

PRE-PRINT

Joinson, A.N., Houghton, D.J., Vasalou, A., Marder, BL. (in press, 2011). Digital Crowding: Privacy, Self-Disclosure and Technology. In S. Trepte & L. Reinecke (Eds), *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web* (pp 31-44). Springer, Heidelberg and New York.

4. Digital Crowding: Privacy, Self-Disclosure, and Technology

Adam N. Joinson, David J. Houghton, Asimina Vasalou, & Ben L. Marder
University of Bath, School of Management.

4.1. Introduction

In this chapter, we introduce and develop the concept of “digital crowding.” Traditionally, crowding has been conceptualized as excessive social contact or insufficient personal space (Altman, 1975). Under these circumstances, not only do people show signs of stress, but they also engage in a number of techniques to escape excessive social contact (Baum & Valins, 1977). For instance, studies of students in shared, crowded spaces find that they spend more time in their bedrooms than in social spaces, are more likely to seek friendships outside of the crowded area, and even sit further away from strangers in waiting rooms (Baum & Valins, 1977). We argue that while much of the discussion of privacy and technology has focused on information flow and leakage, it has ignored the interactive, interpersonal impact of new technology. In this chapter, we begin by examining the key issues raised by technology for privacy. We then discuss earlier, non-technology focused theories that cover interpersonal aspects of privacy. Finally, we examine some ways in which technology might impact on interpersonal privacy, with a specific focus on social network sites.

4.2. Privacy, Technology, and Digital Crowding

Concerns about the privacy impact of new technologies are nothing new. Back in 1996, Schatz Byford argued that, “at no time have privacy issues taken on greater significance than in recent years, as technological developments have led to the emergence of an ‘information society’ capable of gathering, storing and disseminating increasing amounts of data about individuals” (Schatz Byford, 1996, p. 1). In the UK, 11 million children’s details have become accessible to the scrutiny of 390,000 trained professions (BBC News, 2009a); workplace surveillance is an

established practice (BBC News, 2003; Joinson & Whitty, 2008); and social network sites (SNSs) are thriving on users' willingness to disclose and consume personal information (Joinson, 2008) while at the same time they provide users with mixed mechanisms for privacy protection (Bonneau & Preibusch, 2009). Recent developments to increase the personalization of website experiences also pose a problem, with customers who value informational transparency being the least likely to accept personalization and profiling (Awad & Krishnan, 2006).

We are increasingly building Internet services that elicit ever more detailed disclosure from individuals. One driver of this is the move towards more socialized use of technology. For instance, most SNSs cease to function as intended if people do not disclose information about themselves in the form of profiles, photographs, status updates, or tweets and, increasingly, their location (e.g., Burke, Marlow, & Lento, 2009). The most popular SNS, Facebook, has a strict "real name" policy, meaning that this disclosure is usually connected to a non-anonymous individual who relies only on the privacy settings of the site (and the trustworthiness of the organization behind the site) to protect their privacy. This move towards increased sharing—termed "radical transparency"—led Facebook founder Mark Zuckerberg to claim in 2010 that privacy is no longer a "social norm" (BCS, 2010). This ideological position is based on two key assumptions—firstly, that openness and transparency is a positive force in society, and secondly, that openness is generally beneficial in interpersonal relations. Facebook has 10 "principles" that outline this ideology—the first being "*people should have the freedom to share whatever information they want, in any medium and any format*" (Facebook, 2011). Other principles expound the importance of "*the freedom to access all of the information made available to them by others,*" and, "*the freedom to build trust and reputation through their identity and connections.*" However, this identity must be "real"—the terms and conditions of Facebook (Oct 2010 version) stipulate that users "*will not provide any false personal information on Facebook*" (Facebook, 2010). Indeed, Facebook already prevents users from creating usernames with "Fake" in the name, and employs algorithms to attempt to distinguish "real" from "fake" users (Breyer & Zuckerberg, 2005). This creeping transparency is not limited within Facebook—the use of Facebook Connect as an identity management system that allows users to log onto other sites using their Facebook credentials further increases the spread of personal, identifiable information across the Internet.

The privacy issues raised by SNS use are well documented (e.g., Bonneau & Preibusch, 2009; Christofides, Muise, & Desmarais, 2009). Users post personal, identifiable information on their own and other's profiles (Christofides, et al., 2009; Young & Quan-Haase, 2009). They post, share, and tag photographs of themselves and others (Binder, Howes, & Sutcliffe, 2009; Gross & Acquisti, 2005; Nov & Wattal, 2009), update their status with inappropriate information (BBC News, 2009b), boast about illegal activity (BBC News, 2010), and openly discuss their personal relationships on "walls" (a semi-public forum) (Houghton & Joinson, 2010). Such information revelation can be detrimental to the user or can

implicate others (Acquisti & Gross, 2006, 2009; Christofides, et al., 2009), and is often based on optional self-disclosure and encouraged by site settings (Acquisti & Gross, 2006; Bonneau & Preibusch, 2009; Burke, et al., 2009; Nov & Wattal, 2009).

It is not just self-disclosed information that puts users under threat but the visible communications linked to them by “friends.” This co-creation of users’ profiles is carried out through actions such as wall posts, comments, and the tagging of photos or location. Arguably these activities may be thought to pose a greater risk than disclosure by users themselves, for the reason that concerns over privacy and possible harms may not be fully internalized by other users within the decision to disseminate information (e.g., Houghton & Joinson, 2010). Protection from this can be offered through site privacy settings, which allow users control over who and what can contribute to their online image, although these are often too simple or too complex (Bonneau & Preibusch, 2009).

However, threats originate not only from users’ and their friends’ posting of information but from outside access. While a user can be careful and deliberate in what information they post, outside access can also result in privacy violations and personal harm. The use of unsecured login connections by SNSs may allow third parties easy access to account information (Gross & Acquisti, 2005). The default settings of SNSs allow profile pictures, demographic data, and network groupings to be visible to anybody with an Internet connection. The seemingly benign informational aspects that users share about their lives, such as contact information (including mobile phone numbers and e-mail addresses), hometown, sexual and political preferences, date of birth, and partner’s name, can be mined, stored, and abused (Acquisti & Gross, 2006, 2009; Acquisti & Grossklags, 2004; Christofides, et al., 2009; Govani & Pashley, 2005; Gross & Acquisti, 2005; Nov & Wattal, 2009; Tufekci, 2008; Young & Quan-Haase, 2009). This can result in phishing, information leakage, social security fraud, identity fraud, and both online and offline stalking (Acquisti & Gross, 2009; Gross & Acquisti, 2005; Hasib, 2009; Westlake, 2008).

Not all privacy threats on SNSs come from loss of *information privacy* or *control* over personal information—they may also come from excessive social contact, or *digital crowding*. We argue that the evolution of SNSs has led to a situation akin to offline crowding where inability to control interaction, in particular the boundaries between self, small intimate groups, and the public audience, leads to deleterious consequences both for the individual concerned and for the quality of social relations between people. Our argument is based on an analysis of the nature and role of self-disclosure and privacy maintenance in social interaction, and the ways in which SNSs disrupt established practices. Specifically, we argue that SNSs may create digital crowding in three main ways:

- 1) By disrupting the dynamic nature of boundary regulation as social interaction progresses, through the use of discrete privacy settings and preferences.

- 2) By providing multiple audiences, with limited or overly complicated methods to control sharing within set boundaries.
- 3) By encouraging unfettered sharing of personal information that intrudes upon other users.

In the following section, we discuss the nature of self-disclosure, its role in relationships, and its links to privacy theory.

4.3. Self-Disclosure, Relationships, and Privacy Theory

Self-disclosure has been defined as “the process of making the self known to other persons” (Jourard & Lasakow, 1958, p. 91). This results in the sharing of knowledge between pairs of individuals, individuals within groups, or between an individual and an organization (Joinson & Paine, 2007; Petronio, 2002). The notion of simply “disclosing more” must appreciate the duality of self-disclosure that can be measured along two dimensions, breadth and depth (Spiekermann, Grossklags, & Berendt, 2001). Breadth is related to the quantity of information, and depth to the quality (Spiekermann, et al., 2001). Depth can range from biographic information to deeper aspects such as revelations of trust violations or one’s sexual fantasies (Joinson & Paine, 2007). Altman & Taylor (1973) suggest a penetrative, “layered” model of disclosure, akin to an onion. The core layer contains fewer, but deeper, aspects of personality. Towards the peripheral layers of the model are an increasing number of personality aspects, although somewhat shallower. For example, being empathetic would be a core personality construct, whereas types of clothing and basic interaction with others are towards the peripheral layers (Altman & Taylor, 1973). Breadth varies along two planes, frequency and category. Category refers to the number of elements within each layer and frequency refers to their occurrence (Altman & Taylor, 1973).

Self-disclosure is critical to the development and maintenance of relationships. Uncertainty reduction theory (URT) (Berger, 1979; Berger & Calabrese, 1975) posits that greater knowledge of others is associated with greater liking, and uncertainty has been linked to relationship problems (Knobloch, 2007). In a meta-analysis of liking and self-disclosure, Collins and Miller (1994) report three distinct self-disclosure effects: 1) people who disclose are liked more, 2) people disclose more to those they like, and 3) people like those to whom they have previously disclosed. Open disclosure has consistently been related to marital satisfaction and feelings of love (e.g., Hendrick, 1981; Rubin, Hill, Peplau, & Dunkel-Schetter, 1980), and levels of disclosure from one partner to another in dating couples predicts liking (Sprecher, 1987).

Variations in the breadth and depth of self-disclosure are a form of regulation (Derlega & Chaikin, 1977) that serves on the one hand to maintain privacy and on the other hand to determine the type of relationship kept with others; by controlling disclosure, individuals manage the degree of intimacy in a relationship. To give an example, in a public space we cannot help but reveal some peripheral in-

formation, such as our clothes, gender, and approximate age. We keep other members of the public in a non-intimate relationship with ourselves by concealing deeper aspects of our lives. During the process of regulation, people (or individuals) allow themselves to be open and accessible to varying degrees. In order to manage this openness, they engage in a process of *boundary* regulation. Altman (1975) likens boundaries of interpersonal relationships to a selectively permeable cell membrane where the flow of inputs and outputs can be adjusted to reach a desired level of privacy. An important aspect of this theory is that privacy is non-monotonic and is determined as a dialectic process involving a desire for and against various interaction types. The dialectic process suggests that the achievement of privacy requires a balance of opposing forces. For example, the desire to reveal information opposes the desire to conceal information. Depending on the circumstances at a particular moment, one may choose a position on such a continuum that aids the achievement of the desired level of privacy (Altman, 1975). In the context of relationships, desired levels of privacy are partly driven by an individual's need to maintain certainty about another individual or group. Certainty allows them to develop informed judgments about others' personality orientation in order to predict their attitudes or behaviors in a variety of situations (Berger & Bradac, 1982; Berger & Calabrese, 1975). To achieve certainty requires reciprocal information disclosure between those involved while managing the boundaries of communication (Berger, 1993; Berger & Bradac, 1982).

The dialectic management of disclosure and privacy is subject to norms as individuals interact in line with the social situation they are in (Berger & Bradac, 1982). At a cocktail party, it is the social norm to interact with unknown others and begin the conversation with reciprocal peripheral information sharing, slowly moving conversation towards more central constructs (Altman & Taylor, 1973; Berger & Bradac, 1982). However, an individual that shares too much information in such an environment would be labeled a social deviant (Altman & Taylor, 1973) and suspicions would be raised as to their objectives (Berger & Bradac, 1982). For example, taking off one's clothes in a public environment is not only a social *faux pas*, but also illegal. However, change the environment to a doctor's surgery and this is in line with expected social norms (Berger & Bradac, 1982). It is not just the environment that dictates social norms and expectancies of self-disclosure, but also the nature of the relationship between the interaction partners. In the above example of the doctor's surgery, the doctor-patient relationship alongside the environment of the doctor's surgery dictates that we can take off our clothes, and it is acceptable. If one were to get naked in the doctor's surgery but in front of the receptionist, it would again become a social taboo (Berger & Bradac, 1982).

From a relational perspective, the decision to disclose information to others is subject to a series of explicit and implicit rule negotiations. Groups or individuals with whom people share become co-owners and may feel entitled to disclose the shared information further (Petronio, 2002). When discussing the state of a romantic relationship with a close friend, it can be explicitly stated, "don't tell anyone,"

or it can be expected that the friend knows this implicitly (Petronio, 2002). Therefore, alongside privacy norms that are shaped by individual characteristics (e.g., gender, culture), norms are communicated when individuals enter pre-existing boundaries (e.g., the family) or are negotiated when new boundaries are formed (Petronio, 2002).

4.4. Boundaries, SNSs, and “Digital Crowding”

We contend that a privacy threat of SNSs that has been underrepresented in literature comes from excessive self-disclosure, socialization, and social contact—what we term “digital crowding.” As discussed above, the regulation of boundaries and management of disclosure are central to maintaining interpersonal distance between people, and thus establishing different types of relationships. Just as excessive physical contact can lead to a sense of crowding, we hypothesize that excessive digital social contact via SNSs may lead to “digital crowding.”

We focus on two ways in which digital crowding—through excessive contact or sharing—can be detrimental to privacy and the quality of relationships. The first is the dangers inherent in radical transparency or unregulated openness. The second is through overlapping social spheres and users’ inability to maintain dynamic boundaries.

4.4.1. Digital Crowding and Radical Transparency

As discussed above, much social media involves disclosure in some form—whether location, identity, pictures, contact information, or more intimate aspects of one’s life. Indeed, many of the services currently popular simply do not work without disclosure—or the design of the site is such to encourage sharing and openness.

While there is ample evidence that self-disclosure is generally positive in relationships, this is not universally true. Non-disclosure, secrecy, and deceit are also key components of successful relationships (Afifi, Caughlin, & Afifi, 2007; Burgoon & Hale, 1988; Petronio, 1991), and over-disclosure can be as detrimental to relationship development as unwillingness to disclose (Altman & Taylor, 1973; Berger & Bradac, 1982). While studies of the mere exposure effect (Zajonc, 1968) consistently show that familiarity and repeated exposure to objects is associated with increased liking, there is also evidence that over-exposure leads to reduced liking (Erdelyi, 1940; Smith & Dorfman, 1975). Norton, Frost, and Ariely (2007) found that although people expected that increased knowledge of possible romantic partners would be associated with increased liking, this was rarely the case, and more often than not it was associated with reduced liking. In a similar vein, Stafford and Reske (1990) found that students in geographically distant relationships reported being more in love than those who lived in the same town. Before the radical transparency that SNSs imposed, Walther (1996) argued that it is the abil-

ity while online to manage the flow of information, and to self-present selectively, that leads to “hyperpersonal interaction.” Similarly, Petronio (1991) notes that, “*There are good reasons to balance openness with secrecy in a relationship,*” and Afifi et al. (2007) argue that, “*withholding information is sometimes benign or even useful*” (Afifi, et al., 2007, p. 78).

However, in the era of radical transparency there is little scope for secrecy. With its emphasis on sharing, lack of sharing not only leads to a reduced user experience on many web 2.0 sites, but could also be seen as anti-normative (or at least, contrary to the principles and terms and conditions of Facebook). As noted by other privacy researchers (e.g., Acquisti & Gross, 2009; DeCew, 1997), sharing does not need to be intimate to impinge on privacy—indeed, with the opportunity to collect information about others across time and locations, and to aggregate and process that data, the multitude of banalities usually seen on social media services may be more telling than the single intimate outpouring. With the advent of social media and particularly SNSs, alongside “radical transparency,” it is inevitable that we will end up knowing more about people, and also more likely that we end up disliking them because of it.

4.4.2. Digital Crowding and Overlapping Social Spheres

Self-disclosure is used in different ways in different types of relationships (e.g., between same-sex friends, romantic partners, colleagues). Typically when the most popular SNSs were launched their content was targeted at specific markets. Myspace was aimed at teenagers and music lovers, LinkedIn at professionals in high-tech industries, and Facebook at university students. However, the growth in the popularity of these sites, alongside a loosening of entry rules, has brought a widening of user demographics. To give an example, Facebook began by confining entry to people with a Harvard e-mail address, followed by a slow roll out across US campuses using the same “.edu” criteria. When opened up globally, it again began with a focus on university campuses, to be followed in 2006 by being open to all potential users. In recent years Facebook has become popular not only with older generations, but also with social groups very different to those associated with the site in the early days (Gonzalez, 2010). Furthermore, it should be noted that not just users, but also uses themselves may change over time as usage of any complex software is expected, to some extent, to be socially shaped (Dutton, Cheong, & Park, 2004; MacKenzie & Wacjman, 1985; Selwyn, Gorard, & Furlong, 2005). Widening demographics, especially age, has a crucial role within the nature of shared information across boundaries, as users start to befriend parents, grandparents, employers, religious elders, and teachers. As a consequence, a user’s profile may be scrutinized by a number of critical members from different social spheres simultaneously.

Skeels and Grudin (2009) define this group co-presence as “a situation in which many groups important to an individual are simultaneously present in one context and their presence is salient for the individual.” People generally make de-

cisions on what information they share based on which distinct persons or groups are the intended audience (Davis et al., 2005; Jones & O'Neill, 2010; Lederer, Hong, Dey, & Landay, 2004). Privacy issues occur when content meant for one social sphere becomes visible to another. This simultaneity of surveillance can present a challenge for users who endeavor to control information flows (Hewitt & Forte, 2006). The chance that harm may arise out of negative broadcasts increases, particularly when we consider that information online is “persistent” and subject to record permanence (Binder, et al., 2009; Sparck Jones, 2003).

While Facebook provides mechanisms for controlling access to information from different spheres, in the form of “friends lists,” lack of use or over complexity make it likely that they are not effective in separating groups. Binder et al. (2009) refer to this as the “*problem of conflicting social spheres*,” which they argue leads to an increase in “tension” either between the maintainer of the network and one of their connections, or directly between connections (Boyd & Ellison, 2008).

Binder et al. (2009) argue that this increased diversity leads to tension, particularly when the ties involve kinship. They propose that such tension could arise out of disparities between the norms of different social spheres (Binder, et al., 2009). Similarly, DiMicco & Millen (2007), in a study of IBM employees, found that managing profiles with regards to visibility to work-related friends could cause problems. What is fundamental to both these pieces of research is that different social spheres hold different norms, values, and expectations. The issues of conflicting social spheres require rule negotiation and boundary maintenance, otherwise the boundaries become turbulent (Petronio, 2002). Failure to manage boundaries successfully may encourage individuals to become enclosed in their own “self” boundary, severely restricting information throughput (Altman, 1975), and thus the content disclosed to SNSs.

From the perspective of privacy and communication, these overlapping social spheres cause a number of problems. Firstly, we argue that it becomes difficult for a person to manage their boundaries—either through negotiation or acceptance of norms of behavior. Because we may be sharing with multiple audiences, each with its own understanding of what is and is not appropriate, the time and effort to negotiate sharing becomes prohibitive. Secondly, we argue that the role of trust is subverted since while we may have trusted “friends” with whom we have implicit or explicit rules about disclosure, we may also have “friends” who are considerably less close, and with whom there are either no set expectations and rules, or the rules are loosely defined and based on social norms of behavior. The offline equivalent is Altman’s (1975) notion of crowding, where a failure of two privacy mechanisms—control over territory and personal space—leads to *too much* social contact. In instances of overbearing social contact, the individual (or group) will try to close the boundary around the self to prevent information disclosure, or others gaining access to them, to regain control. Consequently, this individual becomes isolated, creating dissonance between their desired level of privacy and their experienced level of privacy.

Overcrowding offline has been studied in terms of personal space, considered to be less than 50 cm between two or more individuals. This distance, like privacy, is non-monotonic. It can differ depending on environment, gender, age group, role, activity, social class, region, desire to be intimate or personal with another, and culture (Aiello & Jones, 1971; Beaulieu, 2004; Evans & Howard; Freedman, 1975). For many SNS users, the online equivalent to personal space is equidistant across audiences and environments. As well as loss of control and the aforementioned issues of information flow on SNSs, individual differences of appropriate disclosure and intimacy demonstrate an array of possible reasons that personal space can be violated, resulting in “digital crowding.”

In online instances we suggest that any unwanted information disclosure or “cross-talk” between multiple audiences that results in the release of information from core layers of the self-construct, is akin to others physically encroaching on one’s intimate or personal space. Both core constructs and personal space relate to intimacy, and a deep level of information, requiring trust for its disclosure or contact. A variation of individual and cultural preferences affects both concepts, and both result in the individual using behavior as a mechanism to regain control. In physical crowding of personal space one might step back from the intruder. In the release of core information, one might close the self-boundary and become isolated. Therefore, difficulties can emerge online when social spheres overlap, when information is leaked to those considered “peripheral” when it is intended for close friends. There may be an emotional reaction, a feeling of privacy violation, and a behavioral mechanism to overcome it.

Digital crowding can also occur from the bombardment of peripheral information disclosure by another: the increased intensity of revelation of the shallower aspects of daily life by other users. An offline example would be a friend that telephones you several times a day with mundane or trivial personal concerns that could be solved easily without consultation, or a child consistently pestering its parents for sweets on a shopping trip. To give an online example, this translates to the continual posting of mundane, useless information via status updates that can result in frustration and annoyance of its readers, ultimately ending in the defriending of individuals.

We hypothesize that the failure of online privacy mechanisms and site designs that allow crowding to occur, such as those on SNSs, will effectively result in the same outcome—*stress and eventual withdrawal*. Paradoxically for SNSs, the success of a site makes it more likely that crowding will occur, meaning that the seeds of failure are sown only in success.

For users, there are a number of possible ways that digital crowding can be reduced. One option is to rely on existing privacy mechanisms to reduce crowding—that is, to engage with the myriad of privacy settings in order to differentiate social spheres, and to re-establish manageable boundaries. This approach will require perseverance to change the settings in parallel with changes to the dynamic social communication boundaries. An alternative approach is one increasingly seen on sites like Twitter—establishing multiple accounts (e.g., one for work, one

for family and friends). Multiple sites could also fulfill this option—for instance, LinkedIn for work, Facebook for social interaction. Users might also establish their desired state of privacy behaviorally—for instance, by limiting the depth of the information about the self that is communicated to others. This solution suggests that the information communicated by users will become increasingly banal as they gain more contacts in different social spheres, assuming that they do not manage their privacy via the site settings.

Failure to adopt multiple accounts, multiple sites, or the privacy settings offered on social media may result in a withdrawal or inhibited posting of content. SNSs encourage continual content provision by their users—otherwise the site lacks any real motivation for visiting (Burke, et al., 2009). The danger for sites is that digital crowding encourages withdrawal—and hence less engagement with the site. An alternative method of controlling digital crowding is to severely limit who is added to the “friends” list on a user’s account. For example, users conscious of these data control issues may only have a small social network of strong ties, but even in these cases, the privacy settings of these strong ties may render the network penetrable.

4.5. Conclusion

People are able to maintain their interpersonal boundaries by managing the amount and depth of information they disclose to others. New technology, in particular social media, makes this more difficult—the sites often rely on disclosure for functionality, personal information can be aggregated across time, and the complexity of privacy settings often makes it difficult for users to differentiate multiple audiences. Together, these effects might equate to a form of *digital crowding*, where excessive social contact prompts users to search for coping mechanisms or to withdraw. The danger, otherwise, is a reduction in liking between contacts and increased tension between an individual and members of different social spheres.

4.6. References

- Acquisti, A., & Gross, R. (2006). *Imagined communities: awareness, information sharing, and privacy on Facebook*. Paper presented at the Privacy Enhancing Technology workshop. Cambridge, UK.
- Acquisti, A., & Gross, R. (2009). *Social Insecurity: The Unintended Consequences of Identity Fraud Prevention Policies*. Paper presented at the Workshop on the Economics of Information Security, University College London.
- Acquisti, A., & Grossklags, J. (2004). Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting. In J. Camp, & Lewis, R. (Ed.), *The Economics of Information Security* (Vol. 12, pp. 165-178): Springer.
- Afifi, T. D., Caughlin, J., & Afifi, W. A. (2007). Exploring the dark side (and light side) of avoidance and secrets. In B. Spitzberg & B. Cupach (Eds.), *The dark side of interpersonal relationships* (2nd ed., pp. 61-92). Mahwah, NJ: Erlbaum.
- Aiello, J. R., & Jones, S. E. (1971). Field study of the proxemic behavior of young children in three subcultural groups. *Journal of Personality and Social Psychology*, 19(3), 351-356.
- Altman, I. (1975). *The Environment and Social Behavior*. Belmont, California: Wadsworth Publishing Company, Inc.
- Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. USA: Holt, Rinehart and Winston, Inc.
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13-28.
- Baum, A., & Valins, S. (1977). *Architecture and social behavior: Psychological studies of social density*. Hillsdale, NJ. and New York: L. Erlbaum Associates.
- BBC News. (2003). Bugged by the boss. BBC News. <http://www.bbc.co.uk/wales/weekinweekout/stories/buggedbytheboss.shtml>. Accessed February 14, 2011.
- BBC News. (2009a). MP's fears at child risk register. BBC News. <http://news.bbc.co.uk/1/hi/england/somerset/8127265.stm>. Accessed February 14, 2011.
- BBC News. (2009b). Facebook remark teenager is fired. BBC News. <http://news.bbc.co.uk/1/hi/england/essex/7914415.stm>. Accessed February 14, 2011.
- BBC News. (2010). A burglar who taunted police on Facebook is jailed. BBC News. <http://news.bbc.co.uk/1/hi/england/manchester/8492500.stm>. Accessed February 14, 2011.
- BCS. (2010). Zuckerberg: Privacy no longer a social-norm. British Computer Society. <http://www.bcs.org/content/conWebDoc/34018>. Accessed February 14, 2011.
- Beaulieu, C. M. J. (2004). Intercultural Study of Personal Space: A Case Study. *Journal of Applied Social Psychology*, 34(4), 794-805.

- Berger, C. R. (1979). Beyond initial interaction: Uncertainty, understanding, and the development of interpersonal relationships. In H. Giles & R. St. Clair (Eds.), *Language and social psychology* (pp. 122-144). Oxford: Blackwell.
- Berger, C. R. (1993). Uncertainty and Social Interaction. In S. A. Deetz (Ed.), *Communication Yearbook 16* (pp. 491-502). London, UK: SAGE Publications Ltd.
- Berger, C. R., & Bradac, J. J. (1982). *Language and Social Knowledge. Uncertainty in Interpersonal Relations*. London, UK: Edward Arnold Ltd.
- Berger, C. R., & Calabrese, R. J. (1975). Some Explorations in Initial Interaction and Beyond: Toward a Developmental Theory of Interpersonal Communication. *Human communication research, 1*, 99-112.
- Binder, J., Howes, A., & Sutcliffe, A. (2009). *The Problem of Conflicting Social Spheres: Effects of Network Structure on Experienced Tension in Social Network Sites*. Paper presented at the CHI 2009, Boston, MA, USA.
- Bonneau, J., & Preibusch, S. (2009). *The Privacy Jungle: On the Market for Data Protection in Social Networks*. Paper presented at the Workshop on the Economics of Information Security, University College London.
- Boyd, D. M., & Ellison, N. B. (2008). Social Network Sites: Definition, History, and Scholarship. *Journal of computer-mediated communication, 13*(1), 210-230.
- Breyer, J., & Zuckerberg, M. (2005). Mark Zuckerberg discusses Facebook. (Video recording, October 26), <http://ecorner.stanford.edu/authorMaterialInfo.html?mid=1567>. Accessed January 2, 2010.
- Burgoon, J. K., & Hale, J. L. (1988). Nonverbal expectancy violations: Model elaboration and application to immediacy behaviors. *Communication Monographs, 55*(1), 58-79.
- Burke, M., Marlow, C., & Lento, T. (2009). *Feed Me: Motivating Newcomer Contribution in Social Network Sites*. Paper presented at the CHI 2009 Conference, Boston, MA, USA.
- 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 and Behavior, 12*, 341-345.
- Collins, N. L., & Miller, L. C. (1994). Self-Disclosure and Liking: A Meta-Analytic Review. *Psychological Bulletin, 116*(3), 457-475.
- Davis, M., Canny, J., House, N., Good, N., King, S., Nair, R., . . . Reid, N. (2005). *MMM2: mobile media metadata for media sharing*. Paper presented at the Proceedings of the 13th annual ACM international conference on Multimedia, Hilton, Singapore, November 06-11, 2005.
- DeCew, J. W. (1997). *In pursuit of privacy: law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.
- Derlega, V. J., & Chaikin, A. L. (1977). Privacy and Self-Disclosure in Social Relationships. *Journal of Social Issues, 33*(3), 102-115.
- DiMicco, J. M., & Millen, D. R. (2007). *Identity Management: Multiple Presentations of Self in Facebook*. Paper presented at the Proceedings of the

- 2007 International Association for Computing Machinery conference on Supporting group work, Sanibel Island, Florida, USA.
- Dutton, W. H., Cheong, P. H., & Park, N. (2004). The social shaping of a virtual learning environment: The case of a university-wide course management system. *Electronic Journal of e-Learning*, 2(1), 69-80.
- Erdelyi, M. (1940). The relation between "radio plugs" and sheet sales of popular music. *Journal of applied psychology*, 24(6), 696-702.
- Evans, G. W., & Howard, R. B. (1973). Personal Space. *Psychological Bulletin*, 80(4), 334-344.
- Facebook. (2010). Statement of Rights and Responsibilities. Facebook. <http://www.facebook.com/terms.php?ref=pf>. Accessed October 2010.
- Facebook. (2011). Facebook Principles. Facebook. <http://www.facebook.com/principles.php>. Accessed February 17, 2011.
- Freedman, J. L. (1975). *Crowding and Behavior*. San Francisco, CA: W. H. Freeman.
- Gonzalez. (2010). About CheckFacebook.com. <http://www.checkfacebook.com/>. Accessed February 15, 2010.
- Govani, T., & Pashley, H. (2005). Student Awareness of the Privacy Implications When Using Facebook. <http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>. Accessed October 6, 2009.
- Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks*. Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society, Alexandria, VA, USA.
- Hasib, A. A. (2009). Threats of online social networks. *International Journal of Computer Science and Network Security*, 9(11), 288-293.
- Hendrick, S. S. (1981). Self-disclosure and marital satisfaction. *Journal of personality and social psychology*, 40(6), 1150-1159.
- Hewitt, A., & Forte, A. (2006). *Crossing boundaries: 'Identity management and student/faculty relationships on the Facebook'*. Paper presented at the Computer Supported Cooperative Work 2006.
- Houghton, D. J., & Joinson, A. N. (2010). Privacy, Social Network Sites, and Social Relations. *Journal of Technology in Human Services*, 28(1), 74-94.
- Joinson, A. N. (2008). 'Looking at', 'looking up' or 'keeping up with' people? *Motives and uses of Facebook*. Paper presented at the CHI 2008 - Online Social Networks, Florence, Italy.
- Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. In A. N. Joinson, K. Y. A. McKenna, T. Postmes & U. Reips (Eds.), *The Oxford Handbook of Internet Psychology* (pp. 237-252). Oxford, UK: Oxford University Press.
- Joinson, A. N., & Whitty, M. (2008). Watched in the workplace. *Infosecurity*, 5(1), 38-40.
- Jones, S., & O'Neill, E. (2010). *Feasibility of structural network clustering for group-based privacy control in social networks*. Paper presented at the

- Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS) 10.
- Jourard, S. M., & Lasakow, P. (1958). Some factors in self-disclosure. *Journal of Abnormal Psychology, 56*(1), 91-98.
- Knobloch, L. K. (2007). Perceptions of turmoil within courtship: Associations with intimacy, relational uncertainty, and interference from partners. *Journal of Social and Personal Relationships, 24*(3), 363-384.
- Lederer, S., Hong, J., Dey, A., & Landay, J. (2004). Personal privacy through understanding and action: five pitfalls for designers. *Personal and Ubiquitous Computing, 8*(6), 440-454.
- MacKenzie, D., & Wacjman, J. (1985). *The social shaping of technology*. Buckingham, UK: Open University Press.
- Norton, M. I., Frost, J. H., & Ariely, D. (2007). Less is more: The lure of ambiguity, or why familiarity breeds contempt. *Journal of Personality and Social Psychology, 92*(1), 97-105.
- Nov, O., & Wattal, S. (2009). *Social Computing Privacy Concerns: Antecedents & Effects*. Paper presented at the CHI 2009, Boston, MA, USA.
- Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. *Communication Theory, 1*(4), 311-335.
- Petronio, S. (2002). *Boundaries of Privacy*. Albany: State University of New York.
- Rubin, Z., Hill, C. T., Peplau, L. A., & Dunkel-Schetter, C. (1980). Self-Disclosure in Dating Couples: Sex Roles and the Ethic of Openness. *Journal of Marriage and Family, 42*(2), 305-317.
- Schatz Byford, K. (1996). Privacy in cyberspace: constructing a model of privacy for the electronic communications environment. *Rutgers Computer and Technology Law Journal, 24*, 1-74.
- Selwyn, N., Gorard, S., & Furlong, J. (2005). *Adult learning in the digital age*. London: Routledge.
- Skeels, M. M., & Grudin, J. (2009). *When social networks cross boundaries: a case study of workplace use of facebook and linkedin*. Paper presented at the Proceedings of the ACM 2009 International Conference on Supporting Group Work.
- Smith, G. F., & Dorfman, D. D. (1975). The Effect of Stimulus Uncertainty on the Relationship Between Frequency of Exposure and Liking. *Journal of Personality and Social Psychology, 31*(1), 150-155.
- Sparck Jones, K. (2003). Privacy: what's different now? *Interdisciplinary Science Reviews, 28*(4), 287-292.
- Spiekermann, S., Grossklags, J., & Berendt, B. (2001). *E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior*. Paper presented at the ACM Conference on Electronic Commerce, Tampa, FL, USA.

- Sprecher, S. (1987). The Effects of Self-Disclosure Given and Received on Affection for an Intimate Partner and Stability of the Relationship. *Journal of Social and Personal Relationships*, 4(2), 115-127.
- Stafford, L., & Reske, J. R. (1990). Idealization and communication in long-distance premarital relationships. *Family relations*, 39(3), 274-279.
- 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.
- Walther, J. B. (1996). Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction. *Communication Research*, 23(1), 3-43.
- Westlake, E. J. (2008). Friend Me if You Facebook: Generation Y and Performative Surveillance. *The Drama Review*, 52(4), 21.
- Young, A. L., & Quan-Haase, A. (2009). *Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook*. Paper presented at the C&T '09, Pennsylvania, USA.
- Zajonc, R. B. (1968). Attitudinal Effects of Mere Exposure. *Journal of Personality and Social Psychology*, 9(2), 1-27.