# Evaluating social media privacy settings for personal and advertising purposes

Rob Heyman, Ralf De Wolf and Jo Pierson

Rob Heyman, Ralf De Wolf and Jo Pierson are based at iMinds-SMIT, Vrije Universiteit Brussel, Brussels, Belgium.

**Abstract**

**Purpose** – *The purpose of this paper is to define two types of privacy, which are distinct but often reduced to each other. It also investigates which form of privacy is most prominent in privacy settings of online social networks (OSN). Privacy between users is different from privacy between a user and a third party. OSN, and to a lesser extent researchers, often reduce the former to the latter, which results in misleading users and public debate about privacy.*

**Design/methodology/approach** – *The authors define two types of privacy that account for the difference between interpersonal and third-party disclosure. The first definition draws on symbolic interactionist accounts of privacy, wherein users are performing dramaturgically for an intended audience. Third-party privacy is based on the data that represent the user in data mining and knowledge discovery processes, which ultimately manipulate users into audience commodities. This typology was applied to the privacy settings of Facebook, LinkedIn and Twitter. The results are presented as a flowchart.*

**Findings** – *The research indicates that users are granted more options in controlling their interpersonal information flow towards other users than third parties or service providers.*

**Research limitations/implications** – *This distinction needs to be furthered empirically, by comparing user's privacy expectations in both situations. On more theoretical grounds, this typology could also be linked to Habermas' system and life-world.*

**Originality/value** – *A typology has been provided to compare the relative autonomy users receive for settings that drive revenue and settings, which are independent from revenue.*

**Keywords** *Online social networks, Twitter, Facebook, LinkedIn, Advertising, Privacy settings*

**Paper type** *Research paper*

## 1. Introduction

Studies related to social media and privacy refer to at least two types of privacy interchangeably. The latter is problematic, as both interpretations downplay important actors in social media (Karahasanovic *et al.*, 2009). Users are either portrayed as cattle generating money for platform owners (Cohen, 2008; Fuchs, 2012a; 2012b) without a choice or users are lauded as empowered agents writing themselves into being free from constraints (Boyd, 2007).

We will maintain two types of privacy throughout the paper to elaborate on their differences. The first type, "*privacy as subject*", can be summarised as the management of information about one's identity *vis-à-vis* the other users. The latter type of privacy has been called lateral or social privacy. In "*privacy as object*", users are not seen by other users. Algorithms sort their behaviour and user-generated content (UGC) for economic benefits derived from big data.

Both perspectives have a blind spot. The micro-level research exploring benefits for users should not underestimate the limits imposed on their system for commercial reasons, which are driven by decisions taken on an aggregated level. The surveillance and critical theory studies have better tools to conceptualise these challenges, but it is impossible to understand why users join these platforms of exploitation in the first place. Coté and Pybus

Received 24 January 2014
Revised 2 April 2014
Accepted 17 April 2014

This research was funded by EMSOC. EMSOC (User Empowerment in a Social Media Culture) (www.emsoc.be) is a four-year project (1 December 2010-30 November 2014) in the SBO programme for strategic basic research with societal goal, funded by IWT (government agency for Innovation by Science and Technology) in Flanders (Belgium). The research project is a cooperation between Vrije Universiteit Brussel (IBBT-SMIT & LSTS), Universiteit Gent (IBBT-MICT & C&E) and Katholieke Universiteit Leuven (ICRI & CUO), coordinated by IBBT-SMIT.

(2007) have combined these perspectives. They have illustrated how users willingly disclose information that can be commodified afterwards. This motivation is situated in the privacy as subject realm where information disclosure is needed to create and manage an identity: "A MySpace profile can be seen as a form of digital body where individuals must write themselves into being" (Boyd, 2007).

We have made this distinction because this blind spot exists and this is counterproductive, as platforms can claim that they solved privacy issues, while only solving one type. The distinction enables more fine-grained measuring of particular types of privacy, but will also enable researchers to compare user preferences *vis-à-vis* this typology. This is prevalent in privacy settings that address a majority of privacy as subject issues and neglect privacy as object issues.

We therefore test the two concepts of privacy through the analysis of privacy settings in the following social media platforms: Facebook[1], Twitter[2] and LinkedIn[3]. We make use of the notion of "affordance"[4], as defined by Donald Norman, to assess design decisions related to privacy settings. Our research questions related to design are: what type of privacy is offered most and what kind of behaviour is encouraged by default settings?

The paper is structured to develop a better understanding of the two types of privacy and the research related to these two interpretations. We start with framing the perspectives that – implicitly – use the perspective of privacy as subject. Next we do the same for privacy as object. Further on, Norman's affordances are operationalised to evaluate design decisions made in favour or against empowerment in these types of privacy. Finally, we map the different settings of the aforementioned social networks.

## 2. Privacy perspectives

Two different logics may occur when talking about privacy and especially privacy in social media. In social media, information can flow in two directions. Naturally, the first flow of information is directed towards other users. This is of the utmost importance for users because it determines how and if they are going to be perceived by peers and other users (Livingstone *et al.*, 2011). The second flow of information concerns the parties that are not seen as people or "friends". These parties collect personal identifiable information (PII) regardless of the profile being private or public (Clarke, 1988; Fuchs, 2011; Gandy, 2003; Solove, 2001). We will address the former type as privacy as subject, because both sender and receiver of information are interpreting, communicating subjects. The latter type, privacy as object, approaches users and their data as manipulable objects, devoid of any agency. Table I gives an overview of the two types of privacy and their characteristics.

A recent Eurobarometer research on social media and electronic identity (European Commission, 2011) surveyed the different opinions and habits Europeans have towards data disclosure. Forty-four per cent worry about their information being used without their knowledge, and 38 per cent fear that this information might be shared with third parties without their agreement. Thirty-two per cent are afraid of the risk of identity theft through information disclosure. Twenty-eight per cent are afraid that it might be used to send out unwanted commercial offers, and finally, 25 per cent worry that their information might be used in different contexts form the one where they originally disclosed the information (European Commission, 2011, p. 56).

**Table I** Privacy as subject and object

| *Privacy as subject* | *Privacy as object* |
|---|---|
| Micro-level (interpersonal) | Macro–meso level (mass of users or objects) |
| Personal information, UGC | Data, big data, anonymous data |
| Identity | Profile |
| Personal motivation for distribution, information disclosure is mostly explicit | Economic motivation, information disclosure is mostly implicit |

The Eurobarometer results show that users are concerned about multiple kinds of privacy threats. However, not all of these threats can be controlled by privacy settings. Krasnova *et al.* (2009) have mapped the various threats social network site (SNS) users perceive. They found four categories through focus-group interviews:

1. general accessibility;
2. social threats;
3. organisational threats; and
4. identity theft.

General accessibility is the fear of users that their information might be found by unintended recipients, such as students, parents, future employers, etc. Social threats are seen as threats arising within the SNS environment of a user, through active or passive use of the service, and typical examples may be cyberbullying or getting tagged in awkward photos. Organisational threats are instances where personal information is exchanged with organisations such as the SNS owner or third parties. Finally, one respondent feared identity theft on SNS. King *et al.* (2011) have adapted this division as institutional and interpersonal privacy threats, which are, respectively, organisational and social threats.

Krasnova *et al.* (2009) interpret privacy as informational privacy, defined by Westin (1970) as: "the right of the individual to decide what information about himself should be communicated to others and under what circumstances". The same definition is used by Diaz and Gürses (2012) to describe privacy paradigms. In this paradigm, the "privacy as control" paradigm, the platform owner is expected to respect the user's choices with regard to settings and with regard to the proposed privacy policy (Diaz and Gürses, 2012; Paul *et al.*, 2011). This is opposed to the conception of a malign or incompetent platform owner with whom as little information as possible is shared, due to the anticipated consequences such as data leakage or transgressions of the privacy policy (Diaz and Gürses, 2012). Another articulation of the access control model approach is Nissenbaum's (2004) privacy as contextual integrity. This theory presupposes that every situation of information disclosure has rules. These rules determine what information flows to whom. A privacy breach occurs when information is flowing outside these rules.

Informational privacy (Westin, 1970) and contextual integrity (Nissenbaum, 2004) are general theories of privacy that focus on meta rules to evaluate privacy. The robustness of these models renders them applicable to both types of privacy. But these robust models are not able to explain why Gmail users share their inbox with an algorithm[5] but would not share the same content with friends. We create this division to explain the different logics at work between third parties and users.

Privacy settings can be seen as an explicit articulation of these rules. But we should not forget that these settings are man-made and, therefore, exclude certain affordances (Norman, 1999). An affordance is the relation that a user has with an object with regard to the properties of that object, for example one of the affordances of a chair is that you can sit on it. Designers may choose to limit functional properties by disabling them physically; it is, for example, impossible to fuel a gasoline car with diesel because the nozzle for diesel is too big to fit in the fuel tank. Privacy settings can also be limited in the same way when options are not offered at all.

### *2.1 Privacy as subject*

Privacy as subject sees users as actors who provide personal information to form and manage their identity. It focuses on "the control of information flow about how and when personal information is shared with other people" (Raynes-Goldie, 2010). We hereby want to emphasise the role of the user and the subjectivity of privacy:

> In privacy as subject we allocate a more or less active role to the user. We consider the user as an active subject defining who can and cannot see his personal information flow. It is not just

about the information flow an sich, but also about using this information for creating meaning in a social context (De Wolf *et al.*, 2013).

It should be clear that privacy as subject presupposes different privacy problems in comparison to privacy as object. However, they cannot be seen as opposites. The latter becomes very clear from a symbolic interactionist (SI) perspective, where we capture the relationship between identity and privacy[6] in such a way we can expose the specific privacy problems related to privacy as subject. The SI school of thought studies how the social world is created through interaction between individuals and the social environment (Collins, 1994; Hewitt, 2007). It is through the act of speech that symbols (e.g. democracy) can be extracted and society can exist. The self is the central concept of study within SI. Mead, one of the founding fathers, defines the self as:

> [. . .] something which has a development; it is not initially there, at birth, but arises in the process of social experience and activity, that is, develops, in the given individual as a result of his relations to that process of a whole and to other individuals within that process (Mead and Morris, 1992, p. 91).

Hewitt (2007), as a contemporary adherent, conceptualises identity as the acting part of the individual next to emotions and cognitions. It is through actions of announcements and placements that an identity crystallises. Announcements can be seen as everything an individual undertakes to be recognised for. Placements are actions of others to recognise announcements. Identity formation is hence a social process. It is important to denote that the whole identity formation process does not take place in an empty space, but is anchored in specific contexts.

Goffman (1990) has discussed the importance of "the presentation of self in everyday life"[7]. He is especially noted for his description of front and back stage. A front stage can be seen as that part where an actor plays a role for the audience. He defines it as "that part of the individual's performance which regularly functions in a general and fixed fashion to define the situation for those who observe the performance" (Goffman, 1990, p. 32). A back stage has to be seen as a place where suppressed front-stage material makes an appearance. On the topic of a back stage he states that "it is here that the capacity of a performance to express something beyond itself may be painstakingly fabricated; it is here that illusions and impressions are openly constructed" (Goffman, 1990, p. 114). Goffman (1990) observed how social institutions were organised and often saw the contours of a back and front stage determine the context of conduct, e.g. a staffroom within a school can function as back stage for a teacher. We claim that this process of back and front stage does not have to be so tangible, but can be expanded to the process of announcements and placements in the formation of an identity. Individuals will only disclose or announce certain information in one particular context and withdraw other. Basically, some information remains in one context (back stage), whereas other is displayed (front stage)[8]. Identity and privacy are thus two sides of the same coin, whereas their common denominator, that is context, plays a valuable role.

In current mass self-communication society (Castells, 2007), the social media ecology can be regarded as a collapsed environment (in comparison to older media environments), where time and space barriers are difficult to draw. In one way this can be considered liberating and even empowering because an identity can be formed without role and other limitations related to context (De Wolf and Pierson, 2012)[9]. Then again, this creates (contextual) privacy problems as well. Context collision (Boyd, 2008), social convergence (Boyd, 2008) or context collapse (Raynes-Goldie, 2010) all refer to a same process that indicates how offline barriers have faded away online[10]. Boyd (2008) points out that this absence of barriers problematises the audience for whom the identity is performed. This is due to invisible audiences: audiences to whom the information flow in time (e.g. future audiences) and space (e.g. friends of friends) was not intended or perceived. Related to this is the privacy problem of blurring boundaries between public and private (Boyd, 2008), e.g. a boss reading a negative announcement on his person by one of his employees on

the Facebook newsfeed. A last problem we find in the notion of forced disclosure, as described by Rosen (2001). The latter indicates that private information, when not fully clear, can only be clarified through more private information (e.g. the only way to clarify your relationship breakup is by providing it with more background)[11]. In combination with context collision, the user could end up with a situation where he implicitly or explicitly is forced to constantly clarify the context with meaning.

Next to these problems we want to emphasise that "more privacy" is not necessarily a good thing and on its own an empty concept. There is always a trade-off between privacy and identity. The more information is withdrawn, the less it is disclosed and can function as an announcement within the process of identity formation. This also indicates that context collision on its own cannot be seen as a privacy breach.

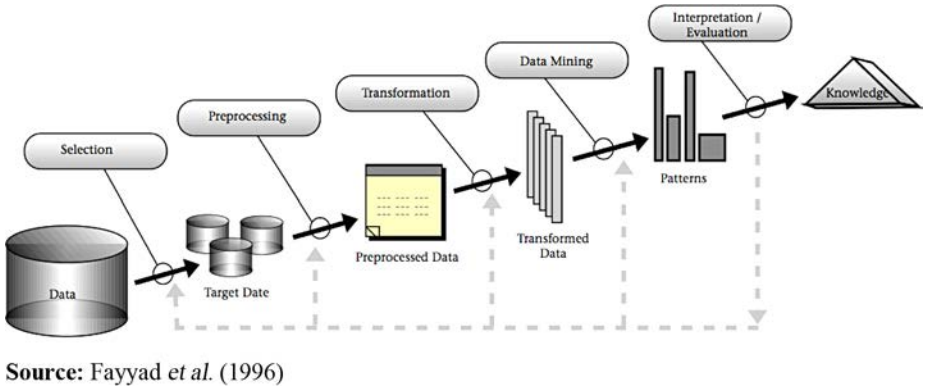
### *2.2 Privacy as object*

Users are objectified as their information enters a database. The process to derive knowledge out of databases is called KDD (Knowledge Discovery in Databases) and data mining is one step in this process (Fayyad *et al.*, 1996, p. 41). This is important because KDD is the tool to objectify individuals and their data into profiles: "The data are recorded as a type of brute facts, de-contextualised and – as far as the machine is concerned – without meaning." (Hildebrandt, 2006b) (Figure 1).

The general goal of KDD is "the nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data" (Fayyad *et al.*, 1996, pp. 40-41). Two types of knowledge are generated through this process: verification and discovery of new information. In the first type, the data are used to verify existing hypothesizes, and in the second type, the data are used to predict whether someone belongs to a certain profile. Commercial uses for these data are recognising distinct customer groups, predicting when people are going to buy a product and recognising fraud or *bad* customers (Fayyad *et al.*, 1996, p. 38; Gandy, 2003, pp. 5-6). "Bad" is emphasised because this is defined from an economic logic, wherein companies do not wish to contact these potential consumers because they cost more than they return.

The data in KDD processes are ordered and changed to fit KDD needs and this implies that they change for privacy as subject as well. As KDD is a computer science discipline, Hildebrandt uses a computer science definition of identity: "the set of true facts that uniquely defines each and every individual" (Hildebrandt, 2006a, p. 9). This idea of true facts presupposes that a person can be defined through categories that apply to anyone (Hildebrandt, 2006a, p. 8).

**Figure 1** KDD process




**Source:** Fayyad *et al.* (1996)

KDD perspectives look at data as fixed categories to define an identity. Identity is reduced to fixed categories and this is in conflict with identity defined in privacy as subject (see earlier). Hildebrandt further uses Deleuze's concept of virtualisation to point out that our identity is in a constant flux and should be seen as something indeterminate and unpredictable (Hildebrandt, 2006a, pp. 10-11). This intangibility gives us freedom and this is taken away in KDD because it presupposes a fixed identity through shared categories or quasi-identifiers.

Users are put in databases for commercial purposes and one of these is marketing. In this case, they are further objectified to commodities. Smythe (1977) conceptualised audiences as commodities in 1977, long before the advent of social media. He questioned what the advertising agencies were buying and what the audience's (of media like news papers, radio and television) involvement was: were they performing labour or not? As the possible actions of users increased [cf. mass self-communication (Castells, 2007)] through the development of social media, users of these media can be more easily seen as labourers (Cohen, 2008; Coté and Pybus, 2007; Fuchs, 2012a; 2012b; Heyman and Pierson, 2011).

Before fully describing users as labourers, we illustrate the different actions performed by users:

1. As users visit social media, they are inadvertently looking at advertising and this attention is bought by advertising companies through demographics, see Figure 2[12].
2. Users produce UGC to create an identity as described in privacy as subject, but this information may also be used for advertising purposes (targeting or integration of social content). Cohen (2008) also notes that this content attracts other users to the platform, which increases the odds that they will look at advertising.
3. Fuchs (2012a, 2012b) and Smythe (1977) also see this exposure to advertising (1) as an inducement for users to learn how to spend their money.
4. Finally, Coté and Pybus indicated that this teaches users how to write themselves into being, and this unintentionally adds value to marketable objects, either by liking them or by writing about them.

Fuchs (2012a, 2012b) refers to a (fictional) minor called Adam, who is being served Facebook advertising based on his monitored interests. "Facebook thus profits and could not exist without the unpaid labor that Adam and millions of his fellow Facebook workers conduct. Adam is the prototypical Facebook child worker" (Fuchs, 2012a, 2012b). This is clearly intended to provoke, but it fails to account for Adam's initial intentions to disclose information. It also exposes a Marxist fallacy shown by Smythe and Livant: "What often escapes attention is that just because the labourer sells it (his or her labour power) does not mean that he or she produces it" [Livant, cited in (Smythe, 1977, p. 7)].

Livant's remark is important because it problematises the over-application of labour to a point where all free time, except from sleeping, will become labour (Smythe, 1977). In this case, we wish to draw attention to the fact that the labour on social media is sold, but that the labour is not deliberately made by the user to be sold. What users generate on social media is made with a different intention, to manage an identity. Labour performed by users on social media can therefore be seen as an emergent, implicit property that would not exist in non-commercial platforms.

To conclude, our distinction (Table II) can now be interpreted differently. The motivations to manage an online identity can be seen as an inducement to allow privacy as object-related processes. As long as these two types of privacy remain reduced to one definition, it is problematical to evaluate privacy settings or policies. This was put very clearly by Mark Zuckerberg himself: "*the privacy is largely false – but for most* students, *the privacy* is good enough" (Stutzman, 2006).

However, by adding Norman's affordances to contextual integrity, we have a way to map empowerment or disempowerment within privacy settings. Empowerment in the general sense is defined as "enabling people to control their own lives and to take advantage of opportunities"

**Figure 2** Facebook targeting options

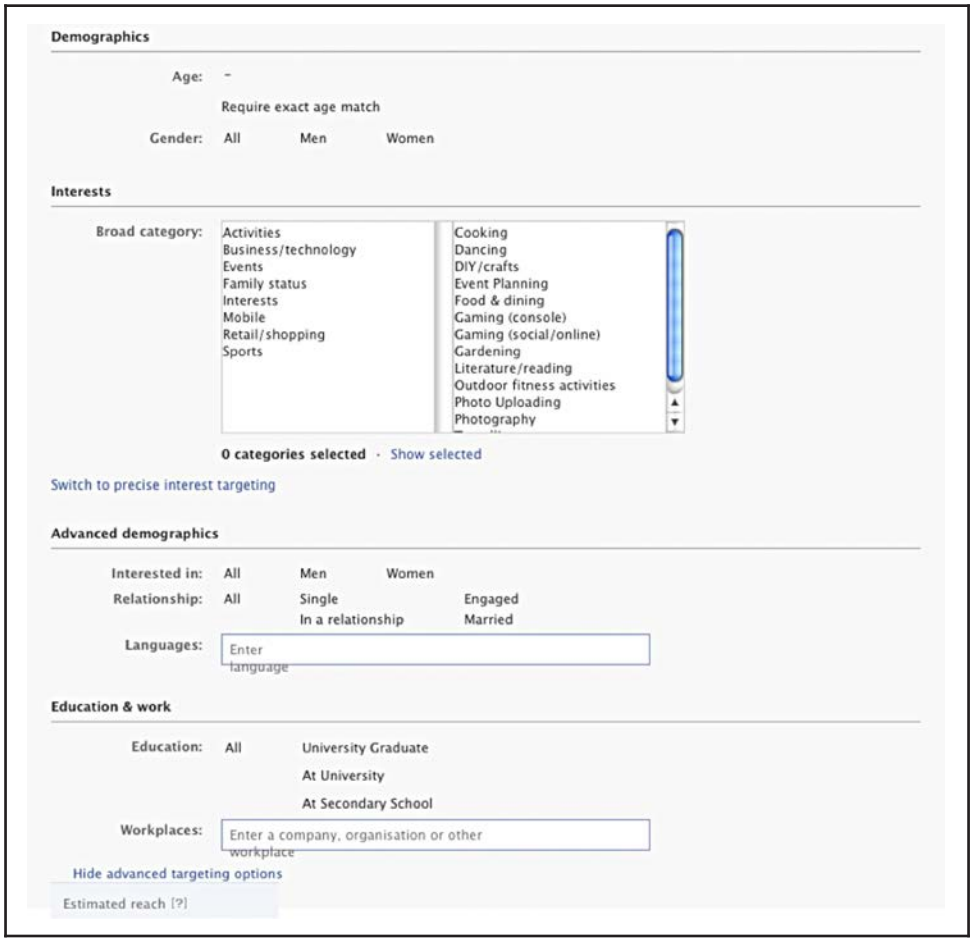



**Table II** Privacy as subject and object

| *Privacy as subject* | *Privacy as object* |
|---|---|
| Micro-level (Interpersonal) | Macro–meso level (mass of users or objects) |
| Personal information, UGC | Data, big data, anonymous data |
| Identity | Profile |
| Personal motivation for distribution, information disclosure is explicit | Economic motivation, information disclosure is implicit |

(van der Maesen and Walker, 2002, p. 24) or in other words "a process, a mechanism by which people, organisations, and communities gain mastery over their affairs" (Rappaport, 1987).

Previous research (King *et al.*, 2011) has already shown that users are uncertain or do not know how to use privacy settings for apps. Krasnova *et al.* (2009) have already argued that organisational privacy or privacy as object threats are hard to address in privacy settings. With this distinction, we wish to see how economic motivations shape the design of privacy settings and thus users' privacy options.

## 3. Research set-up

We will map the different privacy settings provided by three popular social media platforms: LinkedIn, Twitter and Facebook. The mapping was performed in May 2012. The selection of these platforms is based on previous work where we also mapped the information collected from users and how this was communicated. The most important reason to select

these networks was the fact that they rely, or in the case of LinkedIn relied, on advertising as their main revenue stream. Facebook's advertising revenue was 85 per cent of their total revenue stream (PrivCO, 2012, p. 18). Twitter is figuring out ways to increase revenue with promoted tweets, trends and accounts (Dillet, 2012; Swisher, 2011). LinkedIn used to have a slightly bigger revenue for its hiring solutions and this has now grown to 54 per cent, while advertising is only 26 per cent (Rao, 2012) (Table III)[13].

### 3.1 Representation and selection of results

Only those settings will be included that offer a choice with regard to privacy. This implies that settings with regard to notifications, emails and safety will be omitted. To map this, Norman's (Norman, 1999) concept of perceived affordance will be used to discern whether a setting advertises a choice with regard to an access control model:

> [. . .] the term affordance refers to the perceived and actual properties of the thing, primarily those fundamental properties that determine just how the thing could possibly be used. A chair affords ("is for") support and, therefore, affords sitting. A chair can also be carried (Norman, 1998).

Due to the popularity of the concept, affordance covered too many meanings and was divided in two sorts of affordances that are especially useful for the evaluation of computer screens:

> [. . .] designers sometimes will say that when they put an icon, cursor, or other target on the screen, they have added an "affordance" to the system. This is a misuse of the concept. The affordance exists independently of what is visible on the screen. Those displays are not affordances; they are visual feedback that advertise the affordances: they are the perceived affordances (Norman, 1999).

To present the settings in a comprehensible way, we will show them as a flowchart, which represents the path a user has to take through the website structure to change settings. The flowchart is colour-coded to show what options are related to privacy as subject (yellow rectangle), privacy as object (blue oval) or both (green diamond). The analysis is performed on default settings[14], and default settings are indicated with a ticked checkbox symbol (✓) (Figure 3).

*3.1.1 Twitter.* Figure 4 shows Twitter settings.

*3.1.2 LinkedIn.* Figure 5 shows LinkedIn settings[15].

*3.1.3 Facebook.* Figure 6 shows Facebook settings.

### 3.2 Identification of privacy settings

We will first report on characteristics shared by all three social media platforms and we will then continue with more specific aspects pertaining to specific platforms. Yellow is the most common colour, followed by green. This implies that users are given relatively more choices with regard to privacy as subject than as object.

The access control model of privacy as subject is open by default. This implies that users can only limit their communication once they visited the privacy settings and this indicates that users who do not visit settings are more exposed than other users. However, all the settings on the studied social media platforms allow limiting personal communication to user-defined

**Table III** General information

| *Overview of Facebook, LinkedIn and Twitter* | *Facebook February 2004* | *LinkedIn May 2003* | *Twitter March 2006* |
|---|---|---|---|
| Users | 500 million (January 2011) | 101 million (January 2011) | 100 million (October 2011) |
| Average age | 48 per cent 18-34 years | 38 per cent 35-49 years | 42 per cent 30-49 years |
| IPO | 18 May 2012 | 18 May 2011 | N.A. |

Sources: Anon (2011); Parr (2011); Verde (2011)

**Figure 3** Flowchart colour coding

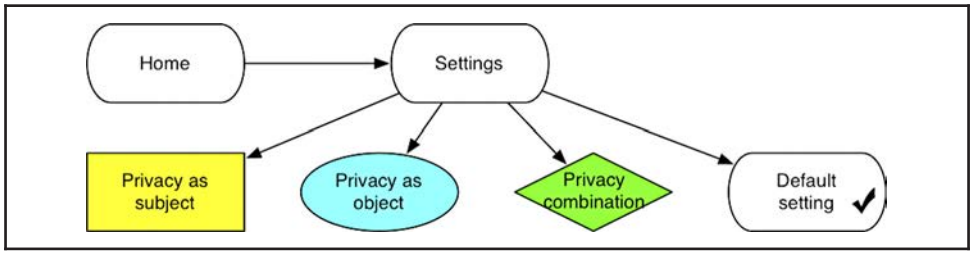
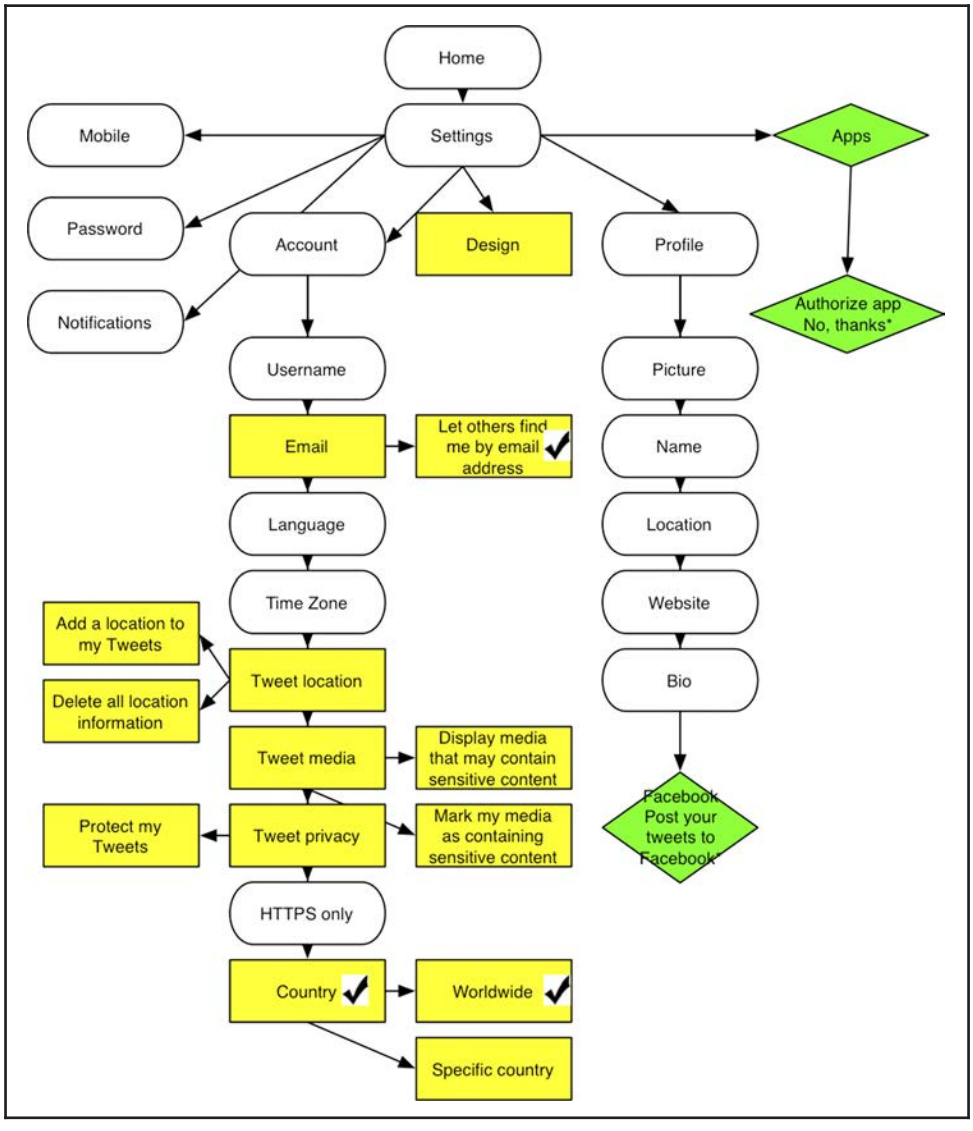


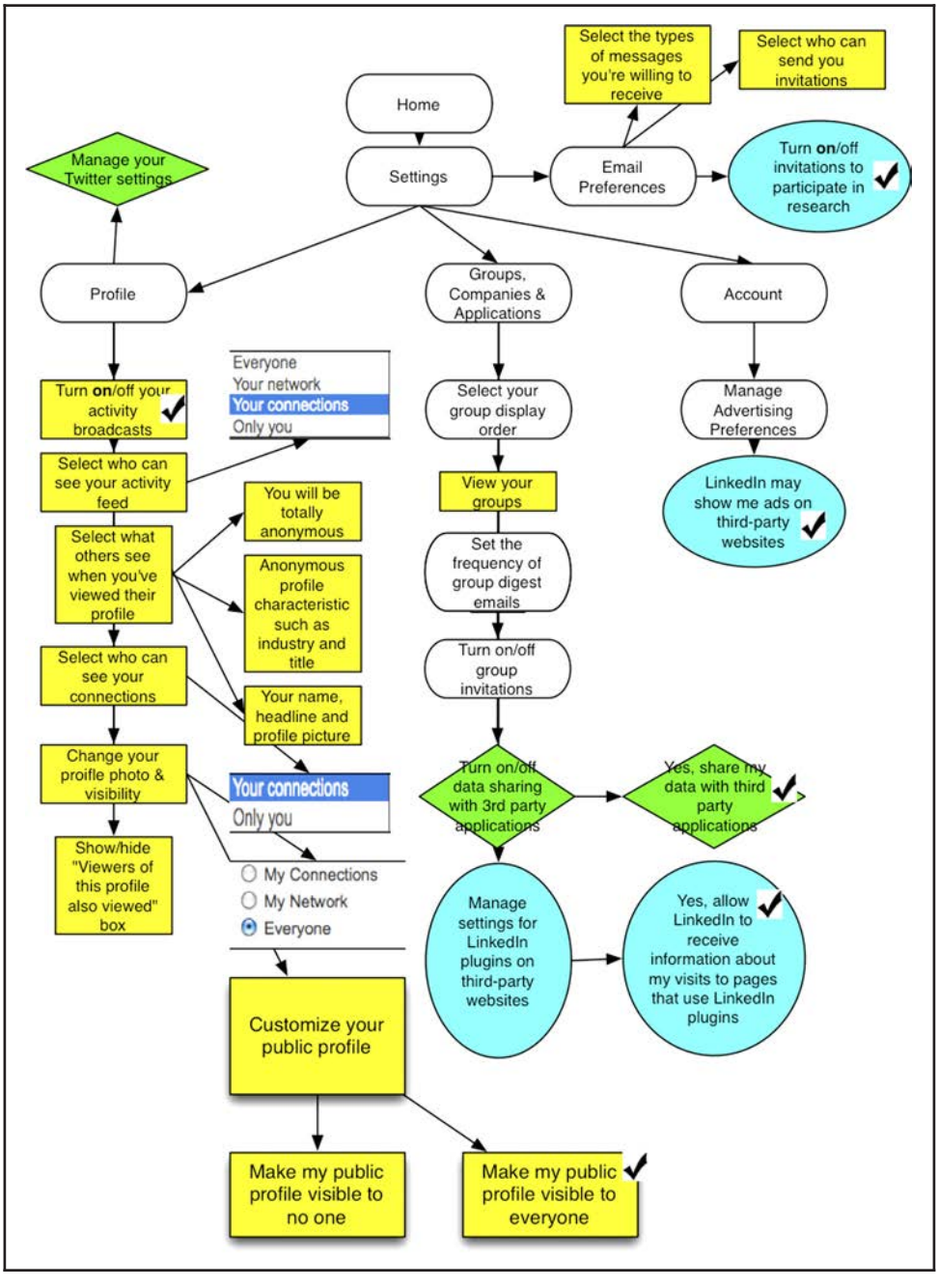

**Figure 4** Twitter settings




groups. Profile searchability[16] can be customised to remain completely hidden, but this option is disabled by default and non-existent for Twitter users.

The options displayed in green show an overlap of both privacies. This is the case for options that are related to advertising and applications. In the case of applications, the user has to decide how and to what extent information from the platform is shared with the

**Figure 5** LinkedIn settings

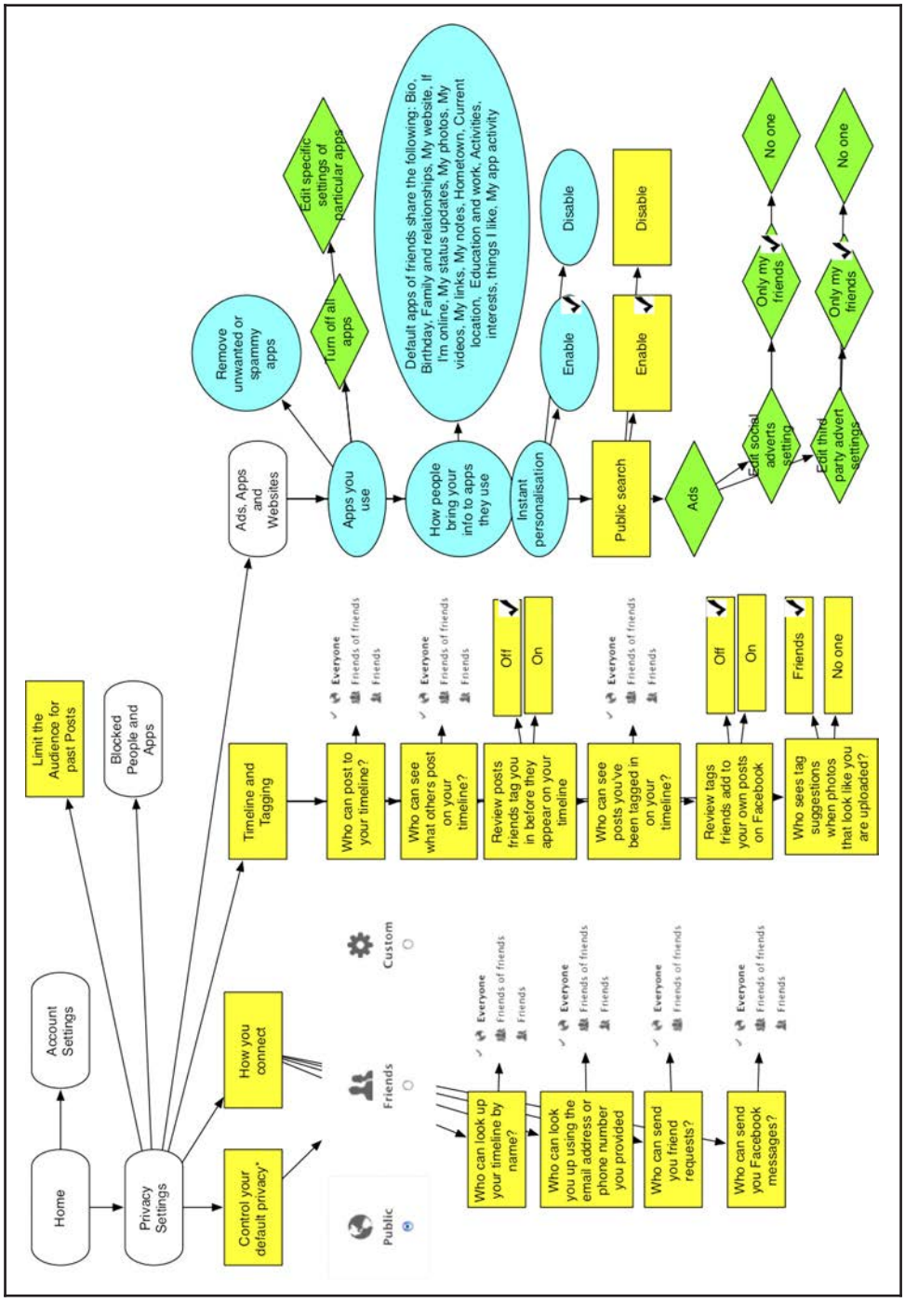



application. Because, the application can usually post things on behalf of the user, it is privacy as subject. Applications may also collect data for other purposes, and therefore, it is also privacy as object.

Green options also refer to advertising, which incorporates users' names and other information in the case of LinkedIn and Facebook[17]. These options are enabled by default, but it is possible to opt-out. The privacy as subject access is limited to connected contacts only because it would lose its social meaning otherwise.

Blue settings are the scarcest, which implies less user choice for privacy as object. Users are unable to choose to opt-out of all targeted advertising, and this is the reason why there are no blue settings in the Twitter flowchart. LinkedIn offers advertisers to advertise outside

**Figure 6** Facebook settings




its platform, through its ad network (Heyman and Pierson, 2011), and users may choose to opt-out. Facebook and LinkedIn personalise websites through plug-ins, and it is also possible to opt-out of this option. Facebook has recently launched an ad exchange, and this will allow advertisers to retarget users who have visited their website or who did not finish their online purchase (Edwards, 2012). It is impossible to disable this form of tracking. Finally, Facebook makes use of "sponsored stories" to integrate UGC, which promotes a brand, product or service. It is impossible for users to opt-out of these "sponsored stories".

## 4. Conclusion

The division of privacy helps to understand why some options are more controllable than others. If we couple this information to the default settings, it becomes clear that all social media platforms try to induce users to generate as much UGC as possible, but also to generate and share as much information as possible. This last inducement is necessary to keep other users on the platform. Users are discouraged to limit their audiences through default privacy settings.

When the amount of privacy as subject and object settings are compared, then it is clear that users are offered a bigger choice over their privacy as subject, but are limited to their privacy as object. The numerical dominance of privacy as subject does not signify that this type of privacy is successfully addressed. Users employ various different social strategies in managing their privacy as subject Boyd and Marwick, 2011, rather than relying on the privacy settings provided by social network providers. This indicates that the given privacy as subject options do not necessarily correspond with the users' expectations or needs.

The instance of a combination of both privacy as object and subject is an epitome of the on-going commodification of users. Users' PII was used to deliver personalised advertising in privacy as object, but now their UGC and reputation are being mobilised to deliver commercial messages. This is problematic because the logic of privacy as object interferes with the logic of privacy as subject, which means that the expanding commodification is now managing our identity through social and integrated advertising.

The proposed distinction may help us to discern what kind of privacy is more controllable for users. When we look beyond privacy settings, the same distinction could be used to evaluate EU privacy legislation, which at first glance favours privacy as object because it is only concerned with the systematic gathering and use of PII. Personal use of PII or privacy as subject is an exception to the legislation. Privacy as subject may become more important due to the friction caused by privacy as object or due to harmful instances such as cyberbullying and sexting.

Our mapping of privacy settings could also serve as a starting point to discuss what the default setting should be, but also whether we should get more settings to control what is left beyond user consideration. The current model allows the freest flow of information, but this might prove harmful for the less aware and literate social media users.

Finally, further research should be done on comparing these settings with privacy policies and user perceptions of the access control models offered by social media. The focus on settings may divert attention to issues that are controllable, which neglects an important part of possible awareness of other information flows.

## Notes

1. www.facebook.com
2. www.twitter.com
3. www.linkedin.com
4. "the term affordance refers to the perceived and actual properties of the thing, primarily those fundamental properties that determine just how the thing could possibly be used" (Norman, 1998).
5. Gmail uses an algorithm to match the content of email messages to advertising to increase relevance.
6. Other theoretical frameworks can/should be used to illustrate the nature of privacy as subject. However, we find this socio-cultural approach especially useful in studying identity – and thereby privacy. We believe that the affordances and problems created by SNS, and social media in general, cannot be studied without the context of conduct. A symbolic interactionist framework emerges as a valuable tool because much attention is paid to the reciprocal relationship between an individual and the group he or she is embedded in.
7. Goffman does not use the term "context" but uses "stage" or "regions", making the analogy with dramaturgy.

8. Our interpretation of identity and privacy is closely related with the theory of Communication Privacy Management (CPM) that focuses on the dialect relationship between telling and keeping information. (Petronio and Caughlin, 2006)
9. One could even state that to act as a performance on stage, as formulated by Goffman (1990), lies closer to the reality than ever before.
10. It is important to underscore that context collision *an sich* does not necessarily indicate a privacy breach. When it is linked to identity, it can develop itself as a privacy problem.
11. When displaying public information, related to a public role like a politician, this does not necessarily have to be the case.
12. Image obtained from www.facebook.com/advertising on May 2012.
13. The authors are aware of the fact that Facebook currently has 900 million users and LinkedIn 161 million, but Twitter numbers were harder to find and we tried to compare these networks for the same period.
14. Twitter and LinkedIn were mapped in May 2011, while Facebook was mapped in September 2011. In preparation of the deliverable, the settings have been reviewed in September 2012. No changes were implemented in any of the three platforms.
15. To keep this diagram readable on one page, we have omitted some of the "on/off" flowchart branches; the default setting is set in bold to keep all information.
16. By this we mean the chance of being found through search engines. This setting has been removed from Facebook with the implementation of Graph Search (Bilton, 2012).
17. Twitter does not attach user information to advertising.

## References


Anon (2011), "Obsessed with Facebook", Online Schools, available at: www.onlineschools.org/blog/facebook-obsession/ (accessed 7 June 2012).

Bilton, N. (2012), "Facebook changes privacy settings, again", *The New York Times*, available at: Facebook Changes Privacy Settings, Again (accessed 22 January 2013).

Boyd, D. (2007), *Why Youth♥ Social Network Sites: The Role of Networked Publics in Teenage Social Life*, John, D. and Catherine, T. (Eds), MacArthur Foundation Series on Digital Media and Learning, Cambridge, pp. 119-142.

Boyd, D. (2008), *Taken Out of Context: American Teen Sociality in Networked Publics*, University of California, Berkeley, CA.

Boyd, D. and Marwick, A. (2011), "Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies", Paper presented at the *Oxford Internet Institute Decade in Internet Time Symposium*, Oxford, September, 22.

Castells, M. (2007), "Communication, power and counter-power in the network society", *International Journal of Communication*, Vol. 1 No. 1, pp. 238-266.

Clarke, R. (1988), "Information technology and dataveillance", *Communications of the ACM*, Vol. 31 No. 5, pp. 498-512.

Cohen, N.S. (2008), "The valorization of surveillance: towards a political economy of Facebook", *Democratic Critique*, Vol. 22 No. 1, pp. 5-22.

Collins, R. (1994), *Four Sociological Traditions*, Oxford University Press, New York, NY.

Coté, M. and Pybus, J. (2007), "Learning to immaterial labour 2.0: MySpace and social networks", *Ephemera: Theory and Politics in Organization*, Vol. 7 No. 1, pp. 88-106.

De Wolf, R. and Pierson, J. (2012), "Symbolic interactionist perspective on linking privacy and identity in social network sites", in ICA, Phoenix, p. 27.

De Wolf, R., Heyman, R. and Pierson, J. (2013), "Privacy by Design through social requirements analysis of social network sites from a user perspective", in Gutwirth, S., Leenes, R. and de Hert, P. (Eds), *European data protection: coming of age*, Springer, Brussels.

Diaz, C. and Gürses, S. (2012), "Understanding the landscape of privacy technologies", *in Information Security Summit, Passau*, p. 6.

Dillet, R. (2012), "Twitter is baking little favors for its advertisers into every change", Techcrunch, available at: http://techcrunch.com/2012/09/18/twitter-changes-are-now-all-about-advertisers-not-the-users/ (accessed 18 September 2012).

Edwards, J. (2012), "Here's what everyone has gotten wrong about Facebook's new ad exchange", *Business Insider*, available at: www.businessinsider.com/facebooks-new-rtb-ad-exchange-is-about-data-not-effectiveness-2012-6 (accessed 21 June 2012).

European Commission (2011), *Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer 359, Conducted by TNS Opinion and Social at the request of Directorate-General Justice, Information Society and Media and Joint Research Centre, Brussels.

Fayyad, U., Piatetsky-Shapiro, G. and Smyth, P. (1996), "From data mining to knowledge discovery in databases", *AI magazine*, Vol. 17 No. 3, p. 37.

Fuchs, C. (2011), "New media, Web 2.0 and surveillance", *Sociology Compass*, Vol. 5 No. 2, pp. 134-147.

Fuchs, C. (2012a), "Dallas Smythe today: the audience commodity, the digital labour debate, marxist political economy and critical theory: Prolegomena to a digital labour theory of value", *tripleC-Cognition, Communication, Co-operation*, Vol. 10 No. 2, pp. 692-740.

Fuchs, C. (2012b), "The political economy of privacy on Facebook", *Television and New Media*, Vol. 13 No. 2, pp. 139-159.

Gandy, O.H. (2003), "Data mining and surveillance in the post-9.11 environment", in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, Vol. 26, Pluto Press, London, p. 41.

Goffman, E. (1990), *The Presentation of Self in Everyday Life*, Doubleday, New York, NY.

Hewitt, J.P. (2007), *Self and Society: A Symbolic Interactionist Social Psychology*, Allyn and Bacon, Boston, MA.

Heyman, R. and Pierson, J. (2011), "Social media use and corporate dataveillance: exploring and assessing digital personal identifiable information (PII) collection tools", in IAMCR 2011, Istanbul, p. 28.

Hildebrandt, M. (2006a), "Privacy and identity", in Claes, E., Duff, S. and Gutwirth, S. (Eds), *Privacy and the Criminal Law*, Intersentia, Antwerp/Oxford, pp. 61-104.

Hildebrandt, M. (2006b), "Profiling: from data to knowledge", *Datenschutz and Datensicherheit-DuD*, Vol. 30 No. 9, pp. 548-552.

Karahasanovic, A., Brandzaeg, P., vanattenhoven, j., Lievens, B., Nielsen, K.T. and pierson, J. (2009), "Ensuring trust, privacy, and etiquette in Web 2.0 applications", *Computer (Special Issue June 09 - Sofware Engineering Ethics)*, Vol. 42 No. 6, pp. 42-49.

King, J., Lampinen, A. and Smolen, A. (2011), "Privacy: is there an app for that?", in Proceedings of the Seventh Symposium on Usable Privacy and Security, p. 12, available at: http://dl.acm.org/citation.cfm?id=2078827.2078843 (accessed 14 January 2013).

Krasnova, H., Gunther, O., Spikermann, S. and Koroleva, K. (2009), "Privacy concerns and identity in online social networks", *Identity in the Information Society*, Vol. 2 No. 1, pp. 39-63.

Livingstone, S., Ólafsson, K. and Staksrud, E. (2011), "Social networking, age and privacy", *EU Kids Online Enhancing Knowledge Regarding European Children's Use, Risk and Safety Online*, available at: http://lenzieprimary.web1.devwebsite.co.uk/_files/social_networking_age_privacy_20111.pdf (accessed 17 June 2012).

Mead, G.H. and Morris, C.W. (1992), *Mind, Self, and Society: from the Standpoint of a Social Behaviorist*, University of Chicago Press, Chicago, IL.

Nissenbaum, H. (2004), "Privacy as contextual integrity", *Washington Law Review*, Vol. 79 No. 1, pp. 101-139.

Norman, D.A. (1998), *Design of Everyday Things*, MIT Press, London.

Norman, D.A. (1999), "Affordance, conventions and design's", *Interactions*, Vol. 6 No. 3, pp. 38-42.

Parr, B. (2011), "Twitter has 100 million monthly active users, 50% log in every day", *Mashable, social media*, available at: http://mashable.com/2011/10/17/twitter-costolo-stats/ (accessed 7 June 2012).

Paul, T., Puscher, D. and Strufe, T. (2011), "Improving the usability of privacy settings in Facebook", *Arxiv preprint arXiv:1109.6046*, available at: http://arxiv.org/abs/1109.6046

Petronio, S. and Caughlin, J.P. (2006), "Communication privacy management theory: understanding families", in Braithwait, D.O. and Baxter, L.A., eds. *Engaging Theories in Family Communication: Multiple Perspectives*, Sage, Thousand Oaks, CA, pp. 35-47.

PrivCO (2012), *Facebook, Inc.*, PrivCO, New York, NY.

Rao, L. (2012), "LinkedIn beats the street, Q1 revenue up 101 per cent to $188.5M; net income up 140 percent", *Techcrunch*, available at: http://techcrunch.com/2012/05/03/linkedin-beats-the-street-q1-revenue-up-101-percent-to-188-5m-net-income-up-140-percent/ (accessed 6 June 2012).

Rappaport, J. (1987), "Terms of empowerment/exemplars of prevention", *American Journal of Community Psychology*, Vol. 15 No. 2, pp. 121-148.

Raynes-Goldie, K. (2010), "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook", *First Monday*, Vol. 15 No. 1, available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

Rosen, J. (2001), "Out of context: the purposes of privacy", *Social Research*, Vol. 68 No. 1, pp. 209-220.

Smythe, D.W. (1977), "Communications: blindspot of western Marxism", *Canadian Journal of Political and Social Theory*, Vol. 1 No. 3, pp. 1-21.

Solove, D.J. (2001), "Privacy and power: computer databases and metaphors for information privacy", *Stanford Law Review*, Vol. 53 No. 6, pp. 1393-1462.

Stutzman, F. (2006), "Facebook's critical success factors", *Fred Stuzman, thoughts about information, social networks, and privacy*. available at: http://fstutzman.com/2006/05/17/facebooks-critical-success-factors/ (accessed 31 May 2012).

Swisher, K. (2011), "Twitter poised to close a two-stage $800m funding, with half used to cash out investors and employees", *All things D*. available at: http://allthingsd.com/20110720/twitter-poised-to-close-a-two-stage-800m-funding-with-half-used-to-cash-out-investors-and-employees/ (accessed 27 November 2011).

Van der Maesen, L.J.G. and Walker, A.C. (2002), *Social Quality: THE Theoretical State of Affair*, European Foundation on Social Quality, Amsterdam.

Verde, A. (2011), "LinkedIn Demographics 2011", available at: www.slideshare.net/amover/linked-in-demographics-and-statistics-2011 (accessed 7 June 2012).

Westin, A. (1970), *Privacy and Freedom*, The Bodley Head, London.

## About the authors

Rob Heyman is a Researcher at SMIT. He has studied six years at the Vrije Universiteit Brussel and got a master's degree in philosophy and communication sciences in 2010. His PhD is part of the EMSOC project (User Empowerment in a Social Media Culture). Rob Heyman is the corresponding author and can be contacted at: roheyman@vub.ac.be

Ralf De Wolf holds a master's in Sociology from the University of Ghent, where he also completed a degree in teaching political and social sciences. He is now working as a PhD researcher within the user research unit of iMinds-SMIT at VUB. His PhD focuses on the social aspects of security and privacy for online social network sites. Key issues are the relationship between identity and privacy and contextual privacy problems.

Jo Pierson has been Researcher and Senior Researcher at SMIT – part of iMinds (Interdisciplinary Institute for Broadband Technology) – since 1996 and holds a PhD in social science (media and communication studies) since 2003. He has been lecturing on undergraduate and masters' courses at the Vrije Universiteit Brussel (Belgium) in the Department of Communication Studies (Faculty of Arts and Philosophy), covering socio-economic issues relating to the information society, digital media marketing and qualitative research methods.