

# Privacy in Social Collaboration

Elena Ferrari and Marco Viviani

## Introduction

With the expression *social collaboration* we refer to the processes of helping multiple people to interact and share information in order to achieve common goals. Nowadays, collaboration and social dissemination of information are facilitated by the Internet and *Social Network Services* (SNS). The reliance of social collaboration on SNS might seem surprising given the differences between their group-centric and individual-centric views. In particular, social collaboration services focus on group activities, identifying groups and collaboration spaces in which messages are explicitly directed at the group and the group activity feed is seen the same way by everyone. In contrast, social networking services generally focus on single personalized activities, sharing messages in a more-or-less undirected way and receiving messages from many sources into a single personalized activity feed.

Despite these differences, in current digital society a convergence between mass communication and personal communication is leading to social and community uses of online social network services. This is because the present use of social media has grown enormously, moving from a niche phenomenon to mass adoption (Gross and Acquisti 2005). For these reasons, it emerges how social interactions on the online world must not be considered as separated entities with respect to collaborating communities in the real (offline) world. In this scenario, it often comes to light how current social network services architectures do not allow to treat and analyze communities and their privacy issues in the online world as really happens in the offline world. This is due, in particular, to the fact that the online world often does

---

E. Ferrari (✉) • M. Viviani

Dipartimento di Scienze Teoriche e Applicate (Department of Theoretical and Applied Sciences), Università degli Studi dell'Insubria (University of Insubria), Via Mazzini 5, Varese, Italia

e-mail: elena.ferrari@uninsubria.it; marco.viviani@uninsubria.it

not have the same boundaries and does not follow the same social norms which are more clear and common in the offline world. This disparity may exist because social norms are connected to particular situations involving users (AA.VV SPION 2011).

In the offline world, more or less clear barriers exist among situations and contexts. In this scenario, privacy is signaled by physical characteristics: e.g., low lighting, enclosed spaces, and relative isolation from others. People who want to conduct a private conversation can recognize the privacy levels of an offline space based on physical properties (Dwyer and Hiltz 2008).

In the online world, missing these clear boundaries and well defined social norms, and due to the fact that users have more control on how their identity is displayed (since each user can decide which information provide to the world), often the context is not clear and it is free to be filled. Online, privacy levels are not signaled by the inherent properties of the online social space in any clear way, except for the common assumption that nothing is private. In this scenario, some argue that privacy in online communities should be a system level requirement, rather than a group of access settings for each member: privacy should apply to an online space and not be a collection of settings attached to each individual member (Dwyer and Hiltz 2008).

## ***Aim and Organization of the Chapter***

In this chapter we address the problems connected to privacy issues in social collaboration, in particular with respect to social network services when used for social and community-based purposes.

The chapter is organized as follows: in section “Social Communities” we describe the concept of social community in the online and in the offline worlds and the relationships between them; in section “Social Networking” we investigate the community-based use of social networks also providing a brief history of their evolution; section “Privacy in Social Networks Services” arises and discusses privacy issues in social network services especially when context issues emerge from online social behavior of users, and describes some concrete privacy concerns in current SNS. Finally, section “Conclusions and Further Research” concludes the chapter.

## **Social Communities**

### ***The Meaning of Community***

First attempts to define the concept of *community* dates back to nineteenth century, with the studies of the theorists Tönnies (Tönnies and Loomis 1957), Toqueville, Durkheim. These theorists follow the desire for a pre-modern society; in this scenario, a community can be described as a private and intimate place that stands for the basic needs of individuals (e.g., warmth, shelter, nurture, etc.), while *society* is seen as a more rational and purposeful (Kivisto 2003).

In current literature, the *existence* and the utility of the concept of community is debated. In particular, the *focus* of community varies from domain to domain: it is a cultural construct or social context for sociologists; in psychology the individual members of a community are emphasized; anthropologists concentrate on interaction among the members of a community. With such wide-ranging and diverse interpretations, the concept of community is definitely an ambiguous and abstract concept.

According to post-modernists, it is only a diluted concept unsuitable to describe current society. Bauman (2001), for example, sees community as an extension of the concept of identity.

Other authors have another vision and think that the concept of community has still its meaning. Turner, for example, sees community as an opposition to *structure*, an expression of the *social nature* of society (Delanty 2003). He calls *liminality* the expression of such a community. Liminal moments refer to events of life not subjected to instrumental rationality, and create a powerful bonding between members of society. In this vision, one obtains a feeling of belonging and relating to others when not being subjected to rules, laws, norms, etc. Then, in interacting with others, members of the community reveals the community itself (AA.VV SPION 2011).

In his hermeneutic approach on community, Cohen defines it in terms of particular kinds of awareness of reality; and as such community is a “symbolization of boundaries by which the community differentiates itself from others” (Delanty 2003).

Lyon (1986) reviews a plethora of definitions of community, noting that the vast majority enumerates three common qualities: shared place, distinctive social interaction and common ties. These three qualities are not independent, but mutually reinforcing instead. They are distinguishable theoretically, and do capture critical facets of what community is characterized for, as Nisbet (1976) observes.

Based on Lyon and other researchers’ work, Carroll (2011) proposes a conceptual model of communities, comprising of collective identity, community engagement, and network of social ties.

According to Zhang et al. (2011), these three elements emphasis different underpinnings of communities: social identities as psychological foundation, social engagement as behavioral manifestation, and network of social ties as structural depiction of communities.

Following these positive perspective on communities, it is possible to divide the concept of community in two categories: *community of interest*, and *community of place*. Community of place refers to a geographical fixed community. A community of interest is based upon a common interest between members. It may be that both communities overlap each other. This teaches us that a community does not need to be anchored in a particular location, but can also exist in the *virtual*.

### ***From Offline to Online Communities***

As emerges from previous section, definitions of a community are diverse and, at times, vague. Despite this, the concept of community is frequently adopted in the digital era to describe social practices in cyberspace. In fact, individuals can share

their common interests by gathering virtually in the online communities associated with social bookmarking sites, blogs and forums, regardless of their physical location. The absence of a spatial environment has not only complicated how a community have to be defined of the Web, but has also raised issues as to how communities in online environments are to be operationalized for detection and investigation (Zhang and Jacob 2012).

For these reasons, a main question we have to address when dealing with the concept of *online community* is if an online community is a reality or a virtuality with respect to classical ‘offline’ communities.

### Thick and Thin Communities

According to Giddens (1990), *virtuality* is a product of modernity that constantly ‘displaces’ individuals from the places and everyday life with which they were familiar: individuals are re-located in different contexts, in which “familiarity and estrangement are recombined”. Similarly, Rheingold (2000)—to our knowledge the first author having introduced the concept of *virtual community*—describes this concept connected to the Internet as an alternative reality, with capacities to transform society (Delanty 2003). When referring to virtual communities, he only considers non-existing offline communities, exclusively rooted in cyberspace. This means that, for him, virtual communities are ‘communities on the Net’: they do not have their counterpart in everyday life. Even further, the downfall of communities can be compensated by a virtual one (Delanty 2003). In this vision, if virtuality is the opposite of reality, it follows that a virtual community on the Web cannot be regarded as the same as—or even similar to—a traditional offline community. According to Zhang and Jacob (2012), because the online environment can only provide the illusion of reality and because a virtual community exists online, it is not part of the real world and thus cannot be understood or even discussed as a real world community might be.

However, a different and interactionist perspective about virtuality and reality is provided by Castells (1996), who includes the concept of virtuality as a part of the real world. New communities like virtual ones are built out of networks of social actors (individuals, families or social groups) (Delanty 2003). In our global network society, spatial communities are replaced by spaceless ones in the virtual space constituted by the Web. Castells affirms that “localities become disembodied from their cultural, historical, geographical meaning, and reintegrated into functional networks, or into image collages, inducing a space of flows that substitutes for the space of places”. Social relations are not changed by the global network society itself; rather, by the individualism inherent in society.

To sum up, in both authors’ visions, communities can be defined as personalized communities embodied in networks and centered on the individual. But where Rheingolds refers to virtual communities as *thick*, Castells would definitely speak of *thin* communities. With ‘thin’ we refer to a virtual reality that is an addition to the offline reality, whereas ‘thick’ can be seen as an equivalent of the offline reality.

Thick communities are often composed of *strong ties*: frequent contact between people who personally know each other. *Weak ties* are often related with thin communities: they are online ties between persons socially and physically distant, not bound into work structures or circle of friends.

## Social Capital

The concepts described above, and their interactions, bring forward another important concept related to communities: the *social capital*. In sociology, Putnam and Bourdieu are probably the most prominent authors on this topic. Putnam defines social capital on a community level as those “features of social organisation such as networks, norms and social trust that facilitate coordination and cooperation for mutual benefit” (Baum and Ziersch 2003). Bourdieu stresses more the individual aspects in his definition of social capital, seen as “the aggregate of the actual or potential resources which are linked to possession of a durable network of more or less institutionalized relationships of mutual acquaintance and recognition” (Baum and Ziersch 2003).

Broadly speaking, it consists on the expected collective or economic benefits derived from the preferential treatment and cooperation between individuals and groups. In Web 2.0 it is fostered by the possibility to maintain long-term contact with people via weak as well strong ties. Which of these ties contribute more to social capital, it is a debated topic.

Granovetter in his paper on the strength of weak ties (Granovetter 1983) states that weak ties are more important in some situations, as for looking a job. He affirms that weak ties are more likely related to sparse networks. Hence, users that are loosely connected within virtual communities can access remote regions and obtain new and non-redundant information. In contrast, dense networks (dominated by strong ties) facilitate frequent, reciprocal and supportive contact. So, whether or not virtual communities can be labelled as thick or thin, both seem to be important for different reasons.

In his revised copy on virtual communities (Rheingold 2000), Rheingold states the following: “A social network with a mixture of strong ties, familial ties, lifelong friend ties, marital ties, business partner ties, is important for people to obtain the fundamentals of identity, affection, emotional and material support. But without a network of more superficial relationships, life would be harder and less fun in many ways. Weaker ties multiply peoples social capital, useful knowledge, ability to get things done”. Following this ‘optimistic’ vision, weak ties in virtual communities enable users to engage and interact with a variety of other users that do not necessarily share the same interests and environments, expanding users’ horizon. At the same time, virtuality offer the possibility to bring offline contacts to online environments enlarging communication possibilities.

Another author, Calhoun, also assign importance to these mediated relationships, although in his more ‘pessimistic’ view, we should not exaggerate these forms (Delanty 2003). Offline communities are supplemented by virtual ones, rather than

substituted. Calhoun has a rather negative view on the capacity of virtual communities to enhance participation, due to compartmentalization in communities: “we are aware of others but not in discourse with them” (Calhoun 1998). This leads to categorization of individuals. This view anticipates the principle of the filter bubble, introduced by Pariser (2011) and described in section “Filter Bubble”. The filter bubble is an effect of the Internet when tailored to the personal identity of the individual, isolating him/her from other perspectives.

## Social Networking

### *Social Network Services as Online Communities*

Summarizing the definition of community as either a place or a metaphor for place in terms of shape, structure, context and experience, the application of *Social Network Analysis* (SNA) (Scott 2012) offers an efficient and productive approach for the detection and investigation of communities as complex social phenomena in social network services. Using the diagnostic tools of SNA, it is possible to capture the structure and function of communities and to provide a relatively objective interpretation of these ‘subjective’ phenomena.

As introduced before, social network services are now entangled in society and not floating around in a vacuum. In fact, in current dynamic digital society, a convergence between mass communication and personal communication is occurring. This convergence has been defined by Castells (2009) as *mass self-communication*. According to Pierson and Heyman (2011), “on the one hand mass communication because social computing tools can potentially reach a global Internet audience. On the other hand self-communication because the message production is self-generated, the potential receiver(s) definition is self-directed and the message or content retrieval is self-selected”. Hence, new social network services and tools for acting ‘socially’ can be seen as an important fraction of mass self-communication. According to boyd and Marwick (2011), social networks can serve multiple ‘public’ purposes: “they can play a civic function, serving to gather people in a democracy. But they can also play a social role, enabling people to make sense of the world around them and understand their relationships to society”.

Formally, it is still boyd that, with Ellison in boyd and Ellison (2007), defines a social network service as “a web-based service that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site”.

From this definition, we can observe that, in general, a social network service is characterized by the following properties:

- It is an online service, platform, or site that focuses on facilitating the building of social networks or social relations among people;

- People can share interests, activities, backgrounds, or real-life connections;
- Each user has a virtual representation, often a profile, plus his/her social links, and a variety of additional services.

Due to these characteristics, and to mass self-communication, it is possible to recognize several online community services aspects in social network services, leading to an overlapping between the two kinds of services.

### *Evolution in Social Network Services*

Many early online services, including Usenet (Hauben and Hauben 1997), ARPANET, LISTSERV, and bulletin board services (BBS) made efforts to support social networks via computer-mediated communication. At that time, also online services such as America Online, Prodigy, CompuServe, ChatNet, included yet some prototypical features of Social Networking Services. Early social networking services on the World Wide Web began in the form of generalized online communities such as Theglobe.com (1995), Geocities (1994) and Tripod.com (1995). These early online communities were essentially focused on bringing people together to interact with each other through chat rooms, and encouraged users to share personal information and ideas via personal web pages by providing easy-to-use publishing tools and free or inexpensive web space. Other online communities (e.g., Classmates.com) followed a different approach: they simply allowed people to link each other via email addresses. In the late 1990s, thanks to the introduction of the concept of ‘user profile’ as a central feature of social networking services, users started to have the possibility to compile lists of ‘friends’ and search for other users with similar interests. By the end of the 1990s, new social networking methods were developed, and many sites began to develop more advanced features for users to find and manage friends (Livermore and Setzekorn 2009). SixDegrees.com in 1997, followed by Makeoutclub in 2000, Hub Culture and Friendster in 2002 represented the first ‘new generation’ social networking services, and soon became part of the Internet mainstream. Friendster was followed by MySpace and LinkedIn. Attesting to the rapid increase in social networking sites’ popularity, by 2005, it was reported that MySpace was getting more page views than Google.<sup>1</sup>

Facebook, launched in 2004, is currently the largest SNS (Hampton et al. 2011). According to socialbakers.com, one of the biggest Facebook statistics portals in the world, at the time of writing the total amount of users is closing in to one billion users.<sup>2</sup> Hence, more or less 1 out of 7 people in the world have a Facebook-account.

Not only Facebook, but also Twitter has acquired a large market share nowadays. Even if it is difficult to determine the precise amount of users on Twitter, the number of ‘tweets per day’ (TPD) give an indication of the usage of this medium. The average TPD in March 2010 was 50 million according to Twitter statistics. The average

---

<sup>1</sup> <http://www.businessweek.com/stories/2005-07-18/news-corp-dot-s-place-in-myspace>

<sup>2</sup> <http://www.socialbakers.com/countries/continents/>

TPD in February 2011 was 140 million. In 2012, with over 200 million active users, over 400 millions tweets daily have been generated, handling over 1.6 billion search queries per day.<sup>3</sup> This huge increase of tweets gives a strong indication on what can be defined as the hype of today. It is uncertain whether this trend will sustain itself over time. In fact, not so long ago other SNS like Friendster and Myspace, were considered as the revelation of twenty-first century. In May 2011 however, Friendster repositioned itself from a social network service to a social gaming site. Likewise the number of MySpace users has declined immensely.<sup>4</sup> Like Friendster, Massive Media (the company behind Netlog), acquired by Meetic, has moved its scope to dating.<sup>5</sup> All these ‘old’ social network services failed to compete with Facebook and Twitter. Maybe the future will bring the same destiny for Facebook and Twitter, maybe not.

Google+, the new social network service of Google, is a new competitor on the SNS market. With 25 million users in 2011, Google+ has been the fastest website to reach that audience size<sup>6</sup> and it is nowadays the second largest social networking site in the world, having surpassed Twitter in January 2013.<sup>7</sup> As of December 2012, it has a total of 500 million registered users, of whom 235 million are active in a given month.

Regardless the success of specific social networks, their evolutions suggest us that social relationship layers on the Internet are here to stay and continue to gain ground (AA.VV SPION 2011).

### *Studies on Social Network Services*

Different studies on real social network services have revealed a clear connection between offline and online communities. In particular, from a large survey study, Wellman et al. (2001) argued that, besides decreasing social capital in communities, online activities can also increase and supplement social capital (described in section “Social Capital”) in different cases. In fact, SNS applications provide an infrastructure for social participation in online and offline communities that facilitates user contribution, communication, and even collaboration.

When conducting research on MySpace, danah boyd and Ellison (2007) found that teenagers are motivated to go on SNS because their offline friends are there too. Parks (2011) when studying MySpace, stated that “offline and online communities are linked in ways that we are only beginning to understand.” Moreover, “...it may be more accurate to say that virtual communities are often simply the online extension of geographically situated offline communities.”

---

<sup>3</sup> <http://www.techvibes.com/blog/twitter-users-tweet-400-million-times-2012-12-17>

<sup>4</sup> Statistics summary for myspace.com

<sup>5</sup> <http://pulse2.com/2012/12/23/meetic-acquires-massive-media-for-25-million/>

<sup>6</sup> <http://in.reuters.com/article/2011/08/03/idINIndia-58589020110803>

<sup>7</sup> <http://www.forbes.com/sites/anthonykosner/2013/01/26/watch-out-facebook-with-google-at-2-and-youtube-at-3-google-inc-could-catch-up/>



Lampe et al. (2006), in their 2006 study on the use of Facebook, found that it is used primarily for maintaining previous, offline relationships. Again, in 2011, according to Pew research center only a small fraction of Facebook friends, are people we have never met offline: 89% of the friends we have on Facebook, we have met more than once offline (Hampton et al. 2011). Confirming these results, an empirical study by Ellison et al. (2011) shows that getting in touch over Facebook with completely unknown people does not influence users' social capital, though getting in touch with latent or weak ties, for social information-seeking activities, has a direct impact on social capital.

In the same way, Cha et al. 2009, studying information propagation in Flickr, showed that social links are a primary way users find and share information in social media (instead of using other features such as search and hot lists).

Similarly to these works, the focus of most research lies on the individual as a user when it comes to investigating online behavior on SNS, not the community referring to an individual embedded in a particular context. Aim of this chapter is therefore to focus on this particular aspect, connected in particular with privacy issues, as emerges from following sections.

## Privacy in Social Networks Services

With respect to other Web applications, social network services present new challenges concerning privacy issues. SNS are built on interaction, they are typically open systems, and have certain semantic characteristics. Each privacy-related declaration has effects beyond the interaction between one individual data subject and one data collector, effects that may concern a number of members of a community who may or may not be users of the same system (Preibusch et al. 2007).

### *The Context Issue*

As introduced in previous sections, the architecture of SNS does not allow sensing the community in the same way an offline world does, due in particular to the absence of a clear definition of the *situation*, as a way for users to act individually and as a community. In fact, in both scenarios (online and offline), only when the condition of a clear situation is satisfied can adequate behaviors be made possible. With adequate behavior, we mean behavior that takes into account all different aspects that (can) influence behavior in a certain *context*. In the online world, a lot of self-representative information is not put into context and this influences the performance of adequate behaviors, also regarding privacy concerns.

According to Hewitt and Shulman (2010): "A definition of the situation is an organization of perception in which people assemble objects, meanings, and others, and act toward them in a coherent, organized way. A definition of the situation, in

other words, organizes meanings in such a way that people can act individually and jointly”. A clear definition of the situation/context is exactly what is absent on SNS. There are many aspects an individual has to take into account, if it wants to perform adequate behaviors. In an offline world more or less clear barriers between contexts exist. Most of the time we know who is present in a situation, what conduct we ought to expect from others, what role we should perform, and where the situation is located. When mass self-communication enters the picture, this more or less clear context disappears (AA.VV SPION 2011).

### ***Social and Instrumental Privacy***

When the definition of the situation is not clear, performances on SNS become difficult in relation to privacy on mainly two levels: *social privacy* and *instrumental privacy*.

The former can be defined, according to Raynes-Goldie (2010) as “the control of information flow about how and when their personal information is shared with other people”. It usually deals with *disclosure*.

The latter refers to the access by governments and corporations to users data, usually via *data mining* techniques (boyd and Hargittai 2010). Instrumental privacy in online environments deals with the problem of not awareness of people about what happens with their personal information, i.e., who and why they are gathered and the possibility for users to do something about it. In this scenario, individuals often lack every ability to act in a meaningful way (Solove 2001).

Disclosure and data mining in social network services are two macro areas including several privacy issues. Concerning the former area, main topics are self-disclosure (Krasnova et al. 2009), context collapse (boyd and Ellison 2007) or context collision (Raynes-Goldie 2010), and forced disclosure (Gross and Acquisti 2005). Concerning the latter area, both emergent and well known topics are represented by filter bubble (Pariser 2011) and link prediction (Lü and Zhou 2011). All these issues in both areas refer to major gaps in the architecture of SNS. These makes it hard for users to interact, represent themselves and create communities and on top of that bear in mind their social and instrumental privacy.

### ***Disclosure***

In general, information disclosure enables an attacker to gain valuable information about a user (or a system). In social network services, disclosure is often concomitant with the social network service use itself. In fact, according to the already cited definition of SNS provided by boyd and Ellison (2007), social network services allow the creation of “public or semi-public profiles within a bounded system”, they foster the articulation of lists of personal connections within the system, and they

allow the transversal of these connection lists within the system. This way, with respect to the general problem of information disclosure, it has become more evident that in SNS the problem of privacy is not bounded by the perimeters of individuals but also by the privacy needs of their social networks and of the communities they belong to. When information is disclosed on SNS (voluntarily or involuntarily), personal data can be utilized not only for the primary purposes for which they were collected. They can be utilized for secondary (from the perspective of the user) purposes that are covered in the SNS's terms of use and in that sense accepted by users (e.g., targeted marketing), but they can also be utilized for other illegal or unwanted purposes, both from the point of view of the user or the members of the community the user belongs to (indirectly affected by user's information disclosure).

For these reasons, particular attention must be provided in managing 'private' and 'public' data, according to the common classification of confidentiality levels. Preibusch et al. (2007) provide two further levels for classifying data confidentiality, taking into account specific 'group' and 'community' aspects of social network services:

- *Private data*: disclosed to the SNS operator for its internal purposes only, its disclosure needs explicit consent;
- *Group data*: disclosed to the SNS operator and accessed by other users of the same SNS that are also in the same group as the user; data disclosure is limited to the group;
- *Community data*: disclosed to the SNS operator and available to all registered and logged-in users of the SNS; the data is not accessible for anonymous SNS visitors;
- *Public data*: disclosed to the SNS operator and made accessible for all SNS visitors, including anonymous visitors.

Even if the concrete details and the application (and even the interpretation) of these confidentiality levels to data depends on the SNSs implementation, their correct definition and use could help in addressing the privacy issues described in the following sections.

## **Self-Disclosure**

Prior research has considered a range of motivations for self-disclosure in social network services. According to the works of Goffman (1959), Donath and boyd (2004) and boyd and Heer (2006), users employ a social network service as a performance of identity. Strategically presenting themselves, through the constructed profiles, users' challenge is to increase their diverse networks of social ties. Similarly, Lampe et al. (2006) note that motivations for use and disclosure within a social network service are a function of offline outcomes such as relational formation and deepening. Works by Bumgarner (2007) and Joinson (2008) illustrate the social motive of social network service use and consequent personal data disclosure: the participants' desire to connect and learn about one another. Without

significant personal sharing in these sites, these motives of use would not be addressed. For this reason, recent research points out that SNSs seem to require self-disclosure by default (Joinson et al. 2011; Nguyen et al. 2012).

The earliest studies on concrete social network services, provided empirical evidence of the remarkable disclosure practices within the sites. Work by Acquisti and Gross (2006) found that students in the Carnegie Mellon University Facebook network extensively shared sensitive information such as political views and sexual orientation in Facebook, and that information shared in Facebook was generally self-reported as valid. Other studies conducted at the time in different university networks, including Stutzman (2006) and Lampe et al. (2006), further evidenced the high degree of personal disclosure within social network services. Large scale studies such as Thelwall (2008) and James and Webb (2008) provided evidence of similar disclosure phenomena in Myspace, once the leading social network service. These findings were corroborated by a national probability study conducted by Lenhart and Madden (2007).

Despite this, it seems nowadays that users are becoming more and more aware of (at least some) privacy risks connected to social networking. In their study concerning the relationship between perceived privacy and comfort with self-disclosure, Frye and Dornisch (2010) analyzed the behavior of 214 US participants. They reported that participants tended to feel more comfortable disclosing information when they perceived the communication tools as offering a higher level of privacy. Concerning Facebook, its transition to a global social network service and the changes to the interface and to site policies have altered the level of trust individuals have in Facebook itself, which was often described as the more trusted social network service (in particular when compared with Myspace (Dwyer et al. 2007)). To combat the increases in privacy and decreased disclosure to a wide audience in the platform, Facebook has consistently changed the nature of sharing certain items in the platform, and the default sharing settings for new accounts.

The increased awareness of users concerning privacy issues, and the consequent better use of privacy settings provided by online social network services, may help in addressing self-disclosure issues and take part in the management of context collapse.

## Context Collapse

*Context collapse* refers to the challenge of managing disclosure across multiple social contexts in a social network service (Marwick and boyd 2011). Also known as context collision (Raynes-Goldie 2010), it represents a problem for social privacy. It refers to the blurring of contexts in an online environment, whereas in an offline environment more or less strict barriers can be distinguished. Combined elements of mass media and personal communication makes difficult to acquire a proper self-presentation to multiple audiences for people.

On the one hand, there is the idea that this problem cannot be solved, because disclosure networks is so large that according to some authors, the concept of

privacy is ‘a zombie’<sup>8</sup> and ‘illusory’ (Hoadley et al. 2010). As stated in AA.VV SPION (2011), practice does not afford ongoing social surveillance of an entire network, but rather alters of particular situational interest. Indeed, the potential for large-scale surveillance exists, but does not occur in practice due to segmentation, non-participation and socio-technical affordance.

On the other hand, it has been showed that users on social network services seem to have the ability for balancing personal and public information. For example they avoid certain topics maintaining, at the same time, authenticity (boyd 2008). Other strategies employed by users to manage multiple contexts in social network services, have been illustrated in the work of Lampinen et al. (2009, 2011). This range of strategies includes self-censorship, and withdrawal of content, creating more inclusive group identities, and sharing different types of content in different spaces. In addition to these behavioral and mental strategies for context and privacy management, individuals also turn towards the application of privacy settings within the site. Numerous studies documented both increased use of privacy within Facebook by students (boyd and Hargittai 2010; Vitak 2013) and the contextual application of privacy settings in relation to perceived harms (Stutzman and Kramer-Duffield 2010), even if not always privacy settings match users’ expectations (Liu et al. 2011; Special and Li-Barber 2012).

## Forced Disclosure

A problem, related to context collapse, is the phenomenon of *forced disclosure*. It follows the same principle of mandatory disclosure in the field of network security, where mandatory disclosure of vulnerabilities is considered a possible solution because it provide incentives for software firms to make the software code more secure and to quickly fix vulnerabilities that are identified (Choi et al. 2010). Similarly, in social network services, forced disclosure refers to the ongoing process of clarifying private information through private information (according to Rosen (2001)). This is necessary because a lot of self-representative information on social network services is not put into context; for this reason, the only way to clarify this is to augment the amount of disclosed (even private) information on these sites. According to AA.VV SPION (2011), when private information is disclosed, the only way of clarifying this is by giving more private information, in particular in situations presenting multiple context collisions (e.g., when a person breaks up his relationship with someone and changes his status from ‘in a relationship’ to ‘single’ only a couple of people will know exactly what happened. The majority of people will not).

The concept of ‘reciprocal self-disclosure’ (Sprecher et al. 2013) can also be considered a sort of ‘de facto’ forced disclosure. This kind of disclosure is ‘forced’ in the sense that, as it has been proved, participants who disclose reciprocally reports greater liking, closeness, perceived similarity, and enjoyment of the interaction after the first interaction than participants who disclose non-reciprocally.

---

<sup>8</sup><http://technosociology.org/?p=35>

## ***Data Mining***

By analyzing the *big data*, i.e., the digital breadcrumbs of human activities sensed as a by-product of the ICT systems that we use, we have today the opportunity to observe and measure how our society intimately works. These data describe the daily human activities: e.g., automated payment systems record the tracks of our purchases, search engines record the logs of our queries for finding information on the web, social networking services record our connections to friends, colleagues and collaborators, wireless networks and mobile devices record the traces of our movements and our communications.

These social data are at the heart of the idea of a knowledge society, where decisions can be taken on the basis of knowledge in these data. Social data analysis can help us understand complex social phenomena, such as mobility, relationships and social connections, economic trends, spread of epidemics, opinion diffusion, sustainability, and so on.

The opportunities of discovering knowledge from social data increase with the risk of privacy violation: during knowledge discovery, the risk is the uncontrolled intrusion into the personal data of the data subjects, namely, of the (possibly unaware) people whose data are being collected, analyzed and mined. Privacy intrusion jeopardizes trust: if not adequately countered, they can undermine the idea of a fair and democratic knowledge society.

### **Filter Bubble**

A *filter bubble* is a result state in which a website algorithm selectively guesses what information a user would like to see based on information about the user (such as location, past click behavior and search history) and, as a result, users become separated from information that disagrees with their viewpoints, effectively isolating them in their own cultural or ideological bubbles. Prime examples are Google's personalized search results and Facebook's personalized news stream.

The term was coined by internet activist Eli Pariser as "that personal ecosystem of information that's been catered by these algorithms" (Pariser 2011); according to Pariser, users get less exposure to conflicting viewpoints and are isolated intellectually in their own informational bubble. For Pariser, the detrimental effects of filter bubbles include harm to the general society in the sense that it has the possibility of "undermining civic discourse" and making people more vulnerable to "propaganda and manipulation". This constitutes a concrete problem in particular for social network service users and the possibility for them to act as a community: according to Miconi (2013) being a bubble built upon individual tastes and preferences, it does not allow any kind of sharing: in short, everybody is 'alone' in the bubble, condemned to find his own way to knowledge. Again, the bubble is invisible, and, unlike traditional media, it does not reveal its bias and selectiveness. For the same reason, whether users like it or not, they can not choose to enter the bubble: participants are not allowed to actively select the filter.

In addition to this problem, filter bubble presents the same privacy issues connected to algorithms collecting information concerning users: once a user has been observed, profiled and recognized on subsequent visit, according to Parsier the risk posed in the filter bubble are not undone with a simple 'privacy settings adjustment'.

## Link Prediction

*Link prediction* is a sub-field of social network analysis. Link prediction is concerned with the problem of predicting the (future) existence of links among nodes in a social network (Liben-Nowell and Kleinberg 2003). Link prediction is the only sub-field of SNA which has focus on links between objects rather than objects themselves. This makes link prediction interesting and different from traditional data mining areas which focus on objects.

Link prediction can lead to privacy concerns when the predicted link is between users who consider this link to be private. In this case, a sensitive link disclosure occurs. In social network data, for example, the friendship relationships of a person and the public preferences of the friends such as political affiliation, may lead to infer the personal preferences of the person in question as well. Therefore, studying how to prevent sensitive link disclosure while providing accurate link recommendations is an important problem.

To solve it, different strategies have been proposed in literature. Concerning the node data, they are usually anonymized with 'classical'  $k$ -anonymity (Samarati 2001) techniques, or more recent and refined  $l$ -diversity (Machanavajjhala et al. 2007) and  $t$ -closeness (Li et al. 2007) techniques.

For the edge data, different anonymization strategies have been proposed. In Zheleva and Getoor (2008), five possible anonymization approaches are described. They range from one which removes the least amount of information to a very restrictive one, which removes the greatest amount of relational data. Bhagat et al. (2010), provide methods to anonymize a dynamic network when new nodes and edges are added to the published network exploiting link prediction algorithms to model the evolution. Using this predicted graph to perform group-based anonymization, the loss in privacy caused by new edges can be eliminated almost entirely. In Xue et al. (2012), authors theoretically establish that any kind of structural identification attack can be prevented using random edge perturbation techniques. This is confirmed also in Díaz and Ralescu (2012).

## Privacy Settings

According to previous sections, many and different are the ways leading to attempts to instrumental and social privacy of users. This is often facilitated, in current social network services, by the way privacy settings are either implemented or used.

Let us take into consideration Facebook, nowadays the most popular and widespread social network service. At the present moment, Facebook allows users to

manage the privacy settings of uploaded content (photos, videos, statuses, links and notes) using five different granularities: Only Me, Specific People, Friends Only, Friends of Friends, and Everyone. Specific People allows users to explicitly choose friends (or pre-created friend lists, discussed below) to share content with. The default or 'recommended' privacy setting for many pieces of content is Everyone, meaning users share their content with all one billion Facebook users if they decline to modify their privacy settings. Facebook allows users to re-use Specific People privacy settings via friend lists. Users create a friend list, add a subset of their friends to it, name it, and can then select the list as a basis for privacy control. Friend lists are private to the user who creates them, unless the user explicitly chooses to display them as part of his profile. The granularity of privacy settings varies according to content type. Photos are grouped into albums, and privacy settings are specified on an album granularity (i.e., all photos in an album must have the same privacy setting). For the remaining content types, users can specify different privacy settings for each piece of content.

As introduced along the chapter, users awareness and use of these settings have changed over time. For example, from early empirical studies, Facebook users in the United States had inconsistent behavior with respect to privacy concerns, demonstrating excessive sharing of personal data and rare changes to default privacy settings (Gross and Acquisti 2005), even users who claimed to be concerned about privacy (Acquisti and Gross 2006). Still in 2006–2008 a low percentage of Facebook profiles in US were restricted to 'friends only' (Lampe et al. 2008). The situation was slightly different in U.K., where in 2008 the majority of the respondents (57.5%) reported having changed the default privacy settings (Joinson 2008).

Now that more recent studies suggest that users are becoming more privacy concerned and more likely to change their privacy settings (boyd and Hargittai 2010), some problems still remain. In fact, according to Liu et al. (2011) and Madden (2012), users are not completely satisfied about social networks way to protect their privacy. The complexity of privacy settings varies greatly across different social network services. In all, according to Madden (2012), 48% of social networks users still report some level of difficulty in managing the privacy controls on their profile. Few users (2%) describe their experiences as 'very difficult', while 16% say they are 'somewhat difficult'. In particular, social networks users who are college graduates are significantly more likely than those with lower levels of education to say that they experience some difficulty in managing the privacy controls on their profiles. In addition to this, according to Liu et al. (2011), 36% of the Facebook content still remains shared with the default privacy settings and, overall, privacy settings match users' expectations only 37% of the time, and when incorrect, almost always expose content to more users than expected.

### ***Contextual and Demographics Privacy Concerns***

The development of Facebook in 2004 as a university network represented yet a meaningful privacy boundary between students from family, employers, and



municipal law enforcement. With Facebook's growth in popularity, users have to deal with the presence of multiple contextual networks in the site. As a result, the known audience and the expected audience in social network services do not always overlap (boyd and Heer 2006; Lampe et al. 2008; Stutzman and Kramer-Duffield 2010). This can be intended to mean that within a system with hundreds of articulated connections, disclosures are intended for a subset of the audience. In most cases, one does not expect their disclosure to range beyond a certain subset of alters. The implication of this finding is often in collision with discourses that argue that disclosure in a socio-technical system is intended to be public (AA.VV SPION 2011).

Demographics seem to affect privacy attitudes and behaviors of social network service users. In general men had less privacy concerns than their female counterparts, and thus tended to disclose more personal information such as telephone numbers and physical addresses on SNSs (Fogel and Nehmad 2009; Madden 2012). Female users and users who have more Facebook friends are more likely to have friends-only profiles (Stutzman and Kramer-Duffield 2010). In addition to this, individual characteristics such as Internet skill, frequency, and type of Facebook use are correlated with making modifications to privacy settings (boyd and Hargittai 2010; Madden 2012). Users display more concern about sharing with their weak-tie friends than with outsiders or companies. Stutzman and Kramer-Duffield suggest that users adopt friends-only profiles mainly to deal with unintended disclosure to their weak ties rather than outsiders (Stutzman and Kramer-Duffield 2010). Raynes-Goldie found that users cared more about protecting information from members of various social circles, rather than protecting their information from companies (Raynes-Goldie 2010).

## Conclusions and Further Research

As emerges from the literature review, privacy management in social network services is receiving growing attention, in particular when connected to context. In fact, privacy risks emerge above all when individuals are forced to manage their disclosures between different situations and spheres of life, across different communities representing for example the professional and personal spheres, or even communities within an 'augmented reality'. That is, a reality we experience that superimposes a layer of virtual data on top of our actual 'sensate' reality. This mix of virtuality and reality adds useful contextual information, that could be used to better protect users' privacy. At the same time, this poses serious data inference problems.

For all these reasons, in last years, the architecture of SNS has been subjected to constant renovation. In order to help users in managing their privacy settings, 'privacy wizards' or recommendation tools have been proposed, based on the observation that real users conceive their privacy preferences based on an implicit social network structure (Fang et al. 2010). Relationship-Based Access Control (ReBAC) techniques follow the same paradigm: ReBAC is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships, capturing the contextual nature of

relationships themselves (Fong 2011) and trust Carminati et al. (2012) among users. Taking into account concrete social network services, designers have attempted to address the problem of group context management through the inclusion of technical features enabling the grouping of contacts. The Facebook ‘Friends List’ feature allows users to aggregate friends according to individually-defined criteria, and then selectively disclose to these lists. Unfortunately, Facebook’s system is still considered in some way too complicated and/or insufficient to provide privacy at the group level (boyd and Hargittai 2010; Liu et al. 2011; Madden 2012). Google+, the Google social network, aims to “bring the nuance and richness of real-life sharing to software”. Google+ has defined ‘circles’ of life where individuals can place their contacts, and share accordingly (Kairam et al. 2012). Thanks to this intuitive feature, Google+ puts effort in making the group management process more simple. In spite of this, the Google+ ‘real name’ policy and the difficulty to enforce privacy concerns over data associated with multiple users, lead influential critics to challenge the privacy gains of Google+ (Hu et al. 2011; AA.VV SPION 2011).

All these efforts are not still sufficient in our opinion. In fact, as also boyd suggests in boyd and Marwick (2011) on the topic of privacy, the solution to this puzzle will not be to restrict data collection or to enhance individual control over specific items of data, but “to think long and hard about what happens as the data flows across networks and as the data is networked together”. In fact, in the current Social Web vision of the Net, different (contextual) graphs often unifies multiple data flows and social networks, and consequently personal information they provide (Berlingerio et al. 2011).

For these reasons, it is necessary to put more emphasis on the interconnections between offline and online world in achieving privacy, and on the concept of context both intra and inter social network services. When the architecture of SNS will be improved in a way to better take into account these issues, numerous problems connected to identity protection and privacy will be probably solved.

## References

- AA.VV. SPION – D2.1 – State of the Art. In: Gürses S, Leuven KU (eds.) Technical report WP2 – D2.1, SBO Security and Privacy for Online Social Networks, Sept 2011
- Acquisti A, Gross R (2006) Imagined communities: awareness, information sharing, and privacy on the facebook. Volume 4258 of Lecture notes in computer science. Springer, Berlin/Heidelberg
- Baum F, Ziersch AM (2003) Social capital. *J Epidemiol Commun Health* 57(5):320–323
- Bauman Z (2001) Identity in the globalizing world. *Soc Anthropol* 9(2):121–129
- Berlingerio M, Coscia M, Giannotti F, Monreale A, Pedreschi D (2011) Foundations of Multidimensional Network Analysis, *Advances in Social Networks Analysis and Mining (ASONAM)*, International Conference, pp. 485–489. doi:[10.1109/ASONAM.2011.103](https://doi.org/10.1109/ASONAM.2011.103)
- Bhagat S, Cormode G, Krishnamurthy B, Srivastava D (2010) Prediction promotes privacy in dynamic social networks. In: *Proceedings of the 3rd conference on online social networks, WOSN’10*, Berkeley. USENIX Association
- boyd d (2008) Taken out of context: American teen sociality in networked publics. Master’s thesis, University of California

- boyd d, Ellison NB (2007) Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13(1):210–230
- boyd d, Hargittai E (2010) Facebook privacy settings: who cares? *First Monday* 15(8)
- Boyd D, Heer J (2006) Profiles as Conversation: Networked Identity Performance on Friendster, *System Sciences*, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference, 3:59c. doi:[10.1109/HICSS.2006.394](https://doi.org/10.1109/HICSS.2006.394)
- boyd D, Marwick AE (2011) Social privacy in networked publics: teens attitudes, practices, and strategies. In: Proceedings of the A DECADE IN INTERNET TIME: OII SYMPOSIUM ON THE DYNAMICS OF THE INTERNET AND SOCIETY, 21–24 September 2011, University of Oxford.
- Bumgarner B (2007) You have been poked: exploring the uses and gratifications of facebook among emerging adults. *First Monday* 12(11)
- Calhoun G (1998) Community without propinquity revisited: communications technology and the transformation of the urban public sphere. *Sociol Inq* 68(3):373–397
- Carminati B, Ferrari E, Viviani M (2012) A multi-dimensional and event-based model for trust computation in the social web. In: Proceedings of the 4th international conference on social informatics – socInfo 2012, Lausanne, 5–7 Dec 2012. Volume 7710 of Lecture notes in computer science. Springer, pp 323–336
- Carroll JM (2011) *The neighborhood and the internet: design research projects in community informatics*. Routledge, London
- Castells M (1996) *The rise of the network society*. Oxford, Blackwell
- Castells M (2009) *Communication power*. Oxford University Press, New York
- Cha M, Mislove A, Gummadi KP (2009) A measurement-driven analysis of information propagation in the flickr social network. In: Proceedings of the 18th international conference on world wide web, WWW'09, Madrid. ACM, New York, pp 721–730
- Choi JP, Fershtman C, Gandal N (2010) Network security: vulnerabilities and disclosure policy. *J Ind Econ* 58(4):868–894
- Delanty G (2003) *Community*. Routledge, New York
- Díaz ID, Ralescu A (2012) Privacy issues in social networks: a brief survey. In: Greco S, Bouchon-Meunier B, Coletti G, Fedrizzi M, Matarazzo B, Yager R (eds) *Advances in computational intelligence*. Brisbane. Volume 300 of Communications in computer and information science. Springer, Berlin/Heidelberg, pp 509–518
- Donath J, Boyd D (2004) Public displays of connection. *BT Technol J* 22(4):71–82
- Dwyer CA, Hiltz SR (2008) Designing privacy into online communities. *Social science research network working paper series*, Nov
- Dwyer C, Hiltz S, Passerini K (2007) Trust and privacy concern within social networking sites: a comparison of facebook and mySpace. In: Proceedings of the 13th Americas conference on information systems (AMCIS), Keystone, Aug 9–12, 2007
- Ellison NB, Steinfield C, Lampe C (2011) Connection strategies: social capital implications of facebook-enabled communication practices. *New Med Soc* 13(6):873–892
- Fang L, Kim H, LeFevre K, Tami A (2010) A privacy recommendation wizard for users of social networking sites. In: Proceedings of the 17th ACM conference on computer and communications security, CCS'10, Chicago. ACM, New York, pp 630–632
- Fogel J, Nehmad E (2009) Internet social network communities: risk taking, trust, and privacy concerns. *Comput Hum Behav* 25(1):153–160
- Fong PW (2011) Relationship-based access control: protection model and policy language. In: Proceedings of the 1st ACM conference on data and application security and privacy, CODASPY'11, San Antonio. ACM, New York, pp 191–202
- Frye NE, Dornisch MM (2010) When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Comput Hum Behav* 26(5):1120–1127
- Giddens A (1990) *The consequences of modernity*. Polity, Cambridge
- Goffman E (1959) *The presentation of self in everyday life*. Anchor Books, New York
- Granovetter M (1983) The strength of weak ties: a network theory revisited. *Sociol Theory* 1:201–233

- Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM workshop on privacy in the electronic society, WPES'05, Alexandria. ACM, New York, pp 71–80
- Hampton K, Goulet LS, Rainie L, Purcell K Social networking sites and our lives. Technical report, June 2011. Available from <http://www.pewinternet.org/Reports/2011/Technology-and-social-networks.aspx>
- Hauben M, Hauben R (1997) Netizens: on the history and impact of Usenet and the Internet. IEEE Computer Society Press, Los Alamitos
- Hewitt JP, Shulman D (2010) Self and society: a symbolic interactionist social psychology. Pearson
- Hoadley CM, Xu H, Lee JJ, Rosson MB (2010) Privacy as information access and illusory control: the case of the Facebook News Feed privacy outcry. *Electron Commer Res Appl* 9(1):50–60. (Special issue: Social Networks and Web 2.0)
- Hu H, Ahn GJ, Jorgensen J (2011) Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In: Proceedings of the 27th annual computer security applications conference, ACSAC'11, Orlando. ACM, New York, pp 103–112
- James, Webb S (2008) A large-scale study of mySpace: observations and implications for online social networks. In: ICWSM'08, Seattle, vol 8
- Joinson AN (2008) Looking at, looking up or keeping up with people? Motives and use of Facebook. In: Proceedings of the SIGCHI conference on human factors in computing systems, CHI'08, Florence. ACM, New York, pp 1027–1036
- Joinson AN, Houghton DJ, Vasalou A, Marder BL (2011) Digital crowding: privacy, self-disclosure, and technology. In: Trepte S, Reinecke L, (eds) *Privacy online*. Springer, Berlin/Heidelberg, pp 33–45
- Kairam S, Brzozowski M, Huffaker D, Chi E (2012) Talking in circles: selective sharing in Google+. In: Proceedings of the 2012 ACM annual conference on human factors in computing systems, CHI'12, Austin. ACM, New York, pp 1065–1074
- Kivisto P (2003) Key ideas in sociocology. Pine Forest Press, New Delhi
- Krasnova H, Kolesnikova E, Günther OG (2009) “It won't happen to me!": self-disclosure in online social networks. In: Proceedings of the 15th Americas conference on information systems, AMCIS 2009, San Francisco, Aug 6–9, 2009. Association for Information Systems, pp 343
- Lampe C, Ellison N, Steinfield C (2006) A face(book) in the crowd: social searching vs. social browsing. In: Proceedings of the 2006 20th anniversary conference on computer supported cooperative work, CSCW'06, Banff (Alberta). ACM, New York, pp 167–170
- Lampe C, Ellison NB, Steinfield C (2008) Changes in use and perception of Facebook. In: Proceedings of the 2008 ACM conference on computer supported cooperative work, CSCW'08, San Diego. ACM, New York, pp 721–730
- Lampinen A, Tamminen S, Oulasvirta A (2009) All my people right here, right now: management of group co-presence on a social networking site. In: Proceedings of the ACM 2009 international conference on supporting group work, GROUP'09, Sanibel Island. ACM, New York, pp 281–290
- Lampinen A, Lehtinen V, Lehmuskallio A, Tamminen S (2011) We're in it together: interpersonal management of disclosure in social network services. In: Proceedings of the SIGCHI conference on human factors in computing systems, CHI'11, Vancouver. ACM, New York, pp 3217–3226
- Lenhart A, Madden M (2007) Teens, privacy & online social networks. How teens manage their online identities and personal information in the age of MySpace. Available from [http://www.pewinternet.org/pdfs/PIP\\_Teens\\_Privacy\\_SNS\\_Report\\_Final.pdf](http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf)
- Li N, Li T, Venkatasubramanian S (2007) t-closeness: privacy beyond k-anonymity and l-diversity. In: Proceedings of the ICDE'07: IEEE 23rd international conference on data engineering, Istanbul, pp 106–115
- Liben-Nowell D, Kleinberg J (2003) The link prediction problem for social networks. In: Proceedings of the 12th international conference on information and knowledge management, CIKM'03, New Orleans. ACM, New York, pp 556–559

- Liu Y, Gummadi KP, Krishnamurthy B, Mislove A (2011) Analyzing Facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM conference on internet measurement conference, IMC'11, Berlin. ACM, New York, pp 61–70
- Livermore CR, Setzeckorn K (2009) Social networking communities and E-Dating services: concepts and implications. IGI Global, Hershey
- Lü L, Zhou L (2011) Link prediction in complex networks: a survey. *Physica A Stat Mech Appl* 390(6):1150–1170
- Lyon L (1986) *The community in urban society*. Waveland Press, Dawley
- Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramanian M (2007) L-diversity: privacy beyond k-anonymity. *ACM Trans Knowl Discov Data* 1(1):24
- Madden M (2012) Privacy management on social media sites. Technical report, Pew Research Center, Feb 2012. Available from: <http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx>.
- Marwick AE, Boyd D (2011) I tweet honestly, I tweet passionately: twitter users, context collapse, and the imagined audience. *New Med Soc* 13(1):114–133
- Miconi A The big G and the never-ending story of knowledge monopolies. *Mediascapes J* (1):158–160
- Nguyen M, Bin YS, Campbell A (2012) Comparing online and offline self-disclosure: a systematic review. *Cyberpsychol Behav Soc Networking* 15(2):103–111
- Nisbet R (1976) *The quest for community*. Free Press, New York
- Pariser E (2011) *The filter bubble: what the internet is hiding from you*. The Penguin Press, New York
- Parks MR (2011) Social network sites as virtual communities. In: *A networked self: identity, community, and culture on social network sites*, Routledge, New York/London
- Pierson J, Heyman R (2011) Social media and cookies: challenges for online privacy. *Emerald J* 13(6):30–42
- Preibusch S, Hoser B, ürses SG, Berendt B (2007) Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling. In: Proceedings of the workshop on data mining for user modelling at UM 2007, 2007. Available from: <http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/DM.UM07-proceedings.pdf>
- Raynes-Goldie K (2010) Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1)
- Rheingold H (2000) *The virtual community: homesteading on the electric frontier*. MIT, Cambridge
- Rosen J (2001) Out of context: the purposes of privacy. *Soc Res* 68(1):209222
- Samarati P (2001) Protecting respondents' identities in microdata release. *IEEE Trans Knowl Data Eng* 13(6):1010–1027
- Scott JP (2012) *Social network analysis*. Sage, Borgatti
- Solove DJ (2001) Privacy and power: computer databases and metaphors for information privacy. *Stanf Law Rev* 53(6):1393–1462
- Special WP, Li-Barber KT (2012) Self-disclosure and student satisfaction with Facebook. *Comput Hum Behav* 28(2):624–630
- Sprecher S, Treger S, Wondra JD, Hilaire N, & Wallpe K (2013) Taking turns: Reciprocal self-disclosure promotes liking in initial interactions. *Journal of Experimental Social Psychology*, 49, 860–866
- Stutzman F (2006) An evaluation of identity-sharing behavior in social network communities. *iDMAa J* 3(1)
- Stutzman F, Kramer-Duffield J (2010) Friends only: examining a privacy-enhancing behavior in facebook. In: Proceedings of the SIGCHI conference on human factors in computing systems, CHI'10, Atlanta. ACM, New York, pp 1553–1562
- Thelwall M (2008) Social networks, gender, and friending: an analysis of myspace member profiles. *J Am Soc Inf Sci Technol* 59(8):1321–1330
- Tönnies F, Loomis CP (1957) *Community & society (gemeinschaft und gesellschaft)*. Michigan State University Press, East Lansing

- Vitak J (2013) Measuring privacy in online spaces: considerations for users attitudes, disclosures, and network composition. In: Measuring networked social privacy workshop, CSCW13, Feb 23–27, 2013, San Antonio (to appear)
- Wellman B, Haase AQ, Witte J, Hampton K (2001) Does the internet increase, decrease, or supplement social capital? Social networks, participation, and community commitment. *Am Behav Sci* 45(3):436–455
- Xue M, Karras P, Chedy R, Kalnis P, Pung HK (2012) Delineating social network data anonymization via random edge perturbation. In: Proceedings of the 21st ACM international conference on information and knowledge management, CIKM'12, Maui. ACM, New York, pp 475–484
- Zhang G, Jacob EK (2012) Community: issues, definitions, and operationalization on the web. In: Proceedings of the 21st international conference companion on world wide web, WWW'12 companion, Lyon. ACM, New York, pp 1121–1130
- Zhang S, Jiang H, Carroll J (2011) Integrating online and offline community through Facebook. In: International conference on collaboration technologies and systems (CTS), 2011, Philadelphia, pp 569–578
- Zheleva E, Getoor L (2008) Preserving the privacy of sensitive relationships in graph data. In: Proceedings of the 1st ACM SIGKDD international conference on privacy, security, and trust in KDD, PinKDD'07, San Jose. Springer, Berlin/Heidelberg, pp 153–171