Asko Lehmuskallio, Sakari Tamminen, Mikael Johnson[1]

Managing Privacy on Social Network Sites

Introduction

The mediation of everyday communication has brought new communicational modes to the fore, which are increasingly based on digital information and communication technologies. We argue that these new modes of communication do often not simply replace existing ways of communication, but broaden the possibilities to interact with other people. Information technology has brought with it automation, the capability to store and use large volumes of data, advances in communication, converging distinct modalities and changing our embodied interactional environments. (cf. Seipel 2002: 21– 23.) In our view, the most important communicational changes are multiple *access* to communicational means, changes in the *scale* of possible information being pushed or pulled, the possibility to *distribute* information to a wide range of possible recipients and the *persistence* of the once sent information due to the technological carriers used, business needs and state regulation mechanisms.

This development is described by concerned intellectuals mainly in two ways. On the one hand using the metaphors of Bentham's (1995) panopticon, Orwell's Big Brother (1995) and the rise of a disciplinary (Foucault 1991) and/or control society (Deleuze 1993). Michel Foucault's "*visibility* is a trap" (Foucault 1991: 200) is cited, in order to refer to the end of privacy and a fragmentation of the common public. On the other hand, a medially connected economy of attention is certified, which makes *invisibility* a trap. Following

---

[1] Contact information: Helsinki Institute for Information Technology (HIIT) –Helsinki University of Technology and University of Helsinki. PO. Box 9800, FI-02015 HUT, Finland, firstname.lastname@hiit.fi.

Markus Schroer (2006): the person who is unable to make himself visible, who is ignored by the glances of other people and the eye of the camera, does to a certain extent not exist in a media society. The private lives of politicians and celebrities are not only investigated with professional paparazzis, journalist-sources and casual citizens armed especially with mobile phone cameras, but politicians and celebrities offer ever more themselves glimpses of their private lives in order to appear more approachable (in the case of politicians) or more interesting (in the case of celebrities). These practices are imitated and exploited further by lay people with less media coverage.

The tension between visibility and invisibility is especially noticeable in regard to social network sites. Here a range of friends, colleagues, relatives and acquaintances have the possibility to share information with each other, add content to each other's site and browse the existing networks of people in one's own network. Even if you do not use these sites yourself, it is ever more likely that pictures and videos of you appear on other people's profiles. Conflicts emerge when private messages are accidentally distributed publicly, people known from other societal contexts get access to delicate information not meant for them to see, data mining with possibly discriminatory consequences becomes possible, third parties use the existing services for target marketing without the user's explicit content etc. While a variety of the conflicts are intended or are accepted as "collateral damage", especially unintended consequences call for a reflection on understanding how these come to be a larger matter of concern – for each of us.

This will be explored in the following. First, by looking at examples of privacy-related conflicts that have emerged in the last years due to ICT use. Second, by discussing privacy not only in Warren's and Brandeis' (1890: 193) sense as "the right to be let alone", but referring to Irwin Altman's (1975 & 1977) suggestion of looking at privacy as a boundary regulation-mechanism, thus implying the need to consider a "right to be included" as well. Third, in introducing specificities of social network sites, analyzed with a framework originally provided by Adele Clarke (2005). Fourth, in focusing on key conflict lines regarding privacy and social network sites (SNS). An analysis of discourses surrounding privacy and SNS and introducing meta-level societal analyses, such as individualization, new forms of capitalism, globalization and changing public-private-relations, have to be postponed due to time constraints. We hope that this explorative work may help in orienting future research questions regarding privacy & SNS and in a broader sense the questions how current and new (dis-)intermediation practices change our surroundings and visual cultures.

Privacy & ICT: Exemplary conflicts

New conflicts are arising due to a discrepancy between intended uses and unintended consequences. A prominent case is Ellen Simonetti's aka *Queen of the Sky's* suspension from work, due to publishing in her blog post "inappropriate pictures in uniform" (Figure 1) (Simonetti 2004). She did not intend to harm her employer in any way – similar postings have been using corporate identities to gain media attention for political causes – but she had to resign because of breaking implicit corporate policies. (cf. Twist 2004.)

Figure 1. Simonetti wrote a book including her firing, using the picture that served for trouble as an eye-catcher on her book cover. (See http://www.myspace.com/queenofsky, last accessed 1 December 2008). Figure 2. Snyder again had posted the picture on the right to her MySpace-profile. (See http://www.thesmokinggun.com/archive/years/2007/0426072pirate1.html, last accessed 1 December 2008).

Another prominent case is Stacy Snyder, whose MySpace-picture captioned "drunken pirate" (Figure 2) was found by officials at Millersville University in Pennsylvania. She was denied her Bachelor of Science degree and a teaching certificate because of being a bad role model for children, although she had had good grades and solid performance evaluations in her studies. (cf. Michels 2008.)

We also have new social situations where user's "lose face" in front of their peers due to ICT-mediated posts being seen by unintended audiences, such as their parents, friends, class mates or siblings. The satirical magazine *The Onion* has a case in point regarding this unintended social disclosure (n.a. 2003.) Losing face in front of family or friends is to some interviewed regarded as more threatening than giving personal information to businesses or the state – a phenomenon we have termed the "Don't tell Mama" effect. In these cases the prime interactional sequence is quite short: a message is posted that is seen by an unintended audience and the person posting the information loses face, or as in the previous cases, educational qualification or one's work. Here visibility seems to be a trap, since high connectivity does bring high visibility.

Other cases that have received fair amount of media attention include the ones where private information is made public because of a desire to participate in the attention economy. Mikael Jungner, the Finnish public broadcasting company's (YLE) manager, has found himself reading many of his private status update lines on Facebook later in newspapers – such as messages regarding his romance with an announcer –, because a journalist has had the opportunity to follow his status updates. (cf. Varis 2007.)

Maybe most prominently, the Finnish foreign minister Ilkka Kanerva had to resign recently because the head of the conservative party *Kokoomus*, Jyrki Katainen, had lack of confidence in his party member's ability to continue running state affairs. Kanerva had been sending sexually oriented text messages to Johanna Tukiainen, a 29-year old erotic dancer. After receiving more than 200 messages, Tukiainen decided to sell them to the yellow press, presumably in order to get free advertising for her and her erotic dance group. The media, with such a scoop at it's hands, decided to capitalize on breaking news and Tukiainen did not have the possibility to stop the yellow press publishing the sold material, although she later wanted to. (cf. n.a. 2008.)

Companies are involved in privacy related issues via data mining. Using SNS becomes only interesting for users if they reveal something of themselves or the character that they "play" on a SNS site (although playing a fictional character is discouraged on many "code of conduct" sites). This makes service providers able to gather rich and detailed user data, which enables pinpointed target marketing and selling user information to third parties. Since SNSs are assumed to consist mainly of interaction between peers, they seem to be especially suitable for word-of-mouthmarketing (or WOM). WOM consists of peers recommending products or services to each other, a form of marketing that is in marketing research literature believed to be especially efficient.

In quite a few cases business interests and end-user privacy collide. A prominent example is Facebook's Beacon feature, which tracks what Facebook users do on specific websites outside of the SNS while logged on to Facebook. At first, the Beacon feature told people in a user's network what they had bought without having gained explicit permission for this (except in the terms of use, which state that all posted content may be used by Facebook in various ways – similar terms are found on other sites as well). Only after a lot of protest, including negative media attention, the Beacon features were changed to give the user a feeling of being in control. (cf. Perez 2007.)

A less thought out example, resulting probably from not even thinking about possible privacy issues, is a dating service's (Match.com) advertising on MSN, one of the most visited sites globally. When visiting MSN's Finnish localization's front page you see each day identifiable profile pictures and user's pseudonyms derived from the dating service da-

tabase. When clicking one of the pictures, the person's rich profile information serves as an advert for using the dating service – quite in contrast to Match.com's explicit claim to care for end-user's privacy. The profile information is shown to casual visitors, including age, gender, religiosity, politic viewpoints and free-form knowledge about the person seeking a dating partner, just to name a few fields that are visible. (cf.http://rakkaus.fi.msn.com/profile/showprofilenocontact.aspx?&uid=4gFKahGn8Yi %2bzmnd87c9uw%3d%3d&handle=maaritmail&tp=MF&trackingid=1002821)

   Additionally we have several cases where digitally collected user information has been stolen or lost (e.g. names and credit card numbers), where the technology used to store people's personal information and network connection breaks down and some data is lost or when a site has decided to end it's service (e.g. Ringo, it is not possible to retrieve videos or contextual information that is of personal importance, such as received comments or one's networks, cf. http://www.ringo.com/). It is also more than likely that a variety of different state institutions gather on these sites much information about their residents and other people they might have interest in the name of state security.

Privacy: The Rights to Be Let Alone and Included

Samuel Warren and Louis Brandeis (1890) are credited for explicitly opening up the discussion on the need for a law regarding individuals' right to privacy. Taking the above exemplary cases, it seems at first sight reasonable that the right to privacy, a right to be let alone, should be of the highest priority. Beate Rössler (2001) has argued that the reason we need privacy is in order to live a "free" and self-determined life and it is in private where we can learn and try out what a free and self-determined life might be. She categorizes privacy into three dimensions, focusing on the individual: 1) informational privacy, regarding control of information that other people know about you (including state and market actors), 2) decisional privacy, regarding control of the decisions and actions that you are making, and into 3) local privacy, asking what spaces can I actually control from other people.

   While Rössler's normative dimensions of privacy are extremely helpful in thinking about the topic, Irwin Altman's (1975) definition of privacy as a boundary-control-process seems to us rather applicable to studying how people actually "do" privacy on social network sites. Altman underscores an aspect often neglected in privacy-discussions, which focus usually on the "right to be let alone" (such as when considering privacy enhancing technologies (PETs) like better encryptions or when considering better data protection

laws)[2]. Altman shows how situationally desired privacy depends on the success of interpersonal boundary-control processes.

If the input level of external interaction is suited to one's situational boundary regulation mechanisms, achieved and desired privacy overlap and no conflicts emerge. But if a person has difficulties in maintaining his/her boundaries, the external inputs are considered to be intrusive and crowding occurs. If again the amount of inputs are insufficient, a feeling of being isolated may emerge. The same applies as well to the amount of output to others in interpersonal boundary-control processes. Too much output may lead to undesired contact, as in Kanerva's, Snyder's and Simonetti's cases, whereas insufficient means for output may lead to social and societal seclusion.

Thus being let alone is only desirable if you do not want to interact with specific actors in a situation, whereas letters, telephones, fax, e-mail, blogs and social network sites are quite often explicitly used to contact other people: friends, relatives, colleagues, acquaintances, company or state representatives or strangers using the same service possibly sharing similar interests. This calls for looking at privacy not only in terms of the "right to be let alone", but also to consider the impact of a "right to be included" – whatever this inclusion to a specific individual means. Similarly this model is useful in showing that a rigid dichotomy between the private and the public is insufficient. What for one actor seems to be a private activity, such as telling other's about one's problems, might for another person be a regular part of public discourse debated on morning TV.

Social Network Sites and Boundary Regulation

Hundreds of different SNS exist, Facebook and Flickr being familiar to the most of us. Others target specific audiences, such as linguistic (MiGente) or religious groups (MuslimSpace, Muxlim), or even pet's owners (Dogster & Catster). (cf. boyd & Ellison 2007.) They attract millions of users worldwide and some of them are listed belonging to the most visited sites on the Internet (cf. http://www.alexa.com).

danah boyd, one of the research pioneers of SNS, and Nicole Ellison, have recently defined Social Network Sites in the following way (2007: 211):

> "We define social network sites 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."

---

[2] For a discussion of the gap between existing privacy policy mechanisms and ICT development see Agre & Rotenberg 1998 and Bennett & Raab 2006.

Although this definition is a starting point for summoning research on a wide variety of web sites, it has been criticized for being too broad, not differentiating enough between different kinds of so called web 2.0 applications, while possibly excluding some websites usually referred to as social network sites (e.g. IRC-galleria, where users profiles show different groups, not lists of individual users). (cf. Beer 2008.) Later boyd & Ellison (2007: 211) state that "What makes social network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks." Although this feature is of great importance at a variety of web-sites referred to as SNS, making one's social networks visible seems to be rather a feature of most mediated interaction: as is the case with using specific clothes related to a territory, clan or interest, choosing first names and possibly surnames in order to show cultural and political affiliations, or related to computer-mediated interaction, choosing specific domain-names, or since the late 1960s and early 1970s, using who- and finger programs in order to retain information of other users in a shared network.

This paper argues that a loose definition of social network sites is most suitable for studying privacy considerations emerging from new forms of computer-mediated interaction to avoid limiting our visions beforehand. Constantly developed and modified web-sites may thus be included as well in the studies, such as homepages that have added Google's Friend Connect, an application enabling the intertwinement of classical web pages with social network features. The specialty of social network sites, attracting users in order to interact in multimodal ways, creates similarly risks and possibilities. Research shows that many people enjoy renewing contacts to old school friends or work colleagues, having the possibility to follow from a distance what people in their extended networks are actually doing, or get to know new people who happen to share similar interests. (cf. Hargittai 2007; Ellison et. al 2007.) The information technology used provides ever more ready components, aggregating and generating friend and interest lists in order to enhance interaction.

Many studies claim that users of newer ICT are generally not very concerned about privacy-related problems.[3] Studies also show, that if users are concerned, they are able to adapt their behavior to new ways of mediated interaction to better control their personal privacy, learning from media or possibly from their own mistakes, and e.g. using acronyms as friends names and avoiding mentioning possibly sensitive information, such as criticizing one's work environment online. (cf. Viégas 2005 for bloggers.) Since many SNSs claim the right to use user-generated content, the boundaries of individuals in relation to these

---

[3] Classic studies have been made by Alan Westin, who divides users often according to privacy fundamentalists, that is the concerned ones, the pragmatists and the unconcerned. For an overview of his studies see Kumaraguru & Cranor 2005.

service providers start to be erased – what is yours is also theirs. In terms of personal boundary regulation it is then interesting why most people are not worried about their 'privacy' – or if they are, these worries are articulated only in the most extreme cases (Tukiainen, Flight attendant, Facebook Beacon, etc). In other words when personal privacy boundary control processes break down. The lack of perceived end-user privacy concerns should nevertheless not be equated with an absence of possible privacy-related conflicts, as the exemplary cases combining intended and unintended consequences show. Similarly, studies highlighting the porous technological components, such as leaking Wi-Fi or Bluetooth access points, or servers that break down should be enough to underline the key argument – privacy becomes problematic to the individual when boundary control processes break down.

Privacy-related research involving users, especially in the field of HCI, does usually not take other privacy-concerns than those articulated in user interviews into account, nor do we have studies comparing different technologies in regard to privacy issues (for an overview, see Iachello & Hong 2007.) We suggest inspecting more fully the different stakeholders and how they actually influence end-user privacy in diverse ICT settings. For such a study we use an extended framework originally provided by Adele Clarke. It draws from Strauss' approach to grounded theory and combines it with guidelines from HCI-research on privacy. Here the following aspects in the analysis of privacy related phenomena are of interest:

- *stakeholders* (individual, collective, implicated/silent),
- *social relations* and *power structures* (who is able to interact with whom and in which ways?),
- *discourse formations* (how do different stakeholders frame the use of specific applications?),
- *norms, regulations and rules* (which behavioral scripts do different stakeholders suggest?),
- *history, traditions, persistence* (how has the application in question evolved, what traditions have emerged and which information is kept and why?),
- *interactional enablers* (how is interaction made possible and what kind of information is hereby suggested?),
- *communicational forms* (how do stakeholders interact with each other?), business models (how is continuous work compensated?), and
- *non-human actants* (what technologies are used to maintain and develop the service, what technologies are necessary in order to be able to participate in the specific interaction?).

Conflict Lines regarding ICT & End-User Privacy

With such a framework and analysis a number of conflict lines are already discernible within the recent discussions and use of SNSs. These are not exclusive but rather overlapping dimensions.

The first line of conflict problematizes the intentionality of action of any given individual within these new services. These can be broken down into three categories: 1) conflicts arising from intended action, such as phishing attacks or capitalizing of private information (Facebook Beacon-controversy), 2) unintended consequences, in sharing of sensitive information available to third parties (Queen of the Sky & Stacy Snyder), 3) intended action coupled with unintended consequences (Finnish foreign minister/Johanna Tukiainen). These problems derive from informational asymmetry and related means of regulating the boundaries and the transfer of information from one context or media to another.

The second line of conflict concerns competing interests. Business models and end-user privacy are often difficult to combine, since SNS generate revenue mainly from venture capitalists, state's technology support, premium user's paying for additional services, selling traditional and new advertising space on sites, selling market information further on and/or trying to capitalize from a first exit strategy (that is building an interesting site, getting many customers and selling the site for a lot of money, e.g. YouTube and Jaiku). Here user-generated content, in forms of log data, text, pictures, audio and video, is often an important part of gathered revenue, turning private information into a capitalised commodity.

A third line of conflict relates to the difficulty of containing and controlling the digital trails of action and the content that is produced and shared (semi-)publicly within SNSs. ICT-mediated interaction becomes easily materially desituated, and can appear spatially and temporally in new contexts. Digital traces users leave behind are difficult to remove. Legal cases trying to prohibit specific uses often only attract new audiences to existing persistent traces of interaction.

A fourth line of conflict is the difficulty to manage one's ever richer "digital identity". Whereas traditionally mediation has unburdened from facework in face-toface situations, social network sites ask especially for attention on facework, while the contexts of interaction are not always clear. Thus some people have seized using specific SNS, since it has been too difficult to separate messages sent to people belonging to different groups, such as friends, work colleagues, and casual acquaintances – in other words, they experience a lack of control mechanisms for the information communicated within these forms of media.

Conclusions

The discourse of invisibility being a trap tends to treat users of newer technologies such as SNSs as simple people seeking media attention and undermining a civic publicity with banalities – especially if they share their information publicly – and they have to be educated. If focusing solely on the right to be let alone, visibility seems to be a trap, since ICT use *does* make data mining easier and possible misuses of personal information become more likely.

If we do not want to ban technologies out of our lives (a possible answer to the thoughts presented), it is important to see that we as societies and invididuals are more than ever bound to a computerized and networked way of living. This is not – contrary to what is usually suggested – outside of our "humanness" but in contrast, currently its condition. Our everyday lives would be impossible to carry on without already having computers everywhere – pervasive and ubiquitous computing already permeating many facets of our current societies. In some sense it would be impossible to tell who we are without these systems. But, as bound as we are to information technology as individuals, as a whole this system provides for at least three novel things *into our relations to each other*: a global scale, distribution and persistence for any action we make. Our (individual and collective) presence and its trails within these systems become more and more uncontrollable and their effects more and more unpredictable.

Although technologies change our possibilities for interaction, we have a variety of persistent uses known from previous times (e.g. snapshot photographers using novel picturing technologies in conventionalized ways not exploring the possibilities of new media). It is important to remember that the social lives of mediated communication are always connected to human beings working behind, with and for them. Or, as Régis Debray (2003) puts it, the external memory of a medium has to be activated by people who carry the knowledge, an internal memory, used to decipher the external one.

References

Agre, Philip E. and Rotenberg, Marc (eds). 1998. *Technology and Privacy: The New Land-scape*. MIT Press.

Altman, Irwin. 1977. Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues* 33: 3, p. 66-84.

Altman, Irwin. 1975. *The Environment and Social Behavior. Privacy - Personal Space - Territory - Crowding*. Monterey: Brooks-Cole Publishing Company.

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

Bennett, Colin J. and Raab, Charles D. 2006. *The governance of privacy: policy instruments in global perspective*. Cambridge, Mass.: MIT Press.

Bentham, Jeremy. 1995. *The Panopticon writings. Edited and introduced by Miran Božovič*. New York – London: Verso.

boyd, danah m. and Ellison, Nicole B. 2007. Social Network Sites. Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* 13: 1, p. 210–230.

Clarke, Adele E. 2005. Situational Analysis. Grounded Theory After the Post modern Turn. Thousand Oaks – London – New Delhi: Sage.

Debray, Régis. 2003. *Einführung in die Mediologie*. Bern - Stuttgart - Wien: Haupt.

Deleuze, Gilles. 1993. Postskriptum Über die Kontrollgesellschaften. In: Ibid. *Unterhandlungen 1972–1990*. Frankfurt am Main: Suhrkamp, p. 254–262.

Ellison, Nicole B.; Steinfield, Charles and Lampe, Cliff. 2007. The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites *Journal of Computer-Mediated Communication* 12: 4, p. 1143– 1168.

Foucault, Michel. 1991. *Discipline and Punish. The Birth of the Prison*. London et al.: Penguin.

Hargittai, Eszter. 2007. Whose Space? Differences Among Users and Non-Users of Social Network Sites. *Journal of Computer-Mediated Communication* 13: 1, p. 276–297.

Iachello, Giovanni and Hong, Jason. 2007. End-User Privacy in Human-Computer Interaction. *Foundations and Trends in Human–Computer–Interaction* 1: 1, p. 1–137.

Kumaraguru, Ponnurangam and Cranor, Lorrie Faith. 2005. *Privacy Indexes: A Survey of Westin's Studies. Technical Report CMU-ISRI-05-138*. Institute for Software Research International, School of Computer Science, Carnegie Mellon University.

Michels, Scott. 2008. Teachers' Virtual Lives Conflict With Classroom. *ABC News* 6.5.,

12

  p. http://abcnews.go.com/TheLaw/story?id=4791295.

n.a. 2003. Mom Finds Out About Blog. *The Onion. America's Finest News Source* 12.11., p
  http://www.theonion.com/content/node/30007.

n.a. 2008. Näin Kanerva tekstaili: "Miten ois koskettaa yökerhossa sua sormilla". *Ilta
  -Sanomat* 1.4., p.
  http://www.iltasanomat.fi/uutiset/kotimaa/uutinen.asp?id=1512893.

Orwell, George. 1995. *1984. Mit einem Nachwort von Herbert W. Franke*. Frankfurt am
  Main – Berlin: Ullstein.

Perez, Juan Carlos. 2007. Facebook's Beacon More Intrusive Than Previously Thought. *PC
  World* 1.12., p. http://www.pcworld.com/article/140182/ face-
  books_beacon_more_intrusive_than_previously_thought.html

Rössler, Beate. 2001. *Der Wert des Privaten*. Frankfurt am Main: Suhrkamp.

Schroer, Markus. 2005. Sehen, Beobachten, Überwachen. Beitrag zu einer Soziologie der
  Aufmerksamkeit. In: Hempel, Leon and Metelmann, Jörg (ed.). *Bild – Raum – Kon-
  trolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels*. Frankfurt am
  Main: Suhrkamp, p. 325–341.

Seipel, Peter. 2002. Law and ICT. A Whole and its Parts. In: Seipel, Peter (ed.). *Law and
  Information Technology. Swedish Views. An anthology produced by the IT Law Ob-
  servatory of the Swedish ICT Commission*. Stockholm: Swedish Government, p. 21–
  32.

Simonetti, Ellen. 2004. Perspective: I was fired for blogging. *Cnet News* 16.12., http://
  news.cnet.com/I-was-fired-for-blogging/2010-1030_3-5490836.html.

Twist, Jo. 2004. US blogger fired by her airline. *BBC News* 3.11., http://news.bbc.co.uk/
  2/hi/technology/3974081.stm.

Varis, Olli. 2007. Koukussa! Yleisradion toimitusjohtaja Mikael Jungner käyttää työai-
  kaansa Facebookissa. *Iltalehti* 5.11., p. http://www.iltalehti.fi/uutiset/
  200711056802976_uu.shtml.

Viégas, Fernanda B. 2005. Bloggers' expectations of privacy and accountability: An initial
  survey. *Journal of Computer-Mediated Communication* 10: 3, p. http://
  jcmc.indiana.edu/vol10/issue3/viegas.html.

Warren, Samuel and Brandeis, Louis. 1890. The Right to Privacy. *Harvard Law Review*
  4: 1, p. 193-220.