***Unpacking "privacy" for a Networked World.*** **Proceedings from CHI 2003, Fort Lauderdale, Florida.**

Writing from an HCI perspective before the mass adoption and popularization of SNS, Palen and Dourish's paper anticipates many of the contemporary privacy issues and shows, through case studies, that many current privacy and DMS issues are not all that new. Expanding Altman's notion of privacy as a dynamic, dialectic process, they propose a model for analysing privacy issues in a networked world. Palen and Dourish argue that 'privacy is neither static nor rule-based.' Rather than simply setting rules and enforcing them, privacy is about being selective and optimizing access to the self. This important way of thinking about networked privacy is later developed by Tufekci (2008) (see below) and is echoed in different forms by later theorists. Palen and Dourish also critically identify and categorise novel challenges to privacy: spatial boundary threats; temporal boundary threats resulting from the persistence of data online; and intersections of different spaces (also known as context collision or violation of contextual norms, see Nissenbaum (2010) below). Also notable is the paper's focus on adults, rather than the focus on youth which pervades the majority of later research on networked privacy, sociality and SNS.

Contrasted with later work that uses similar models to understand youth behaviours on SNS, Palen and Dourish show that adults face similar privacy threats.

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479-497. Retrieved from http://www.surveillance-and-society.org/articles2(4)/lateral.pdf

Combining theory with contemporary examples such as Google searches, online verification services and DIY investigative tools, Andrejevic introduces the concept of 'lateral surveillance,' or peer monitoring, where individuals employ the same strategies used by police or marketers in order to gather information on the various people in their lives. He shows how fear and suspicion are employed to normalize and encourage peer-based surveillance: "In an age in which everyone is to be considered potentially suspect, all are simultaneously urged to become spies - for our own good." While Andrejevic does not explicitly make the link between SNS and lateral surveillance, Andrejevic does use the early SNS Friendster as an example (although, interestingly, he frames it as a dating site - which is technically true - rather than an SNS. This speaks to how relatively new the mass adoption of the concept of SNS is). Friendster, Andrejevic argues, uses peer referrals and connections to 'side-step the self-presentation of prospective dates' to find out the 'truth'. In essence, Friendster is peer-enabled surveillance. The notion of lateral or peer surveillance is later picked up and further developed to describe and understand activities on SNS, such as by Albrechtslund (2005) (see below) and has become an useful way of thinking about surveillance and privacy on SNS.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312

In this article, based on a classroom attitudinal survey of 65 American undergraduates, Barnes identifies the 'privacy paradox,' a concept which has framed much of the early, youth-focused privacy research on SNS. The privacy paradox is based on the perceived difference in privacy attitudes and reported privacy behaviours between adults and teens. Put simply, adults are concerned about invasion of privacy, while teens freely give up personal information. More recently, the privacy paradox has been broadened to encompass a discrepancy between privacy concerns and privacy behaviours. The sentiment regarding cavalier youth privacy attitudes and ensuing threats from online predators was reflected in the MySpace moral panic which was occurring around the same time the article was published. Overall, Barnes provides a useful summary of the 'youth do not care about privacy' thread which runs through most early SNS and privacy research and is still seen today.

Acquisti, A., & Gross, R. (2006). ***Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*****. Proceedings from Privacy Enhancing Technologies Workshop, Cambridge, UK.**

Along with Barnes (2006), Acquisti and Gross provide one of the first studies of Facebook, privacy and youth. They were also the first to identify Facebook as a privacy threat due to its large database of user information combined with its culture of of 'being yourself.' In line with Barnes (2006), they find that although most users express general concerns about privacy, they are unconcerned about their privacy on Facebook. Instead, they worry about *other* people's privacy on the site. Acquisti and Gross also found that 30% of respondents were completely unaware of the visibility of the information they post on Facebook. Historically, this study (based on data mining and surveys of 294 US college and high school communities) is also interesting because, in the context of recent research such as Utz and Krämer (2009) (see below), it shows how SNS usage and privacy attitudes have significantly changed. At the time of their research, Facebook was still called 'thefacebook,' was still a niche student-only site and had relatively few (9 million) users. Indeed Stutzman & Kramer-Duffield (2010) note that use of privacy controls have increased significantly since 2006. However, as Tufekci (2008) (see below) shows, perceived changes in privacy behaviour may also be due to a change in the definition of privacy.

Bigge, R. (2006). The cost of (anti-)social networks: Identity, agency and neo-luddites. ***First Monday*****,** ***11*****(12). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1421/1339**

Writing during the heyday of generally unreflective excitement about the revolutionary potential of the internet and 'Web 2.0,' Bigge provides one of the first academic critiques of SNS. He presents a nuanced argument for an alternative perspective on SNS that runs counter to boyd's (2006) conception that has been widely taken up by academics and mainstream commentators alike. While boyd argues that SNS are emancipatory for teens - they offer youth who are coming of age a much-needed space to play and develop their identities, a place to express themselves and build cultural knowledge - Bigge argues SNS sites are actually oppressive. They act as a form of digital enclosure where users engage in unpaid digital labour in the form of self-generated surveillance. The output of this labour is massive amounts of personal data that can be surveilled, repurposed, datamined and sold. Furthermore, Bigge argues, even if one is concerned about one's privacy or the commodification of one's identity, opting out is not an easy choice. For Bigge, "membership [has become] a necessity, rather than an option." The social costs of non-participation are essentially that one does not exist (a fact happily reported by Facebook co-founder Chris Hughes). This observation also provides a deeper conception of the reasons why, despite privacy or surveillance concerns (the privacy paradox), users still use SNS. Finally, Bigge proposes an examination of the companies behind SNS, rather than the overwhelming focus on users which is still prevalent today. Drawing on Langdon Winner's (1980) *Do Artefacts have Politics?* Bigge argues that SNS have "informational and spatial politics" and must be examined from that perspective.

Dourish, P., & Anderson, K. (2006). Collective information practice: exploring privacy and security as social and cultural phenomena. *Human-computer interaction*, *21*(3), 319-342. Retrieved from http://www.dourish.com/publications/2006/DourishAnderson-InfoPractices-HCIJ.pdf

Dourish and Anderson provide a comprehensive overview of HCI perspectives on privacy and security (in other words, understanding privacy and security in terms of how people interact with systems). They also provide an examination of the three approaches to, and their inherent drawbacks of, the models used to to think about people and privacy. These approaches are economic rationality (the most common conception), practical action and discursive practice. Dourish and Anderson argue that privacy and security must be seen as embedded in social and cultural practices, rather than simply a technical phenomenon. Furthermore, we must take into account the role of factors such as risk, danger, secrecy, trust, morality, power, identity and so on when considering privacy and security designs and behaviours. Counter to the economic rationality model which holds that privacy is a series of trade-offs, they propose an alternative way of thinking about privacy and security as a collective information practice. This model suggests that we collectively produce understandings of the ways in which information should be shared, managed or withheld. Information and privacy practices, thus, are contextual and performative, rather than static and uniform.

Solove, D. J. (2007). Privacy in an Overexposed World. In *The Future of Reputation.* Yale University Press. Retrieved from http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text/futureofreputation-ch7.pdf

Through case studies and examples from Facebook and the physical world, Solove provides a useful summary of US privacy law and its shortcomings in the age of DMS and SNS. He particularly focuses on the notion of privacy in public, loss of privacy through obscurity and the limits of the strict public/private divide. Solove concludes that American law needs to adopt more nuanced understandings of privacy that go beyond the existing public/private divide. He advocates for a definition of privacy similar to Nissenbaum's privacy in context (2010) (see below) and Altman's privacy as boundary control (as discussed in Tufecki (2008), see below and Palen and Dourish (2003), see above). He also argues that users need more control over their information (as with the European Union style privacy laws that are common in most of the world). This chapter is also useful because Solove's case studies can be used to show that many privacy concerns which are framed as novel and as a result of social networks are really not new. Rather, SNS and digital media have made them more common or more exaggerated.

Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance. *First Monday*, *13*(3). Retrieved from http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949

In this theoretically grounded paper which draws on surveillance studies and computer ethics (specifically Andrejevic's (2005) notion of lateral surveillance, see above), Albrechtslund argues that given the their characteristics (sharing of activities, preferences and beliefs to socialize) SNS are anchored in surveillance practices and as such, the activities on SNS can be seen as participatory surveillance. Participatory surveillance, he argues, comprises a mutual horizontal practices made up of "the personal information people share – profiles, activities, beliefs, whereabouts, status, preferences, etc. [it represents] a level of communication that neither has to be told, nor has to be asked for. It is just 'out there'..." Participatory surveillance is sharing, rather than a trade. Counter to the common framing of conventional and lateral surveillance as disempowering, disciplinary and controlling, Albrechtslund argues that participatory surveillance can be potentially empowering, subjectivity building and playful. Overall, Albrechtslund shows a different aspect of of surveillance (the social side), thereby providing insight into what motivates SNS use, despite privacy concerns. He argues that applying only the common panopticon-based framework to SNS use yields moral panics or anger at youth for 'oversharing,' which get in the way of actually understanding what people are doing on SNS and why. In so doing, Albrechtslund provides insight into the shortcomings of assumptions embedded in the privacy paradox.

Zimmer, M. (2008). The externalities of Search 2.0: The emerging privacy threats when the drive for the perfect search engine meets Web 2.0. *First Monday*, *13*(3), 2008. Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2136/1944

Zimmer provides a critical examination of the overlooked implications for privacy and DMS resulting from from the integration of search technology with SNS and 'Web 2.0' (now usually referred to as social media.) "Search 2.0," as Zimmer calls it, results in the loss of privacy through obscurity due to the concentration and aggregation of one's online activities. Search 2.0 enables an unprecedented level of top-down surveillance through tracking, aggregation and deep database creation. In the past, bits of personal information were spread across the web. Now, SNS facilitates (and encourages) mass self-reporting of everyday activities in exchange for convenience and social benefits. These massive databases can now easily be searched, cross referenced, and aggregated using Google. The potential real-life costs of Search 2.0 are increased disciplinary power through the repurposing of collected data by third parties such as law enforcement; and an increased ability to impose a panoptic sort on users, where they are identified, assessed and classified based on their economic value and thus their level of access to goods and services. What makes Search 2.0 even more potent, Zimmer argues, is its allure combined with its invisibility. Even though most social media requires the sharing of personal information in order to participation, the majority of users do not know they are being tracked or surveilled nor how their information is being used. The design of social media does not make the data collection obvious nor does it provide any method to opt out. The improvement of one's life thanks to social media is hard to resist, and the invisibility of the potential privacy threats inherent in their use make it easy for users to overlook. Zimmer concludes with a few suggestions on potential solutions for the problems he identifies: government regulations, industry self-regulation and a change in the design of social media.

boyd, d., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. Retrieved from http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Through a comprehensive overview of the literature on, and history of, SNS, boyd and Ellison provide a critical foundation for SNS research from a user perspective. Their literature review of the interdisciplinary scholarship covers the current issues of SNS research, including privacy in the context of context and impression management by users. boyd and Ellison also cover literature on friendship; the connection between the online and offline worlds and the privacy paradox raised by Barnes (2006). boyd and Ellison present a broad definition of SNS as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system." They also propose that researchers use the term "social network sites" rather than "social networking sites" - two terms that are often used interchangeably. The critical difference is that social network*ing* suggests that new connections are being formed whereas social network sites match what they argue is actually going on - the building and maintenance of existing contacts by users.

Beer, D. D. (2008). Social network (ing) sites… revisiting the story so far: A response to danah boyd & Nicole Ellison. *Journal of Computer-Mediated Communication*, *13*(2), 516-529.

Responding to the influential summary by boyd and Ellison's (2008) (see above) of the history and scholarship of SNS, Beer provides a critical analysis of some of the key issues in SNS research. First, he disagrees with their proposal that researchers use the term social network sites in lieu of social networking sites as the term *networking.* Beer argues that this term is too broad and means too many things, and would lose the nuance that separates sites like YouTube from Facebook. Second, he argues against what he see as their artificial segregation of online and offline life, especially with respect to social interactions and friends. With SNS in the mainstream, this distinction is unrealistic. Beer points out that we can no longer easily distinguish between online and offline nor a "Friend" (online) and "friend" (offline). With the mass adoption of SNS, they are more often than not the same person. The lack of distinction between online and offline also speaks to how online surveillance and privacy are critically intertwined with physical safety and privacy. Third, and most importantly for surveillance and privacy researchers, he argues that the focus thus far (especially that of boyd and Ellison and the research agenda they call for) has been almost exclusively on users, thereby ignoring the critical role of the structures that create and shape these sites, both literally and discursively. In line with Bigge (2006), Beer states that we must also examine the companies that make SNS, advertising strategies, software designers, third party users, and, more broadly, the role of capitalism and capitalist interests in the design of SNS. Most critically in the context of surveillance and privacy, he argues, we must examine the 'motives and agendas of those that construct these technologies in the common rhetoric of the day.'

Krishnamurthy, B., & Wills, C. E. (2008). ***Characterizing privacy in online social networks.*** **Proceedings from Proceedings of the first workshop on Online social networks.**

Combining a user study with a survey of various SNS, this conference paper provides an informative overview and systematic characterization of SNS privacy settings, defaults, and the design of general content sharing features on a number of sites, including Facebook, Twitter and MySpace. Krishnamurthy and Wills show potential privacy threats and information leakages from other users, marketers and third party application developers. The description of Facebook, especially with respect to the Networks feature, is already somewhat dated. However, this datedness of relatively recent research speaks to the speed at which Facebook's privacy settings change and the challenges it poses for policy and research. Krishnamurthy and Wills conclude that overall, privacy settings are permissive and provide more information than is functionally necessary (as in the case of Facebook applications).

Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. ***Bulletin of Science, Technology & Society*****,** ***28*****(1), 20-36.**

Tufekci provides a nuanced analysis of the privacy paradox which goes beyond the common "students say they are worried but they don’t care" and "students say they are worried but they don't know" conceptions of youth, privacy and SNS use. Most conceptions of privacy, she argues, are based on the notion of privacy as total withdrawal ('the right to be let alone'). This model does not take into account the benefits of publicity, which gives rise to the apparent privacy paradox. Thus, building a framework based on Goffman (1959) and Altman (1975), Tufekci argues that "a better understanding of this conundrum [the privacy paradox] can be achieved by recognizing that in the self-presentation context provided by these Web sites, privacy should be understood as a process of optimization between disclosure and withdrawal." Using this model to expand on Acquisti and Gross' 2006 study (see above), Tufekci conducted a study with 70 American undergraduates who were users or nonusers of Facebook and MySpace. She found that instead of being completely unconcerned about their privacy, youth know there are benefits to publicity, so they must balance privacy and disclosure. Using Tufekci's model, then, shows the privacy paradox is not a paradox at all. Tufekci also identifies the inherent privacy-threatening and DMS-enhancing properties of SNS: persistence, searchability and cross-indexability. These properties lead to audiences who are obscured to users, or who exist in the future. In other words, users do not know necessarily who will be looking at their profile, or even when.

Utz, S., & Krämer, N. (2009). The privacy paradox on social network sites revisited: the role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2). Retrieved from http://www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1

Through a short literature review and summary of three survey-based studies of European SNS users and their privacy attitudes (totalling ~450 participants), Utz and Krämer provide an updated analysis of Barnes' (2006) privacy paradox. This revisitation is necessary and timely, they argue, as much has changed since 2006. SNS have reached mass adoption; online relationships and identities are now usually anchored offline; and mainstream awareness about SNS and privacy issues has increased as a result of mainstream coverage of the issue. In response, the companies behind SNS began providing users with more granular privacy controls. Based on these changes and the evolution of SNS design and use, Utz and Krämer suggest that previous work which supports the privacy pardox should be taken as 'snapshots' rather than static and final conclusions. Indeed, Utz and Krämer's studies suggest that a number of important shifts have occurred with respect to privacy behaviours along with the broader changes with respect to SNS identified earlier: users are now actively changing their default privacy settings and their concern about privacy is influenced by social norms. If a user's friends are more private, then that user generally is as well. In some cases, increased narcissism decreases privacy protection (but not always, such as with respect to making an email address or mobile number public. Their studies also confirm Tufekci's (2008) findings (see above) that users balance the costs and benefits of disclosure and privacy. For example, the more concerned users were about reaching a large audience and leaving a positive impression, the less restrictive their privacy controls were. Utz and Krämer conclude with some useful insights on user education (especially for youth) with respect to privacy protection. Since their findings suggest that concern about privacy is directly linked to stricter privacy controls, educating users on the privacy risks will result in better privacy behaviours. This education becomes even more important since social norms and peer pressure play a role in privacy behaviours.

Lenhart, A. (2009). Adults and Social Network Websites. Retrieved from http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx

Most SNS research thus far, especially with respect to privacy and surveillance, focuses on teens and university students. In this context, this report, based on 2 surveys of 2,253 adult Americans, provides a valuable look at privacy attitudes and behaviours among adult SNS users. In the areas where age groups were compared, the report suggests that privacy attitudes among teens and adults are drastically divergent. However, younger people are still far more likely to have an SNS profile than their older counterparts. Specifically, the survey found that "most, but not all adult SNS users are privacy conscious." And while adults are generally more aware than teens of potential privacy threats on SNS from other people (such as being found or identified), the difference between the two groups is rather small. Indeed, teens were actually *more* likely than adults to believe that with enough work, a stranger could identify them from their SNS profile. The report also provides a valuable look at the uptake of SNS among adults, the use of multiple profiles, the purpose of use (social or professional) and the age-based SNS preferences.

Nissenbaum, H. (2010). ***Privacy in Context: Technology, Policy, and the Integrity of Social Life.*** **Stanford: Stanford University Press.**

In this book, Nissenbaum provides a nuanced and detailed philosophical examination of the problems of privacy in a digital age and formulates an analytical framework in the form of contextual integrity, that is, she argues, a step towards solving many contemporary privacy issues. In part one, Nissenbaum provides a useful overview of the characteristics of surveillance threats and how they pose threats to privacy. In part two, she provides a critical survey of the main legal, theoretical and policy-based approaches to privacy. The core concept of the book is contextual integrity, which is based on a definition of privacy as the contextually appropriate control of personal information about oneself. Contextual integrity, Nissenbaum argues, can be used to explain violations of privacy that, by traditional conceptions of privacy based on the usual legal definition of privacy framed by the public/private divide, are not considered violations of privacy at all. For Nissenbaum, proper privacy design respects social contexts and context-relative information norms "which prescribe the flow of personal information in a given context, are a function of the types of information in question." When these norms are ignored, it is experienced as a violation of privacy (or in Nissenbaum's terms - a violation of contextual integrity). In

Nissenbaum's contextual integrity, SNS violate privacy because they violate contextual informational norms by mixing surveillance and social life. Users share their information on Facebook in the context of socializing. They are not expecting to have the company behind Facebook surveilling them or using that information for purposes unrelated to social activities.

Stumpel, M. (2010). ***The Politics of Social Media: Facebook: Control and Resistance.*** **Master's thesis. University of Amsterdam, Amsterdam.**

In this Master's thesis, Stumpel draws on Manuel Castell's notion of reprogramming and switching to analyse Facebook's use of discursive strategies and framing to support its continual push towards increasingly open site features and privacy settings combined with the commercial exploitation of user information (such as datamining and targeted advertising) collected through Facebook's user surveillance. For example, he argues, Facebook has used a consistent strategy whereby it announces a new feature which challenges privacy norms in a novel way. Users protest, and Facebook apologizes, yet it essentially keeps things the same. In this way, Facebook continually pushes the privacy envelope, one small bit at at time. Stumpel balances this analysis with an account of the various countertactics used against Facebook by hackers and general users. Because the vast majority of SNS research focuses on users and user behaviour, Stumpel's focus on the company behind Facebook itself provides valuable insight. For example, by shedding light on Facebook's ideology of 'openness and transparency,' Stumpel provides a useful context for understanding why Facebook makes the privacy decisions it has. While this discussion of this ideology is critical, more work needs to be done to unpack the ideology and the driving factors behind it. Stumpel also provides an comprehensive historical overview of Facebook's continual privacy changes as well as its privacy blunders. He concludes that there is currently no effective means for users to resist exploitation on Facebook.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. ***First Monday*, *15***(**1-4). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2775/2432**

Based on an ethnographic study of a community in Toronto of young adults who use Facebook, Raynes-Goldie provides an overview of privacy attitudes and behaviours. She particularly focuses on the tactics users employed to maintain their privacy, such as periodically deleting wall posts or the use of aliases, as well as the ways in which users can violate the privacy of others largely resulting from design flaws on Facebook. Raynes-Goldie also makes an important distinction between two key forms of privacy in the context of SNS; institutional and social. Previously, most conceptions of privacy (especially those in a legal context) defines privacy in terms of data protection (in other words, how institutions manage and use the personal information they collect about individuals). What is equally important, yet often overlooked, Raynes-Goldie argues, is social privacy in terms of the management of the disclosure of personal information with respect to one's friends, acquaintances and family members. Social privacy is concerned with identity and context management on Facebook, rather than on controlling what the company behind Facebook does with one's information. Given this distinction, Raynes-Goldie argues that users *do* care about privacy, it is just that they care about social privacy rather than institutional privacy. Like Utz and Krämer (2009) and Tufekci (2008), Raynes-Goldie provides a resolution ofthe privacy paradox. This article highlights the need for policymakers to widen the scope of what is considered privacy, and thus what needs to be protected.

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *Journal of Human-Computer Interaction*, *26*(11-12), 1006-1030.

With the aim of advising SNS designers, this interdisciplinary study draws on sociology, information systems and psychology to examine the tension between social privacy (based on Raynes-Goldie (2010), see above) and what Brandtzæg et al. argue are the most important success factors on SNS: content sharing and sociability. The authors call this tension the 'privacy dilemma.' As privacy increases, sociality and content sharing (the reverse of this is also true). This dilemma causes a problem for designers because sociality and content sharing are core to the current design of SNS. In this way, the privacy dilemma resolves the privacy paradox (which does not account for the tradeoff between sociality and privacy), while at the same time identifying a more nuanced and contemporary research problem. The study employs a novel approach that combines in-depth interviews with Norwegian youth (390 participants) and adults (210 participants) with a usability study. Such an approach, especially with respect to the comparison of young and old users, is probably the first of its kind in SNS, privacy and surveillance studies. As the authors note, the increasing adoption of SNS by adults make such an approach necessary. Brandtzæg et al. supported Raynes-Goldie's (2010) findings that youth *do* care deeply about social privacy. Building on that finding, the authors found that even though adults believed youth to be more open and prone to privacy violations, young people were actually more aware of strategies to maintain their social privacy than their adult counterparts. One of these tactics, the authors note, is social conformity, which "occurs when an individual's actions are exposed to increased visibility or surveillance by other members of a group (e.g., "followers" on Twitter and "friends" on Facebook)." Combined with Lenhart (2010), this report suggests that the common conception of youth versus adult privacy behaviours, understandings and potential risks nuanced rather than are black and white. In some cases, adults are at a higher privacy risk than youth.

Acknowledgements

The author wishes to thank the organisers of the *Cyber-surveillance in Everyday Life: An International Workshop* for their generous support in the development of this annotated bibliography.

Additional Citations

Altman, I. (1975). *The Environment and Social Behavior: privacy, personal space, territory, crowding.* Belmont: Wadsworth Publishing Co.

boyd, d. (2006). Identity Production in a Networked Culture: Why Youth Heart MySpace. Retrieved from http://www.danah.org/papers/AAAS2006.html

Goffman, E. (1959). *The Presentation of Self in Everyday Life.* New York: Anchor Books.

Stutzman, F., & Kramer-Duffield, J. (2010). *Friends only: examining a privacy-enhancing behavior in facebook*. Proceedings from Proceedings of the 28th international conference on Human factors in computing systems.