

Online Privacy in Social Media: A Conceptual Exploration of Empowerment and Vulnerability

Jo PIERSON

iMinds SMIT Vrije Universiteit Brussel

Abstract: Current transitions in the media and technology landscape go together with a shift from mass media and personal media to media for 'mass self-communication'. This is illustrated by the way that Web 2.0 or social media (like social network sites and micro-blogging) are becoming commercially engrained in Western everyday life, and the belief that the user is in the driver's seat of socio-technical innovation. However we observe a paradox. On the one hand the instruments and means for empowering users through social media are proliferating, reinforcing the idea of users effectively becoming empowered. On the other hand we find that empirical evidence about what user empowerment really consists of is too a large extent missing and that a risk of denial of the empowerment downside exists. After all if we indeed find opportunities for user empowerment, also the counterpart of disempowerment is at stake. The latter is particularly visible in the relation between social media, empowerment and privacy. In this paper we take a closer look at how people's disempowerment and vulnerability is being reconfigured within the changing media landscape of mass self-communication. To illustrate these transitions, we focus on issues of privacy in relation to social media. In particular we take a critical view on how vulnerability takes shape in online consumer privacy. For this we first discuss the notions of mass self-communication, empowerment and privacy more generally. Next we highlight to what extent privacy for consumers using social media is different and how their vulnerability changes from an external and internal perspective. The transition from the classic view on privacy to online privacy to online consumer privacy illustrates that the notion 'privacy' needs to be rethought. The paper is based on a literature review to deconstruct and explore the key concepts empowerment, disempowerment, vulnerability and privacy in relation to mass self-communication and social media.

Key words: social media, privacy, surveillance, empowerment, vulnerability.

■ ICT, internet and social media

Media and Information and Communication Technologies (ICT) are undergoing substantial changes, based on socio-economic transitions and digitisation. This goes hand in hand with an intensified process of convergence between the formerly strictly separated sectors of audiovisual media, telecommunication and computer industry. The traditional one-way broadcasting media landscape turns into a converged media ecosystem,

transformed by Internet 2 based technologies and applications (PASCU, OSIMO, ULBRICH, TURLEA & BURGELMAN, 2007). One of the highly visible outings is the proliferation of information and communication technologies (ICT) like 'social media', also denoted as 'Web 2.0' (O'REILLY, 2005), 'participative web' (VICKERY & WUNSCH-VINCENT, 2007) or 'social computing' (PASCU, 2008).

The general belief is that this shift in ICT, from unidirectional to conversational media (SPURGEON, 2008) has lowered the technological thresholds for everyday users to cooperate for their own benefit (SAVERI, RHEINGOLD & VIAN, 2005), to participate in online environments and social network sites (BOYD & ELLISON, 2007), to co-create business value (PRAHALAD & RAMASWAMY, 2004) and possibly to become 'prosumers' or producing users (BRUNS, 2008; TOFFLER, 1980). Another characteristic of social media is that it promises to enable user-centric, collaborative knowledge sharing, community-building activities using the internet (PUNIE, LUSOLI, CENTENO, MISURACA & BROSTER, 2009). This discourse has created expectations on new opportunities for user empowerment in different societal arenas of everyday life.

In line with critical scholars like VAN DIJCK & NIEBORG (2009), VAN DIJCK (2009) and FUCHS (2010), we are aware that these changes in the internet landscape and the claims made on agency and societal impact are often overrated. We also acknowledge that the discourse on these transitions is framed by the celebrative manifestos and management books that favoured the internet industry being in a downturn after the bubble burst at the end the 1990. ¹ Nevertheless we cannot overlook that these new media and internet are becoming an integrated part of everyday life in major parts of Western society (HAYTHORNTHWAITE & WELLMAN, 2002), and in some countries we see that commercial internet media are fully domesticated. DEUZE (2012) frames this as 'media life', where we are increasingly living 'in media' instead of 'with media'. This perspective also fits in the idea of 'mediation' stating that "mediated connection and interconnection" are part of the infrastructure of most people's lives in the internet age (MANSELL, 2012; SILVERSTONE, 2006). The role and relevance of social media is thus framed as a contradictory phenomenon that - like any socio-technical system - does not have a one-dimensional

¹ Typical examples of these manifestos and management books are *The Cluetrain Manifesto* (LEVINE, LOCKE, SEARLS & WEINBERGER, 2001), *Wikinomics* (TAPSCOTT & WILLIAMS, 2007), *Groundswell* (LI & BERNOFF, 2008), *Here Comes Everybody* (SHIRKY, 2008) and others.

effect, but complex interconnected effects (FUCHS, 2012a: 5; FUCHS, 2008). This is particularly visible in the way that communication is happening via internet, where increasingly complex and rich ways of interaction between people are enabled by social media applications like (micro) blogging, wiki, podcasting, social tagging, online social gaming, and in particular through social network sites (SNS). Especially the latter web platforms (e.g. Facebook, LinkedIn, MySpace, ...) receive a lot of attention for the moment, which are typically defined as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site" (BOYD & ELLISON, 2007).

In line with the work by CASTELLS (2009), we find how current transitions in the media and technology landscape go together with a shift from mass media and personal media to media for 'mass self-communication'. CASTELLS (2009: 55) sees the latter as the new kind of communication in contemporary society. On the one hand mass communication because social media can potentially reach a worldwide internet audience. On the other hand 'self-communication' because the message production is typically self-generated, the potential receiver(s) definition is self-directed and the message or content retrieval is self-selected. However the different forms of communication (mass media, interpersonal communication and mass self-communication) complement rather than substitute each other.

The notion of 'mass self-communication' indicates well the techno-dialectic changes taking place in communication and media production, diffusion and consumption, on macro and micro level. Castells situates the current ICT landscape as a struggle between the global multimedia business networks attempting to commodify the internet and the unprecedented autonomy for communicative subjects to communicate at large, labelled as the creative audiences or users.² On the one hand he states that the potential autonomy is shaped, controlled, and curtailed by the growing concentration and interlinking of corporate media and network operators on a global scale (CASTELLS, 2009: 135). On the other hand ARSENAULT & CASTELLS (2008) stress that the greater communicative autonomy of the

² As indicated by FUCHS (2009), there is however no clear definition of the notion of 'autonomy'.

media consumers could help them to become media citizens, and thus restore the balance of power vis-à-vis their would be controllers. In this regard the rise of mass self-communication also intensifies the move towards 'networked individualism' where the individual person becomes the portal or hub for different networks around him or her (HAYTHORNTHWAITE & WELLMAN, 2002). This gives media consumers a lot of freedom and leverage in how, when, what and with whom communication takes place. However at the same time the increased level of individual control often implies more responsibilities given the possible heavier consequences.

■ Empowerment/disempowerment

These pros and cons are linked to notions of respectively 'user empowerment' and 'user disempowerment'. 'Empowerment' is a widely used concept charged with meaning. It has a long tradition in social welfare and civil society literature, but also in science, business and policy fields.

In a general sense empowerment is defined as "enabling people to control their own lives and to take advantage of opportunities" (van der MAESEN & WALKER, 2002: 6) or in other words "a process, a mechanism by which people, organisations, and communities gain mastery over their affairs" (RAPPAPORT, 1987: 122). In this way it refers to the capacity of individuals, communities and/or groups to access and use their personal/collective power, authority and influence, and to employ that strength when engaging with other people, institutions or society (PUNIE, 2011; PAGE & CZUBA, 1999) see empowerment as a multi-dimensional social process that helps people gain control over their lives. It is a process that fosters power in people for use in their lives, in their communities and in their society, by acting on issues they define as important.

In this article we apply the notion within the domain of media and ICT from an interdisciplinary perspective. This is the only perspective which can give a more truthful insight as "no single perspective offers a complete explanation of the evolution of the communication system in the information society" (MANSELL, 2012: 29). In particular 'privacy' is a multi-disciplinary issue that has been and should be analysed from various perspectives (HUI & PNG, 2006). Different levels of empowerment can be identified regarding ICT, in particular on an individual level and on a community level. However,

we prefer to take an integrated perspective, the so-called social-ecological approach. This is defined as: "the interaction between people and their environment, based on mutual respect and critical reflection, by which individuals as well as controlling institutions change in such a way that individuals get a bigger influence on people and institutions that prevent them from acquiring an equal position in society" (Translated from Dutch, DELAHAIJ, 2004: 16).

When applying this perspective of empowerment in context of mass self-communication and social media, we start from the following citation by Robin Mansell:

"[...] the implications of the new media are contradictory. Once connected, there are no grounds for simply assuming that citizens will be empowered to conduct their social lives in meaningful ways. There is, therefore, a growing need to examine whether the deployment of new media is consistent with ensuring that the majority of citizens acquire the necessary capabilities for interpreting and acting upon a social world that is intensively mediated by the new media." (MANSELL, 2002: 409)

The notion of 'capabilities' refers here to the work of welfare economist Amartya SEN (1999), where he starts from a normative egalitarian view by stating that people have certain entitlements in the welfare state. According to Sen one should focus on the 'functionings', defined as the various things people value doing or being. They differ from very elementary ones like being healthy, having a job, being well educated or having an adequate income, to more complex ones like work satisfaction, achieving self-respect, being happy or taking part in the life of the neighbourhood. 'Capabilities' are understood as the functionings that a person is actually able to achieve. Capabilities in this sense are the underpinning of the freedom of people to construct meaningful lives. We thus define user empowerment in relation to social media as the capability for interpreting and acting upon the social world that is intensively mediated by mass self-communication.

In the mass self-communication realm, with the proliferation of social media tools, three main issues are at stake in order to be empowered or – the flip side – not to become disempowered: inclusion, literacy and privacy.

- First, there is no automatic link between social media and user empowerment as not all users are able, willing or even permitted to get involved and participate by means of or through digital media. This refers to the issues of access, digital inclusion, infrastructure and regulation.

- In addition, we need to be aware that not all users are capable of getting as involved with these media technologies as they would like to be, referring to the issue of digital media literacy.

- Third, even if they have access and are (social) media literate, the question remains to what extent users are self-reflexive and sufficiently aware of changing privacy and surveillance aspects, i.e. how their digital activities are being monitored, processed, analysed and commodified by third parties.

So – referring to our earlier definition – empowering people in the context of mass self-communication means enhancing the capabilities of genuinely understanding and acting upon the social world by social media, on the levels of inclusion, digital literacy and privacy. However we observe a paradox. On the one hand the instruments and means for mass self-communication by users through social media are proliferating, reinforcing the idea of users effectively becoming empowered. On the other hand we find that empirical evidence about what user empowerment really consists of is to a large extent missing and a risk of denial of the empowerment downside exists (VAN DIJCK, 2009). After all if we indeed find opportunities for user empowerment, also the counterpart of disempowerment is at stake. The latter means that the social world intensively mediated by mass self-communication creates (new) circumstances of vulnerability where people do not always have the necessary capabilities to optimally interpret and act upon other people and institutions for acquiring an equal position in society. This risk of disempowerment is particularly visible in relation to issues of social media, privacy and surveillance, which is therefore the focus of this article.

■ Vulnerability

As mentioned before the unprecedented autonomy of media consumers and hence increased self-directed control over time, place and content of communication and interaction with many more people, increases the chance of negative (but also positive) consequences and implies more responsibilities. There is for example a substantial chance that online user practices via social media are more persistent in time, have a broader geographical reach and are picked up by unwanted receivers. This means that the 'vulnerability' of people engaging in mass self-communication changes and possibly increases, which intensifies the need for

empowerment and aggravates the risk of disempowerment. Where vulnerability defines the circumstances of potential risk as they are, disempowerment refers to people actually losing power and capabilities to gain control over their lives mediated by social media. We now further elaborate on the notion of vulnerability.

The concept of 'vulnerability' (and its opposite 'security') has been intensively discussed in the studies on human development, geography, disaster reduction, and risk communication (VILLAGRAN, 2006). It is often - wrongfully - equalled with 'poverty', but it in fact has (or can have) a much broader meaning. We can also apply this broader notion in the field of media and communication studies. However vulnerability has not yet a developed theory and accepted indicators and methods of measurement. Though CHAMBERS (1989/2006) sees an external side of vulnerability related to 'exposure' (see also BALL, 2009: 647) and an internal side related to 'coping capacities'. WATTS & BOHLE (1993) and BOHLE (2001) have further expanded this differentiation, keeping the structure of external and internal sides of vulnerability. They have defined vulnerability as a multi-layered and multi-dimensional social space defined by the political, economic, and institutional capabilities of people in specific places and times. The external perspective refers mainly to the structural dimensions of vulnerability exposure, while the internal dimension of vulnerability focuses on coping and action to overcome or at least mitigate negative effects (BOHLE, 2001).

This twofold approach of vulnerability is also reflected in the way social media technologies have been approached from a social constructivist perspective, confronting the structural element of 'affordances' with the action-oriented element of 'practices'. Exposure to vulnerability results from the 'affordances', defined as the combination of perceived and actual properties of the (social media) technology, primarily those fundamental properties that determine just how that technology could possibly be used (PIERSON *et al.*, 2006; NORMAN, 1988). Coping with vulnerability happens in the 'practices', defined as 'recognisable entities', but at the same time "require constant and active reproduction or performance" (HAND, SHOVE & SOUTHERTON, 2005). In this way a 'practice' is seen as a routinised type of behaviour. From a social constructivist perspective there is no essential use to be derived from the technological (social media) artefact itself, because technologies should be studied in their context of user practices and users and technologies should be seen as co-constructed (OUDSHOORN & PINCH, 2003). We use the structure of external and internal sides of vulnerability and the related affordances and practices of social media, for our further analysis. For this we take a closer look at how

people's vulnerability and disempowerment are reconfigured within the changing media landscape of mass self-communication. To illustrate these transitions, we focus on privacy in relation to social media. More in particular we take a critical view on how vulnerability takes shape in online consumer privacy. For this we first discuss the issue of privacy more generally. Next we highlight to what extent privacy for consumers of social media is different and how their vulnerability changes from an external and internal perspective.

■ Exploring online privacy of social media consumers

The notion of privacy becomes prominent at the end of the 19th century, more in particular in the legal academic literature in the US. In their seminal article WARREN & BRANDEIS (1890) define privacy as "the right to be left alone". Soon after that this right was taken up in law texts and regulation by a range of international and national bodies, like in the European Convention on Human Rights (ECHR), the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the OECD, and in the European regulation (e.g. the Data Protection Directive 95/46/EC and the e-Privacy Directive 2002/58/EC being revised for the moment). However, the legal protection of a person against infringements of his or her privacy is only a minimum requirement which needs to be fulfilled. In addition other norms and rules can prevail. For example bodies in different sectors can install separate and more stringent self-regulation and co-regulation guidelines.

Online consumer privacy

Given their prominence we foremost discuss for-profit social media, that for their income depend on advertising or commercial services. These are web platforms such as Facebook, YouTube, Last.fm, Blogger, Flickr, Twitter, Netlog, Digg, etc. In this type of mass self-communication the users are by definition also consumers, because – in return for using the online services – they pay with their personal data, the user-generated content and their attention to advertising - like online banners. (BERMEJO, 2009; SMYTHE,

1977).³ This kind of commercial give-and-take is not necessarily a problematic issue. It can be a fair deal between the social media user and the commercial social media service, as long as each party in the deal clearly understands the context and the terms of condition, supporting an informed consent. However more often than not, the users are not really aware of what kind of deal is struck and how to possibly alter the conditions (GRABER, D'ALESSANDRO & JOHNSON-WEST, 2002; McDONALD & CRANOR, 2009). Therefore it is important to pay sufficient attention to the issue of consumer privacy in a digital environment and how this is part (or not) of the broader commodification and trade-off in social media.

There have been many studies that investigate the trade-off benefits and costs associated with the processing of personal information and respect for privacy, in particularly in the field of economics of privacy (BAUER, KORUNOVSKA & SPIEKERMANN, 2012; ACQUISTI, 2010; HUI & PNG, 2006). Most of these studies are part of the administrative or instrumental social science research tradition. Our framework starts from the critical tradition in Science and Technology Studies (STS) where: "[...] attention is drawn to the potential of innovations in technologies to be associated with people's empowerment and their disempowerment, depending on the extent to which they are able to master or control the innovation process" (MANSELL, 2012: 37). The latter perspective of linking online privacy with vulnerability and empowerment, has received much less attention in research on social media.

Therefore after having sketched some broad characteristics how privacy is changing in relation to consumers of commercial social media applications, we now aim to better understand how this could affect the consumer empowerment. More in particular we turn to the ways in which the vulnerability of these consumers is changing and hence also the possible risks of disempowerment. As mentioned before 'vulnerability' has an external side of 'exposure' and an internal side of 'coping'. Each side has specific characteristics when coupled with mass self-communication.

³ We could also use the well-know quote: "If you are not paying for it, you're not the customer; you're the product being sold" by Andrew Lewis aka blue_beetle on MetaFilter (<http://www.metafilter.com/95152/Userdriven-discontent#3256046>).

External side of vulnerability: social media affordances of exposure

Part of the typical affordances of social media is that the thresholds for more and other types of personal data becoming publicly diffused, are lowered. This is demonstrated by the fact that mass self-communication increases exposure by opening up private domains which in the past were much more difficult to access. This kind of disclosure of private information can happen explicitly because it is part of the action: sharing, liking, tweeting and filling in user generated content (UGC). But, other information is captured apart from explicit communication actions, it is gathered implicitly. Common examples are mouse clicks, browsing behaviour, operating system and browser information (PIERSON & HEYMAN, 2011). A more accurate way to conceptualise these two types of exposure is linking them to the ability of managing an identity vis-à-vis other users (BOYD, 2007) (privacy as subject perspective) and to the surveillance perspective wherein users are reduced to data (GANDY, 2003) (privacy as object perspective). 'Privacy as subject' sees users as actors that provide personal information in order to form and manage their identity. It is not just the information flow as such, but also about using this information for creating meaning in a social context (DE WOLF *et al.*, 2012). 'Privacy as object' is related to the historical need to process large amounts of data, to what happens with data and how these processes objectify users in two ways: they are reduced to a fixed identity and their online data are being surveilled and commodified, often unknowingly (HEYMAN, DE WOLF & PIERSON, 2012). We exemplify these two different types of the exposure side of vulnerability related to social media.

The most visible type of disclosure is happening on an explicit way in the case of 'privacy as subject'. The explicit exposure is done by people themselves by making details of their private life openly available via all kinds of social media applications, especially SNS. As more and more people are consciously putting personal information online, of themselves and of others, the 'digital footprint' of these individuals has been growing steadily over the last couple of years. However a US study found that 60% of internet users are not worried at all about the amount of personal information that is accessible online (MADDEN, FOX, SMITH & VITAK, 2007).

Yet these revelations increase the vulnerability to the extent that the disclosure of personal data and the interactions that follow, do not happen at the users' discretion. There are many popular accounts in news media, replicated in research papers, of 'unexpected' and 'regrettable' disclosures that cross the different contexts of home, work and school: old pictures being

harmful for job chances, disclosing cheating during exams to school teachers, partners discovering adultery, tax authorities discovering undeclared belongings, unwanted contacts etc. All this can lead to risk of collapsed contexts, stalking, reputation damage, losing a job, cyberbullying, divorce, blackmailing, and other harmful events. Danah BOYD (2011) has identified four affordances that characterise the external vulnerability in so-called 'networked publics', in contrast to un-mediated publics: (1) scalability (i.e. social media content can become very visible in an easy way), (2) replicability (i.e. online content can be easily duplicated and copied to another context, making it unable to discern the original from the duplicate), (3) persistence (i.e. online expressions are automatically recorded and stored indefinitely, lasting for a long time), and (4) searchability (i.e. more personal content can be retrieved through search which was not the case in unmediated publics). The latter characteristics hold the social risk of destabilizing core assumptions people make when engaging in social life (FARINOSI, 2011; GUERSES & PIERSON, 2012). Yet at the same time these affordances can help people in new ways of identity construction or "writing oneself into being" (BOYD, 2008).

Besides the explicit exposure of personal data, we increasingly also find implicit ways in the case of 'privacy as object', mainly initiated by producers and suppliers of (commercial) websites. Each internet user leaves traces or footprints, and very often the user is not aware of these traces. The traces include personal data and transaction data about browsing and communication behaviours on social media. In a commercial setting this type of online information can be sold as a commodity to advertising clients, data warehouses and other marketing companies. In this way the working of social media is based on the collection, storage, usage, and analysis of a large amount of personal and transaction data (FUCHS, 2012a, 2012b). Hence consumer tracking is becoming the new foundation of the online advertising economy with a spending of \$23 billion in 2009. Research by AT&T Labs and Worcester Polytechnic Institute in 2010 has found tracking technology on 80% of 1,000 popular sites, which is up from 40% of these sites in 2005 (ANGWIN, 2010). There is a whole array of tracking tools to scrutinise, analyse and categorise the behaviour of internet users. Well-known examples are the use of recommendation systems, cookies, profiling, online behavioural advertising, deep packet inspection (DPI) and data mining (PIERSON & HEYMAN, 2011; McSTAY, 2011).

The vulnerability aspect relates to the issue of surveillance linked to computing and social media, also denoted as 'dataveillance'. This is the "systematic monitoring of people's actions or communications through the

application of information technology" (CLARKE, 1991). Digitisation and networking have changed surveillance and have made people more vulnerable (LYON, 1994: 51-52). GANDY (1993) talks about the 'panoptic sort', which he defines as: "a difference machine that sorts individuals into categories and classes on the basis of routine measurements" (GANDY, 1993: 15). LYON (2003) introduces the idea of 'social sorting' when linking the panoptic sort to computers and internet :

"The surveillance system obtains personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access, and so on" (LYON, 2003: 20).

GANDY (2002) also analysed data mining as a form of panoptic sorting, where DANNA & GANDY (2002) highlight some fundamental concerns about fairness and distributive justice regarding price discrimination, weblining and marketing discrimination. Price discrimination can lead to exclusion, often without the customer knowing. In a report on the surveillance society WOOD (2006: 44) observes that consumers have thus become increasingly vulnerable within the personal information economy.

The two perspectives of privacy as subject and privacy as object show how exposure as the external side of vulnerability can take shape. These kinds of exposure can offer significant opportunities regarding identity construction or for receiving more personalised (commercial) goods and services. However simultaneously the current architecture of internet and social media enabling these increased forms of exposure can create a world where people are more vulnerable to harm. Solove even talks about 'architectures of vulnerability':

"If we view certain privacy problems as architectural, we begin to see how the design and structure of information flows affect movement, communication, association, and other fundamental practices in a free and democratic society" (SOLOVE, 2003).

Internal side of vulnerability: social media practices of coping

The internal side of vulnerability refers to the ways that consumers are able (or not) to harness themselves against vulnerability in their everyday social media practices. Here we look at the specificities of privacy practices by consumers. Like the general concept of privacy, also the notion of consumer privacy covers many different views and concerns. In order to

better situate and understand the levels on which consumers can develop coping capacities to mitigate their vulnerability regarding (online) privacy, we need to take into account two central aspects: control and consumer knowledge (LANIER & SAINI, 2008).

First of all there is the control the media consumer has (or not) on the information that is disclosed about himself. GOODWIN (1991: 152) makes a difference between two types of control in relation to consumer privacy:

"(...) the consumer's ability to control (a) presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present."

If a consumer is not able to control who is present or who can approach him, he senses a breach of relational privacy (WALRAVE, 2002). This presence can be physical, like being unexpectedly approached by a sales person in a shopping mall for promoting a product or service. However this type of privacy also refers to mediated forms of contact via (new) media, like being called by telemarketers in the evening or receiving spam in your personal e-mail box. There are different national initiatives to empower consumers in better controlling their relational privacy, like the initiative by the Dutch consumer organisation to make consumers more literate about the kind of psychological tricks that are used in telemarketing. They developed an audiovisual digital self-training exercise to support consumers to not be misguided too easily.⁴ Initiatives related to mediated forms of contact are for example the UK Mailing Preference Service (MPS) list, the US National Do Not Call Registry or the Belgian Robinson list. This is a list of people who do not want to receive specific types of marketing transmissions, but it can also inform a business which types of communication are welcome. A similar self-regulatory initiative has been taken in the online field in the US. At the end of 2010 the Federal Trade Commission (FTC) proposed adding a 'do not track' (DNT) option to internet browsers, so that consumers could control if they wanted to be followed by advertisers (NN, 2012).

Another type of consumer control is the control over information obtained during market transactions by others not present during the original transaction. We notice an increasing importance for this type of informational privacy breaches, given the growing prominence of ICT in marketing and

⁴ <http://www.consumentenbond.nl/actueel/nieuws/nieuwsoverzicht-2010/Telefonische-verkooptrucs-ontrafeld> (last time consulted on 20 October 2012).

consumer research. This is typically linked to implicit exposure of personal data that we find in the 'privacy as object' perspective (see above). The information on the consumer and the transactions are stored in databases and further processed and diffused, with or without consulting the consumer. Typical examples are information bits related to personal and transaction data generated by electronic payments, the use of loyalty cards in supermarkets, filling in personal information for receiving a coupon, consulting a website, etc. From the supply side this presumes transparency in the aims of collecting, processing and commercialising of consumer data, which needs to be made explicit in a clear privacy statement (e.g. on a website). This type of consumer control is also central in the debate concerning opt-in (consumers giving explicit permission to use personal data for commercial purposes) and opt-out (the right to oppose the use or re-use of personal data). In the sphere of networked publics the audience is often invisible (BOYD, 2011). This is not only true for online friends, but also for the 'audience' receiving information from social media use and interactions, but not present during the original transaction. A familiar example is the internet cookie. We found that the use of cookies has increased substantially over the years and that they are often obfuscated by website owners, third parties and browser manufacturers to keep them out of sight (PIERSON & HEYMAN, 2011). This means that extra effort is required to create transparency around the ways that the personal and transaction data are collected, stored, used, analysed, and monetised. Only in this way the empowerment of consumers can be sufficiently strengthened.

In order to exercise the control, there is a second central aspect that is essential for consumer privacy is the consumer knowledge (LANIER & SAINI, 2008: 16). This refers to the degree to which consumers are literate about and understand data collection of the companies with which they interact, as well their related privacy rights (FOXMAN & KILCOYNE, 1993: 107). For example to manage one's privacy on an SNS like Facebook, one needs to navigate through 50 settings with more than 170 options.⁵ BOYD & HARGITTAI (2010) found that technological knowledge and familiarity definitely matter when looking at how people approach the privacy settings of their Facebook accounts, given the relationship between adjusting privacy settings and frequency of use as well as skills. They conclude that:

⁵ <http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html?ref=personaltech> (Facebook privacy settings on 20 October 2012).

"This is particularly significant when we consider the role of default settings. If those who are the least familiar with a service are the least likely to adjust how their account is set up regarding privacy matters then they are the most likely to be exposed if the default settings are open or if the defaults change in ways that expose more of their content. This suggests that the vulnerability of the least skilled population is magnified by how companies choose to set or adjust default privacy settings." (BOYD & HARGITTAI, 2010).

Hence it is more and more a challenge for the average consumer to be well informed and to gather sufficient knowledge to cope with his or her online privacy vulnerability.

Further research

Based on this conceptual exploration of changing perspectives in online consumer privacy and social media, the next step is to further operationalise and substantiate the conceptual framework of empowerment and disempowerment based on the vulnerability issues. For this we are further developing and applying the notions of 'privacy as subject'⁶ and 'privacy as object'⁷ by way of interdisciplinary research from an STS perspective, integrating media and communication studies methods with computer science - requirement engineering in security and privacy (GUERSES & PIERSON, 2012). Inspired by the steps taken in a typical Technology Assessment (TA) process (SMIT & van OOST, 1999), this means that we first identify the particular technological surveillance affordances of the social media tools and the possible consequences these can have on people and society (HEYMAN & PIERSON, 2011). Next we gather the perspectives and practices of the different stakeholders linked with the particular social media technology, like marketing industry, policy makers and especially consumers (DE WOLF & PIERSON, 2012; HEYMAN & PIERSON, 2012). Finally we aim to inform and possibly steer the technological design of Privacy Enhancing Technologies (PET), in order to avoid negative consequence and to further positive outcome. This approach fits in with the notion of 'privacy by design',

⁶ 'Privacy as object' is our key empirical research topic in the Flemish EMSOC project (User Empowerment in Social Media Culture) in Belgium (www.emsoc.be), a four-year Strategic Basic Research project (SBO) by three universities funded by the IWT (government agency for Innovation by Science and Technology) (2010-2014).

⁷ 'Privacy as subject' is our key research topic in the Flemish SPION project (Security and Privacy for Online Social Networks) in Belgium (www.spion.me), a four-year project in the SBO programme by four universities, funded by IWT (2011-2014).

referring refers to the philosophy and approach of embedding privacy into the design specifications of various technologies (CAVOUKIAN, 2009; DE WOLF, HEYMAN & PIERSON, 2012).

■ Conclusion

Rheingold argues that the new network technologies available today that open "new vistas of cooperation also make(s) possible a universal surveillance economy and empower[s] the bloodthirsty as well as the altruistic" (RHEINGOLD, 2002: xviii). We have explored how the vulnerability of people is changing in relation to online consumer privacy when engaging with new network technologies of mass self-communication. Consumers are possibly disempowered by new and extended ways of exposure, linked to the affordances of social media from a 'privacy as subject' perspective (cf. scalability, replicability, persistence and searchability) as well as a 'privacy as object' perspective (cf. dataveillance and social sorting). Besides the external side of vulnerability, also the internal side can create a need for empowerment. Especially as we observe that the ways to cope with vulnerable privacy situations are becoming increasingly complex. At the same time industry is heavily investing in ways to maximise the commodification of social relations via mass self-communication. It is in their interest to lower the thresholds for access to personal data and loosen privacy measurements.

The use of social media and in particular SNS shows the difficulty of getting control over and fully understanding your personal mediated communication. In order to better harness consumers and develop coping capacities, we foremost need to strengthen the digital (consumer) literacy on the level of understanding privacy and personal data. The question is then what consumers can or should do to empower themselves in the rapidly changing digital media landscape. It is important that internet users are aware of what happens (or can happen) with their personal data being explicitly or implicitly available via social media. First of all people need to take into account that everything that is disclosed online, will possibly stay online and have a global reach. Second one can never be certain that only the audience for whom the message was meant, will get to see it. Third there is always the risk that people or organisations will use their personal information for other purposes of which they were not (sufficiently) aware. And fourth one needs to know that explicit and implicit private data can be

the subject of further analysis by means of cookies, profiling and data mining.

Future research needs to take a critical look at the differences on the micro-level of everyday user practices between various consumers and consumer groups. This not only means investigating what consumers are able to do, but also what they know, what their preferences are and what they effectively do. The outcome should be matched with the technological affordances and industry developments with regard to new techniques for tracking and exposing online consumer behaviour. Only in this way we can take the necessary actions on the level of awareness raising, educational tools and policy action, in order to keep privacy as a normal good, so as a good that everyone may afford or even as a public good (PAPACHARISSI, 2010).

References

- ACQUISTI, A. (2010): "The economics of personal data and the economics of privacy", paper presented at Joint WPISP-WPIE Roundtable: The Economics of Personal Data and Privacy - 30 Years after the OECD Privacy Guidelines, 1 December 2010, Paris (France).
- ANGWIN, J. (2010, 30 July): "The web's new gold mine: your secrets", *The Wall Street Journal*.
- ARSENAULT, A. H. & CASTELLS, M. (2008): "The Structure and Dynamics of Global Multi-Media Business Networks", *International Journal of Communication* (2), 707-748.
- BALL, K. (2009): "Exposure: exploring the subject of surveillance", *Information, Communication and Society*, 12 (5), 639-657.
- BAUER, C., KORUNOVSKA, J. & SPIEKERMANN, S. (2012): On the value of information: what Facebook users are willing to pay (Paper 197). Paper presented at European Conference on Information Systems (ECIS) 2012'2012, Barcelona (Spain).
- BERMEJO, F. (2009): "Audience manufacture in historical perspective: from broadcasting to Google", *New Media & Society*, 11 (1&2), 133-154.
- BOHLE, H.-G. (2001): "Vulnerability Article 1: Vulnerability and Criticality", *IHDP Newsletter* UPDATE.
- BOYD, D. M.:
- (2008): *Taken Out of Context - American Teen Sociality in Networked Publics* (Ph.D. thesis), Berkeley: University of California, 393.
 - (2011): "Social network sites as networked publics: affordances, dynamics, and implications", in Z. PAPACHARISSI (Ed.) *A networked self: identity, community, and culture on social network sites*, New York: Routledge, 39-58.

BOYD, D. M. & ELLISON, N. B. (2007): "Social network sites: Definition, history, and scholarship", *Journal of Computer-Mediated Communication*, 13 (1).

BOYD, D. M. & HARGITTAI, E. (2010): "Facebook privacy settings: who cares?", *First Monday*, 15 (8).

BRUNS, Axel (2008): *Blogs, Wikipedia, Second life, and Beyond: from production to produsage*, New York; Oxford: Peter Lang.

CASTELLS, M. (2009): *Communication power*, Oxford: Oxford University Press.

CAVOUKIAN, A. (2009): *Privacy by design: take the challenge*, Toronto: Information and Privacy Commissioner of Ontario Canada.

CHAMBERS, R. (1989/2006): "Vulnerability, coping and policy (Editorial introduction)", *IDS Bulletin*, 37 (4), 33-40.

CLARKE, R. (1991): "Information Technology and Dataveillance", in C. DUNLOP & R. KLING (Eds.), *Controversies in Computing*, New York: Academic Press.

DANNA, A. & GANDY, O. H. (2002): "All that glitters is not gold: digging beneath the surface of data mining", *Journal of Business Ethics*, 40, 373-386.

DE WOLF, R. & PIERSON, J. (2012): "Privacy beyond the individual: analyzing group based access control models on social network sites from a user perspective", paper presented at Communication Policy and Technology section for IAMCR Conference 'South-North Conversations', 15-19 July 2012, Durban (South-Africa).

DE WOLF, R., HEYMAN, R. & PIERSON, J. (2012): "Privacy by Design through social requirements analysis of social network sites from a user perspective", paper presented at 5th International Conference CPDP (Computers, Privacy and Data Protection), 25-27 January 2012, Brussel (Belgium).

DELAHAIJ, R. (2004): "Dossier empowerment: empowerment methoden bij allochtone jongeren", Utrecht: FORUM: Instituut voor multiculturele ontwikkeling.

DEUZE, M. (2012): *Media life*, Cambridge: Polity Press.

FARINOSI, M. (2011): "Deconstructing Bentham's panopticon: the new metaphors of surveillance in the Web 2.0 environment", *TripleC*, 9 (1), 62-76.

FOXMAN, E. R. & KILCOYNE, P. (1993): "Information technology, marketing practice, and consumer privacy: ethical issues", *Journal of Public Policy & Marketing*, 12 (1), 106-119.

FUCHS, Christian:

- (2008): *Internet and society: social theory in the information age*, London: Routledge.

- (2009): "Some reflections on Manuel Castells' book *Communication Power*", *TripleC*, 7 (1), 94-108.

-
- (2010): "Social Software and Web 2.0: Their Sociological Foundations and Implications", in S. MURUGESAN (Ed.), *Handbook of Research on Web 2.0, 3.0, and X.0: Technologies, Business, and Social Applications* (Vol. II), Hershey, PA: IGI-Global, 764-789.
 - (2012a): *Internet and surveillance: the challenges of Web 2.0 and social media*, New York: Routledge.
 - (2012b): "The political economy of privacy on Facebook", *Television & New Media*, 13 (2), 139-159.

GANDY, O. H.:

- (1993): *The panoptic sort: a political economy of personal information*, Boulder, Colo: Westview.
- (2002): "Data mining and surveillance in the post-9.11 environment", paper presented at International Association for Media and Communication Research'2002, Barcelona (Spain).

GOODWIN, C. (1991): "Privacy: recognition of a consumer right", *Journal of Public Policy & Marketing*, 10 (1), 149-166.

GRABER, M. A., D'ALESSANDRO, D. M. & JOHNSON-WEST, J. (2002): "Reading level of privacy policies on internet health Web sites", *Journal of Family Practice*, 51 (7), 642-645.

GUERSES, S. & PIERSON, J. (2012): "Requirement engineering meets social sciences: re-wiring socio-technical systems for tackling privacy and responsabilization", paper presented at Political Economy section for IAMCR Conference South-North Conversations, 15-19 July 2012, Durban (South-Africa).

HAND, M., SHOVE, E. & SOUTHERTON, D. (2005): "Explaining Showering: a Discussion of the Material, Conventional, and Temporal Dimensions of Practice", *Sociological Research Online*, 10 (2).

HAYTHORNTHWAITE, C. A. & WELLMAN, B. (2002): "The internet in everyday life", in B. WELLMAN & C. A. HAYTHORNTHWAITE (Eds.), *The internet in everyday life is this meant to be written twice?*, Oxford: Blackwell, 3-41.

HEYMAN, R. & PIERSON, J.:

- (2011): "Social media use and corporate dataveillance: exploring and assessing digital Personal Identifiable Information (PII) gathering tools", paper presented at Communication Policy & Technology section for IAMCR Conference 'South-North Conversations', 13-17 July 2011, Istanbul (Turkey).
- (2012): "Profiling the profilers: analysing the gathering and mining of personal data for online marketing purposes based on Privacy Impact Assessment approach", paper presented at Amsterdam Privacy Conference (APC) 2012, 7-10 October 2012, Amsterdam (The Netherlands), 25.

HEYMAN, R., DE WOLF, R. & PIERSON, J. (2012): "Not all privacy settings are created equal: evaluating social media privacy settings for personal and advertising purposes", paper presented at Political Economy section for IAMCR Conference 'South-North Conversations', 15-19 July 2012, Durban (South-Africa).

HUI, K.-L. & PNG, I.P.L. (2006): "The economics of privacy", in T. HENDERSHOTT (Ed.), *Handbooks in Information Systems* (Vol. 1), Amsterdam: Elsevier, 471-498.

LANIER, C. D. Jr. & SAINI, A. (2008): "Understanding consumer privacy: a review and future directions", *Academy of Marketing Science Review*, 12 (2), 1-45.

LEVINE, R., LOCKE, C., SEARLS, D. & WEINBERGER, D. (Eds.) (2001): *The cluetrain manifesto: the end of business as usual*, Cambridge (MA): Perseus Books Group.

LI, C. & BERNOFF, J. (2008): *Groundswell: winning in a world transformed by social technologies*, Boston: Harvard Business School Publishing.

LYON, D.:

- (1994): *The electronic eye: the rise of surveillance society*, Oxford: Polity Press.

- (2003): "Surveillance as social sorting: computer codes and mobile bodies", in D. LYON (Ed.), *Surveillance as social sorting*, New York: Routledge, 13-20.

MADDEN, M., FOX, S., SMITH, A. & VITAK, J. (2007): *Digital Footprints: Online identity management and search in the age of transparency*, Washington: Pew Internet & American Life Project.

MANSELL, R.:

- (2002): "From digital divides to digital entitlements in knowledge societies", *Current sociology*, 50 (3), 407-426.

- (2012): *Imagining the Internet: communication, innovation, and governance*, Oxford: Oxford University Press.

McDONALD, A. M. & CRANOR, L. F. (2009): "The cost of reading privacy policies", *I/S: A Journal of Law and Policy for the Information Society*, 4, 543-897.

McSTAY, A. (2011): *The Mood of Information: A Critique of Online Behavioural Advertising*, New York: Continuum.

NN (2012, June 9th): "Microsoft and privacy: change of track - data on people's online behaviour are worth both paying for and arguing over", *The Economist*.

NORMAN, D. A.:

- (1988): *The psychology of everyday things*, New York: Basic Books.

- (1999): "Affordance, conventions and design", *Interactions*, 6 (3), 38-42.

O'REILLY, T. (2005): "What is Web 2.0? Design Patterns and Business Models for the Next Generation of Software".

<http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html> (last accessed on 15 June 2012).

Also published in *COMMUNICATIONS & STRATEGIES*, no. 65, Dossier "Web 2.0 – The internet as a Digital Common", 1st Q. 2007.

OUDSHOORN, N. & PINCH, T. J. (2003): *How users matter: the co-construction of users and technologies*. Cambridge, Mass.; London: MIT Press.

-
- PAGE, N. & CZUBA, C. E. (1999): "Empowerment: What is it?", *Journal of Extension* 37 (5), October 1999. <http://www.ioe.org/ioe/1999october/comm1.php>
- PAPACHARISSI, Z. (2010): "Privacy as a luxury commodity", *First Monday*, 15 (8).
- PASCU, C. (2008): *An Empirical Analysis of the Creation, Use and Adoption of Social Computing Applications: IIPTS Exploratory Research on the Socio-economic Impact of Social Computing*, Seville: Institute for Prospective Technological Studies.
- PASCU, C., OSIMO, D., ULBRICH, M., TURLEA, G. & BURGELMAN, J.-C. (2007): "The potential disruptive impact of Internet 2 based technologies", *First Monday*, 12 (3).
- PIERSON, J. & HEYMAN, R. (2011): "Social media and cookies: challenges for online privacy", *Info*, 13 (6), 30-42.
- PIERSON, J. & HEYMAN, R. (2011): "Social media and cookies: challenges for online privacy", *Info*, 13 (6), 30-42.
- PIERSON, J., JACOBS, A., DREESSEN, K., van den BROECK, I., LIEVENS, B. & van den BROECK, W. (2006): "Walking the interface: uncovering practices through proxy technology assessment", *EPIC 2006 Conference Proceedings* (Ethnographic Praxis in Industry Conference, organised by Microsoft and Intel), published by American Anthropological Association, USA, 29-40.
- PRAHALAD, C. K. & RAMASWAMY, V. (2004): "Co-creation experiences: the next practice in value creation", *Journal of Interactive Marketing*, 18 (3), 5-14.
- PUNIE, Y. (2011): "Introduction: New Media Technologies and User Empowerment. Is there a Happy Ending?", in J. PIERSON & E. LOOS & E. MANTE-MEIJER (Eds.), *New media technologies and user empowerment*, Frankfurt am Main: Peter Lang, 9-23.
- PUNIE, Y., LUSOLI, W., CENTENO, C., MISURACA, G. & Broster, D. (2009): *The Impact of Social Computing on the EU Information Society and Economy*, Seville: IPTS European Commission - Joint Research Centre.
- RAPPAPORT, J. (1987): "Terms of Empowerment/Exemplars of Prevention", *American Journal of Community Psychology*, 15 (2), 121-148.
- RHEINGOLD, Howard (2002): *Smart mobs: the next social revolution*, Cambridge, MA: Perseus.
- SAVERI, A., RHEINGOLD, H. & VIAN, K. (2005): *Technologies of cooperation*, Palo Alto: Institute for the Future.
- SEN, A. (1999): *Development as freedom*, Oxford: Oxford University Press.
- SHIRKY, C. (2008): *Here comes everybody: the power of organizing without organizations*, New York: Penguin Press.

- SILVERSTONE, R. (2006): *Media and morality: on the rise of the mediapolis*, Cambridge: Polity press.
- SMIT, W. A. & van OOST, E. C. J. (1999): *De wederzijdse beïnvloeding van technologie en maatschappij - Een technology assessment-benadering*. Bussum: Uitgeverij Coutinho.
- SMYTHE, D. W. (1977): "Communications: Blindspot of Western Marxism", *Canadian Journal of Political and Social Theory*, 1 (3), 1-27.
- SOLOVE, D. J. (2003): "Identity Theft, Privacy, and the Architecture of Vulnerability", *Hastings Law Journal*, 54, 1-46.
- SPURGEON, C. (2008): *Advertising and new media*, London: Routledge.
- TAPSCOTT, D. & WILLIAMS, A. D. (2007): *Wikinomics - How mass collaboration changes everything*, New York: Penguin Group.
- TOFFLER, A. (1980): *The third wave* (1st ed.), New York: Morrow.
- van der MAESEN, L. J. G. & WALKER, A. C. (2002): *Social Quality: The Theoretical State of Affairs*, Amsterdam: European Foundation on Social Quality.
- VAN DIJCK, J. (2009): "Users like you? Theorizing agency in user-generated content", *Media, Culture & Society*, 31 (1), 41-58.
- Van DIJCK, J. & NIEBORG, D. (2009): "Wikinomics and its discontents: a critical analysis of Web 2.0 business manifestos", *New Media & Society*, 11 (5), 855-874.
- VICKERY, G. & WUNSCH-VINCENT, S. (2007): *Participative web and user-created content: web 2.0, wikis and social networking*, Paris: OECD.
- VILLAGRAN, J. C. (2006): *Vulnerability: a conceptual and methodological review*, Bonn: United Nations University - Institute for Environment and Human Security.
- WALRAVE, M. (2002): "e-Privacy: Marketing on the internet and privacy issues - Evaluation of online privacy statements in respect to the European dataprotection directive (95/46/EC) and the Belgian privacy law (8/12/92 and 11/12/98)", paper presented at IAMCR - International Association for Media and Communication Research'2002, Barcelona (Spain).
- WARREN, S. & BRANDEIS, L. D. (1890): "The right to privacy", *Harvard Law Review*, 4 (5), 69-83.
- WATTS, M. J. & BOHLE, H.-G. (1993): "The space of vulnerability: the causal structure of hunger and famine", *Progress in Human Geography*, 17 (1), 43-67.
- WOOD, D. M. (2006): *A report on the surveillance society: for the information commissioner by the Surveillance Studies Network*, London: UK Information Commissioner.