Online Social Networking as Participatory Surveillance

Article *in* First Monday · March 2008

DOI: 10.5210/fm.v13i3.2142 · Source: DBLP

1 author:

Anders Albrechtslund
Aarhus University
32 PUBLICATIONS **956** CITATIONS

SEE PROFILE

First Monday, Volume 13, Number 3 - 3 March 2008

PEER-REVIEWED JOURNAL ON THE INTERNET

Online social networking as participatory surveillance

by Anders Albrechtslund

Abstract

In this article, I argue that online social networking is anchored in surveillance practices. This gives us an opportunity to challenge conventional understandings of surveillance that often focus on control and disempowerment. In the context of online social networking, surveillance is something potentially empowering, subjectivity building and even playful — what I call participatory surveillance.

Contents

Introduction

In this article, I study online social networking as a practice based on participatory surveillance. My theoretical approach is founded in the cross field between surveillance studies, computer ethics and philosophy of technology. I will pursue three research questions in this order:

1. How can we conceptualize the practice of online social networking? I have chosen to study this practice through the lenses of space, place and time for two reasons: Firstly, these perspectives offers a way to discuss the off-line-online debate (*e.g.*, boyd, 2007a; Ellison, *et al.*, 2007; Nip, 2004) in a non–dualist way. Secondly, spatial metaphors have been discussed as an important frameworks in relation to the Internet (*e.g.*, Graham, 1998), just as developments relating to place and time play an interesting role in relation to social networking sites today.

   In the context of social networking sites and the offline–online debate, I argue that it is an unproductive abstraction to make a sharp distinction between the physical world and the virtual world. Instead, online social networking must be viewed as a mixed world and relating to both online and offline activities.

2. What kind of discourse surrounds the practice of online social networking? Social networking sites are dominating online activities today (boyd and Ellison, 2007; Lenhart and Madden, 2007) and this presence has, of course, led to divided opinions about the pros and cons. Especially surveillance–related scenarios have been discussed and a number of concerns voiced. With this question I want to focus on the conceptions of surveillance inherent in the arguments about online social networking.
3. What can we learn about surveillance through social networking? Characteristic of online social networking is the sharing of activities, preferences, beliefs, etc. to socialize. I contend that this practice of self–surveillance cannot be adequately described within the framework of a hierarchical understanding of surveillance. Rather, online social networking seems to introduce a participatory approach to surveillance, which can empower – and not necessarily violate – the

user.

The practice of online social networking: Space, place and time

In this section I will connect space, place and time to online social networking by focusing on three correlating aspects. First, cyberspace and other defining spatial metaphors for the Internet will be discussed along with the characteristics of online social networking. Second, I focus on the role of geographical locations for online socializing. Third, the temporal aspect will be discussed in connection with the online friendship phenomenon.

Cyberspace

The computing vocabulary has been dominated by spatial metaphors, *e.g.*, operating systems with *desktops* and *windows*, and this discourse has been extended to the Internet. The term *cyberspace* was coined by William Gibson (1984) and popularized in his novel *Neuromancer* and, today, it is widely used as a metaphor for the Internet and the Web. As such, cyberspace can be considered the space of online activities, including mundane Web surfing and social interaction, and this spatial metaphor thus differs from the physical Internet consisting of servers.

Other influential spatial metaphors include *global village*, *the information highway*, *domain*, *Web site* and the reference *over at* to describe relations between Web sites. Today, services associated with Web 2.0 — such as wikis, blogs, folksonomies, and, of course, social networking sites — have adopted and are elaborating on these spatial metaphors. A prominent example is *online communities*, which is a key phrase in understanding social activities.

An obvious reason for the spatial discourse in relation to computing and the Internet could be the desire to organize and classify. A space represents a hierarchy, which can be useful to categorize and "clean up" entities and their relations. However, the metaphor has limits, since cyberspace is not constrained by the same laws as physical space (Shirky, 2005). The Web cannot adequately be described in terms of classic ontological organization, as it is interrelated in a non–hierarchical way reminiscent of an organism, Deleuzian rhizome (Klei, 2002) or other self–organizing socio–technological systems (Fuchs, 2005).

A prominent example of interest is the social networking site MySpace. This site, which even by name is associated with the spatial metaphor, is according to ratings (Alexa, 2008) among the most popular Web sites in the world. Like most other social networking sites, MySpace is built on the principle that a user and the user's friends fill out their space by providing information in the form of text, images, audio and video. The owner of a space provides details in a profile with personal information. According to a report from Pew Internet & American Life Project (Lenhart and Madden, 2007), a vast majority of teens (82 percent) provides their real first name for their profile [1].

Also, a majority of profile holders provides pictures of themselves and their friends as well as the name of their hometown. However, only a small minority includes their full name, phone number and e–mail address. Besides profiles, the space includes a list of friends [2] and a commenting feature, and these three features – profiles, friends and comments – make up the basic structure of MySpace as well as most other social networking sites (boyd and Ellison, 2007). In addition to these core features, many sites include blogging, file sharing and other tools.

A place for socializing

An emergent trend in the context of social networking sites is geographical tagging. Geotagging is a way to add geographical information to media such as Web sites, RSS feeds and images to help users find a wide variety of location–specific information. Social networking sites and related services and applications such as del.icio.us, Flickr and Google Earth facilitate geotagging, and this contributes to the building of a place–based folksonomy.

This entails an interesting new relation between cyberspace and physical places, which adds to the already extended information infrastructure of Web 2.0. Online social networking sites already give insights into users' thoughts (blogging software), their likes (social bookmarking services), what music they are listening to (*e.g.*, Last.fm), and the practice of geotagging means sharing information about the whereabouts of the user and, in some cases, the people in the vicinity of the user.

Furthermore, a number of specialized sites and services have emerged that specifically make use of geographical information, and these are often known as "mobile social software" (MoSoSo). The main purpose of MoSoSo is to facilitate social, romantic or business encounters by associating time and location data to online social networks. Examples of this trend include Plazes.com (detecting location and connects the user to things nearby) and My MoSoSo (which uses Wi–Fi peer–to–peer *ad hoc* mode to facilitate networking with people within a two–minute walk).

The relation between cyberspace and physical spaces is interesting, since it demonstrates that online social networking is not only *online*. Studies have shown that there are both an online–to–off-line and offline–to–online trend with regards to the developments of friendships (*e.g.*, Ellison, *et al.*, 2007; Parks and Floyd, 1996). However, the socializing related to geo–based networking sites is supposed to *take place* in a mixed zone, online and off-line, and this leads to new perspectives on cyberspace and geographical places.

Whereas cyberspace is an abstract, virtual space, the geographical places are not. Even though the relations and practices are similar, geo–based social networking changes the rules for shared personal information. Here, people are supposed to meet in person at their current geographical location, while cyberspace offers the opportunity to construct an identity beyond bodily presence. Thus, the question concerning surveillance is different in this context, as the online social networking profile is linked to the users physically being there in person.

Eternal friendships

It is said that true friendships last forever, however, in the case of online social networking this sentiment gets a completely different meaning. The digital trails of an online friendship — true or not — really *do* last forever, since they are stored indefinitely on servers. Moreover, the documentation of friendships becomes easily accessible because of the digital, portable nature of the information. Thus, cyberspace changes social relations and practices concerning temporality, organization and audience.

danah boyd has suggested that online social networking as a mediated public is characterized by four properties: persistency, searchability, replicability and invisible audiences (boyd, 2007a). Online social networking is persistent, because the communication is stored indefinitely. The consequence of this is, of course, that the things people write in their blogs, comment posts and other seemingly instant and situation–based communication will be available for later scrutiny. It can enter into other, completely different, lines on communication later in life, which has the potentiality of embarrassment, or even damages to social life and career opportunity. At least, those are the fears often mentioned by critics.

The second property, searchability, makes information available at the convenience of a few keywords and phrases instead of time–consuming collection and sorting of information. The almost instant access to things the searcher is looking for does make a difference compared to the slow process of "digging out" what he or she wants to find.

Thirdly, the digital nature of online social networking makes it replicable. As with other digital information, online social communication can be detached from its specific media and perfectly reproduced, even altered, and put into other contexts.

boyd's final point is the invisible audience of online social networking. Even though people obviously communicate online with a specific audience in mind, *e.g.*, their friends, the public nature of online social networking makes the information available to a much larger audience, potentially everyone with access to the Internet.

Together, these four properties make friendships "eternal" – or at least existing beyond the control of the involved persons. Social interaction, which is thought to be something of the moment and tied to a certain situation, is made into the opposite, that is, something asynchronous and accessible. What is thought to be of the present is now forever a potentiality of the future.

Surveillance discourses of online social networking

Here, I want to focus on the implicit assumptions that surround the public and academic debate about social networking sites. While trying to avoid reducing a nuanced debate to stereotypical positions, I will highlight certain aspects of the discussion that relate to conceptions of surveillance: The idea of social networking sites as sources of information for secondary purposes, moral panics and conspiracy theories relating to online social networking, and the discussion about the possible delayed consequences of socializing in mediated publics.

A snoop's dream

Online social networking can have a touch of private communication to it due to its situational and mundane character, but mediated publics are obviously not private. This dilemma is, of course, a central part of the discussion concerning surveillance and privacy issues, and it is especially evident in connection with secondary uses of available information at social networking sites.

It is well known that since the terrorist attacks of September 11, 2001, government surveillance has increased especially in the U.S. These measures include an interest in online social networking (Marks, 2006). The U.S. National Security Agency (NSA) funds research to develop ways of mass harvesting

information shared in online social networks, and this news has, of course, been widely noticed among bloggers.

Government interest in online social networking is easy to understand. To profile potential criminals and terrorists, it is necessary to combine a wide range of information about people. This information includes social relations, such as shared activities and circles of friends, as well as personal data about political views, religious beliefs, sexual orientation, and preferences regarding everyday life activities.

It is exactly this sort of information which can be found when studying online social networking. Most social networking sites ask their users to provide these sorts of details; in part this information appears in casual digital conversations within given social networking communication platforms. Consequently, the needed information to profile people is not something hidden that must be uncovered or retrieved using exotic technologies, human agents or advanced bugging equipment. People themselves are publishing this information in question, free for all to see and collect. Of course, this makes online social networking appear as a "snoop's dream" (Marks, 2006).

It is only a question of connecting the dots, so to speak, since personal data is available, to some extent from the same source, and often in a combination of difference sources. A useful concept to describe this situation is David Lyon's "leaky containers" [3]. Lyon uses this concept to describe how data move freely between different sectors of society with the result that information from discrete contexts, *e.g.*, private life, work life and shopping, are being mixed rather than contained separately.

An example from the online social networking world is the news story that police have used the video sharing service YouTube to solve crimes (*e.g.*, Maxcer, 2007). Apparently, police in Canada and U.S. have posted surveillance footage of crimes as videos on YouTube, encouraging users to identify the alleged criminals. The police are using social networking sites during criminal investigations is an example of leaky containers, since public and private, official and social, mix in completely new ways. Social communication becomes a tool for the police, and criminal investigation becomes part of social interaction.

Moral panics

Online social networking can have serious consequences and has therefore given rise to a number of concerns from moral panics (*e.g.*, Roush, 2006) to spying plots (*e.g.*, Marks, 2006) and even conspiracy theories (*e.g.*, Bruce, 2007; Greenop, 2007).

In public opinion and academia, many people have voiced concern and amazement about the openness, or perhaps thoughtlessness, expressed in the behavior of social networking site's users. As Jon Callas, chief security officer at the encryption software maker, PGP, puts it: "I am continually shocked and appalled at the details people voluntarily post online about themselves" (quoted in Marks, 2006).

Like Callas, many people are puzzled and appear to be almost offended by the frankness in communication and, perhaps, carelessness that some people, especially youngsters, display with regard to their personal privacy. In the academic discussion, explanations have been sought as to why people reveal so much personal information while socializing online. Here is a representative example:

> "While privacy may be at risk in social networking sites, information is willingly provided. Different factors are likely to drive information revelation in online social networks. The list includes signalling o because the perceived benefit of selectively revealing data to strangers may appear larger than the perceived costs of possible privacy invasions; peer pressure and herding behavior; relaxed attitudes towards (or lack of interest in) personal privacy incomplete information (about the possible privacy implications of information revelation); faith in the networking service or trust in its members; myopic evaluation of privacy risks […] or also the service's own user interface, that may drive the unchallenged acceptance of permeable default privacy settings." [4]

Besides the possible design issues in social networking sites with regards to privacy settings and awareness, most of the explanations are focused on shortcomings on the part of the user. As the above example illustrates, these alleged user shortcomings range from ignorance to indifference and dependency on others.

This has led to discourses of education and protection, since the argument goes that youngsters apparently need to be trained in a code of conduct with regards to online activities to learn how to protect themselves. In 2006, the Deleting Online Predators Act (DOPA) was introduced and passed (410–15) in the U.S. House of Representatives. The bill is supposed to protect minors from predators by instructing facilities receiving federal aid, *e.g.*, public libraries, to block access to social networking sites, where youngsters might encounter adults seeking sexual contact.

Certainly, many dangers lurk in the transparent world of mediated publics, including potential privacy invasion, miscarriage of justice based on false information and, not least, the menace of predators who want to harm young people. These dangers are real and should be treated accordingly. However, critics claim that the education and protection discourse is also a moral panic.

Jenkins and boyd point out that DOPA will not achieve its purpose of protection and, worse, it will have severe social damages (Jenkins and boyd, 2006; Roush, 2006). boyd argues that only a marginal number of child abductions are related to online social networking, and Jenkins argues that the restrictions put on Internet use at public libraries will deepen the cultural gap between kids who must rely on Internet access at the library and kids who have access at home.

Life after social networking

Among the many concerns about online social networking, the possible consequences of this (dangerous) practice in later life are often discussed. When youngsters lead a life in mediated publics, the fear is that their adolescent thoughts, musings and immature actions might become a millstone around their neck, since the information will be embarrassingly accessible later on. One such speculation has to do with getting a job in adult life (Tribble, 2005a; 2005b).

To Tribble (2005a; 2005b), the fundamental practice of sharing information is puzzling. Thus, the point of departure in the first article – with the rather pointed title "Bloggers Need Not Apply" – is a question: "The pertinent question for bloggers is simply, why? What is the purpose of broadcasting one's unfiltered thoughts to the whole wired world."

The author is convinced that past online social networking will be damaging to an applicant's chances for employment. Tribble, who is also involved in hiring people, will be skeptical of such a candidate. In support of this conviction Tribble offers two arguments relating to breach in privacy. First, the discomfort felt by colleagues, when they know someone at the department is blogging. They might fear that the new colleague air "dirty laundry" at the department. Second, the candidate can have difficulties hiding personal preferences and beliefs from employer and co–workers.

Tribble argues from personal experience as an employer: "We felt deceived by his overstatement of his academic expertise. In this case, it was not the candidate's own blog, but that of a boasting friend, that revealed the truth. The lesson? Be careful what you let a close associate's blog say about you. What that associate sees as complimentary may cast you in an unflattering light in the eyes of a search committee" (Tribble, 2005).

danah boyd among others has criticized the reluctance to hire people based on the fact that they have or are taking part in online social networking. In a response to a case study in *Harvard Business Review*, boyd argues that online social networking is part of her generation's culture and will therefore also be a natural part of that generation's past. If employers leave out candidates who have an online history, then they will "miss out on the best minds of my generation. Bright people push the edge, but what constitutes the edge is time–dependent. It's no longer about miniskirts or rock and roll; it's about having a complex digital presence" (boyd, 2007b).

It can be added to this employer#150;focused argument that discriminatory practices against people with online histories could be considered an ethical injustice similar to discrimination based on gender, race or, for that matter, the candidate's history of exercising free speech in public debate.

Participatory surveillance

Looking at discourses in the context of online social networking and related Web 2.0 services and applications, a traditional and rather negative conception of surveillance appear. Surveillance is associated with snooping, spying and privacy invasion, and it is a prevalent view that everything related to it should be avoided if possible. This is in line with familiar frameworks such as Big Brother and Panopticon, but the problem is that they do not seem to adequately describe the actual practice of online social networking.

In the following I suggest using the concept of *participatory surveillance* [5] to develop the social and playful aspects surveillance. First, online social networking is related to the traditional hierarchical surveillance concept. Second, the aspect of mutuality will be studied. Third, I will elaborate on the idea of participatory surveillance with regards to user empowerment, subjectivity building and information sharing.

The hierarchical, vertical concept of surveillance

A conventional understanding of surveillance is that it is a hierarchical system of power. This common understanding is represented in familiar metaphors such as "Big Brother" and "Panopticon," both of

which illustrate a vertical, hierarchical power relation between the gaze of the watcher that controls the watched. The hierarchical conception of this relation puts the power into the hands of the watcher while the watched is a more or less passive subject of control. In the case of hierarchies in the Orwellian sense, surveillance is also part of the destruction of subjectivity under surveillance and an effort to render lifeworld meaningless.

The moral panics, conspiracy theories, and the difficulties in understanding why people actually would want to engage in online social networking all reflect this dystopian view on surveillance. It is the basis for the discourses of protection and education as well as for the idea that users are either perfroming cost–benefit analyses before creating an account on a social networking site or simply do not know enough about the lurking dangers of surveillance. In other words, it is difficult to understand the phenomenon of online social networking and related Web 2.0 services and applications when we apply this notion of surveillance.

Although the Panopticon was more or less disregarded after Bentham (Lyon, 1991) until Michel Foucault's (1975) *Surveiller et punir: Naissance de la prison*, apart from a few notable exceptions (*e.g.*, Himmelfarb, 1968), it has since been the dominating conceptual framework within surveillance studies. Interestingly, students of surveillance have often tried to go beyond the Panopticon, and a number of different concepts have been introduced, *e.g.*, the *electronic panopticon* (Lyon, 1994) and *superpanopticon* (Poster, 1990; 1996) where computerized databases are discussed as a technologically enhanced realization of Panopticon that encompasses cultural innovations brought about by databases.

However, it still seems that writing and talking about going beyond the Panopticon — rather than actually doing it — is the case, as indicated in the recent book edited David Lyon (2006) entitled *Theorizing surveillance: The panopticon and beyond*. In it, Lyon laconically states "[t]he panopticon refuses to go away" [6].

The panopticon model is indeed a strong framework for discussing surveillance theoretically, and in many cases it is a fitting one. Therefore, I am not suggesting a change of directions or something similar within surveillance studies, but rather an expansion of the field of study. The many excellent theoretical, conceptual and methodological approaches are useful and necessary point of departures for any student of surveillance – and in the context of online social networking. However, if we want to better understand this and other related practices, it is necessary to challenge the hierarchical conception of surveillance.

Surveillance as a mutual, horizontal practice

The word *surveillance* is etymologically associated with the French word *surveiller*, which translates simply as *to watch over*. The verb suggests the visual practice of a person looking carefully at someone or something from above. Both in ordinary language and within academic debate, the practice of "watching over" has become a metaphor for all other monitoring activities. Thus, the understanding of surveillance is not limited to a visual practice; rather it involves all senses — data collection and technological mediation.

The visual metaphor implies a spatial hierarchy where the watcher is positioned *over* the watched. Yet, this does not mean surveillance is necessarily a hierarchical power relation in which the watcher controls the watched. Similar to the broadening of the concept to include all senses, data collection and technological mediation, surveillance can be seen as a "flat" relationship or even in favor of the person under surveillance, either negatively as actively resisting the gaze (Ball and Wilson, 2000; McGrath, 2004) or positively as exhibitionistic empowerment (Koskela, 2004).

Further, the surveillance relationship can be mutual, as described by Mark Andrejevic who has introduced the concept *lateral surveillance*:

> "Lateral surveillance, or peer–to–peer monitoring, understood as the use of surveillance tools by individuals, rather than by agents of institutions public or private, to keep track of one another, covers (but is not limited to) three main categories: romantic interests, family, and friends or acquaintances." [7]

Although Andrejevic does not directly make the connection, lateral surveillance seems like a useful concept to throw light on certain aspects of online social networking. However, Andrejevic brings over the power relations from the Panopticon to the peer–to–peer monitoring, arguing that these technologies actually amplify the top–down monitoring. The consequence is law enforcement technologies are brought into social life:

> "The participatory injunction of the interactive revolution extends monitoring techniques from the cloistered offices of the Pentagon to the everyday spaces of our homes and offices, from law enforcement and espionage to dating, parenting, and social life. In an era in which everyone is to be

> considered potentially suspect, we are invited to become spies – for our own good." [8]

In other words, lateral surveillance makes us spies in a disciplinary society.

Although lateral surveillance is an interesting and thought–provoking concept, it does not adequately explain the practice of online social networking as described in the above. However, I would like to hold on to the idea of surveillance being a mutual practice, as it corresponds to some of the characteristics of online social networking. I will replace the vertical relation with a horizontal, which makes it possible to understand some of the positive aspects of being under (mutual) surveillance.

Empowerment, subjectivity building and sharing

In the following, I will call attention to two aspects of surveillance in the context of online social networking which are missing or underdeveloped in the previously discussed concepts. These are the idea of user empowerment and the building of subjectivity, and, second, the understanding of online social networking as a sharing practice instead of an information trade. Together, these two aspects, along with mutuality, makes up what I call participatory surveillance.

As mentioned earlier, a hierarchical conception of surveillance represents a power relation which is in favor of the person doing the surveillance. The person under surveillance is reduced to a powerless, passive subject under the control of the "gaze." When we look at online social networking and the idea of mutuality, it appears that this practice is not about destructing subjectivity or lifeworld. Rather, this surveillance practice can be part of the *building* of subjectivity and of making sense in the lifeworld.

An illustrative example is Hille Koskela's (2004) discussion of the use of webcams, TV shows and mobile phones. She introduces the concept *empowering exhibitionism* to describe the practice of revealing your (very) personal life. By exhibiting their lives, people claim "copyright" to their own lives [9], as they engage in the self–construction of identity. This reverts the vertical power relation, as visibility becomes a tool of power that can be used to rebel against the shame associated with not being private about certain things. Thus, exhibitionism is liberating, because it represents a refusal to be humble [10].

Online social networking can also be empowering for the user, as the monitoring and registration facilitates new ways of constructing identity, meeting friends and colleagues as well as socializing with strangers. This changes the role of the user from passive to active, since surveillance in this context offers opportunities to take action, seek information and communicate. Online social networking therefore illustrates that surveillance – as a mutual, empowering and subjectivity building practice – is fundamentally social.

Turning to the second aspect – from trading to sharing – it is expedient to elaborate on the concept of participation. To participate is to engage in something, but it is not necessarily something we do out of individual desire or pleasure. Examples could be found in all contexts of life, including work–related situations and charity efforts. However, participation as an engaging act is voluntary and must be well–defined in relation to the pseudo–participation we know from the Panopticon and Orwell's *Nineteen Eighty–Four*.

The Panopticon is set up in way for the prisoners to take part in their own surveillance by internalizing the gaze of the watcher, and in Orwell's novel the citizens of Oceania ends up taking part in their own (and others') surveillance in their "love" of Big Brother. Here, the self–surveillance is inflicted on the people watched, as they are caught up in a power relation (Foucault, 1975) or as a result of the brainwashing carried out by the Ministry of Love (Orwell, 1949). Both of these disciplinary practices disempower and, thus, disengage the subject of surveillance. Therefore, concepts such as *participatory panopticon* (Cascio, 2006) are contradictory or, at best, redundant, if the internalizing of the gaze is interpreted as a form of pseudo–participation.

The practice of online social networking can be seen as empowering, as it is a way to voluntarily engage with other people and construct identities, and it can thus be described as participatory. It is important to not automatically assume that the personal information and communication, which online social networking is based on, is only a commodity for trading. Implicit in this interpretation is that to be under surveillance is undesirable. However, to participate in online social networking is also about the act of sharing yourself – or your constructed identity – with others.

Accordingly, the role of sharing should not be underestimated, as the personal information people share – profiles, activities, beliefs, whereabouts, status, preferences, etc. – represent a level of communication that neither has to be told, nor has to be asked for. It is just "out there", untold and unasked, but something that is part the socializing in mediated publics. One of the findings in the earlier mentioned Pew Internet & American Life Project report (Lenhart and Madden, 2007) is that a great majority of teens use online social networking to keep in touch with friends they rarely see in real life. In this case, participatory surveillance is a way of maintaining friendships by checking up on information other people share. Such a friendship might seem shallow, but it is a convenient way of keeping in touch with a large circle of friends, which can be more difficult to handle offline without updated personal information –

untold and unasked.

Conclusion

In this article, I have tried to shed light on the social aspect of surveillance, as a form of participatory surveillance involving mutuality, empowerment and sharing. It should be stressed that my intention is not to belittle the potential dangers of surveillance on the Web. There are many threats, ranging from privacy invasion and social sorting to fraud and identity theft (Gross and Acquisti, 2005). Precautions must be taken to avoid these dangers.

My point is that we should not let the awareness of these threats take over when we study online social networking. When we study the actual practice, we should not be "lured" into only seeing the dangers in things. Rather, online social networking is an opportunity to rethink the concept of surveillance.

About the author

Anders Albrechtslund holds a Master's Degree in Philosophy (2003) from the University of Southern Denmark, and since February 2005 is a Ph.D. candidate at Aalborg University in Denmark. His research interests include philosophy of technology, surveillance studies and computer ethics.

Acknowledgements

I am grateful to my colleagues at Aalborg University who have generously contributed to the development of this article with excellent comments and suggestions. I have also been helped in the work process by having the opportunity to present the arguments of this article at meetings and conferences sponsored by the Aalborg University's Human Centered Informatics Postgraduate Research School and the Association of Internet Researchers annual conference.

Notes

1. It should be stressed that the Pew Internet & American Life Project report studies online social networking as a whole. Therefore, the percentages apply to online social networking in general and not MySpace in particular.

2. In connection with online social networking sites, a list of friends should not be confused with the "offline" understanding of friendship as something mutual, caring and perhaps even rather exclusive. Online friends can be all of this, but they can also be acquaintances, contacts, people who find you interesting, etc., thus, most people tend to have a lot of online friends. Presidential candidate Barack Obama had 305,151 friends on MySpace as of 1 March 2008 (http://www.myspace.com/barackobama).

3. Lyon, 2001, pp. 37–48.

4. Gross and Acquisti, 2005, p. 73.

5. The concept "participatory surveillance" have been used before by Mark Poster, 1990. *The mode of information: Poststructuralism and social context.* Chicago: University of Chicago Press, and T.L. Taylor, 2006. "Does WoW change everything? How a PvP server, multinational player base, and surveillance mod scene caused me pause," *Games & Culture*, volume 1, number 4, pp. 318–337. Poster argues that today's circuits of communication and databases constitute a superpanopticon, where individuals are not just disciplined but take active part in their own surveillance even more by continuously contributing with information to databases. Taylor uses the concept to study collaborative play in the online computer game *World of Warcraft*, arguing that norms and coercion, play and pleasure are not necessarily antithetical.

6. Lyon, 2006, p. 4.

7. Andrejevic, 2005, p. 488.

8. Andrejevic, 2005, p. 494.

9. Koskela, 2004, p. 206.

10. Koskela, 2004, p. 210.

References

Alexa, 2008. "Alexa.com's Web site rankings system — Myspace.com," at http://www.alexa.com/data/details/traffic_details/myspace.com, accessed 30 January 2008.

Mark Andrejevic, 2005. "The work of watching one another: Lateral surveillance, risk, and governance," *Surveillance & Society*, volume 2, number 4, pp. 479–497, and at http://www.surveillance-and-society.org/articles2(4)/lateral.pdf, accessed 28 February 2008.

Kirstie Ball and David C. Wilson, 2000. "Power, control and computer–based performance monitoring: Repertoires, resistance, and subjectivities," *Organization Studies*, volume 21, number 3, pp. 539–565.

danah boyd, 2007a. "Social network sites: Public, private, or what?" *The Knowledge Tree*, edition 13 (May), at http://kt.flexiblelearning.net.au/tkt2007/?page_id=28, accessed 30 January 2008.

danah boyd, 2007b. "We Googled you: Should Fred hire Mimi despite her online history?" Case commentary, *Harvard Business Review* (June), at http://www.danah.org/papers/HBRJune2007.html, accessed 30 January 2008.

danah boyd and Nicole B. Ellison, 2007. "Social network sites: Definition, history, and scholarship," *Journal of Computer–Mediated Communication*, volume 13, number 1, at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, 30 January 2008.

danah boyd and Henry Jenkins, 2006. "MySpace and Deleting Online Predators Act (DOPA)," *MIT Tech Talk* (26 May), at http://www.danah.org/papers/MySpaceDOPA.html, accessed 28 February 2008.

Chaddus Bruce, 2007. "CIA Gets in your Face(book)," *Wired*, at http://www.wired.com/techbiz/it/news/2007/01/72545, accessed 30 January 2008.

Jamais Cascio, 2006. "The rise of the participatory panopticon," *WorldChanging*, at http://www.worldchanging.com/archives//002651.html, accessed 30 January 2008.

Nicole B. Ellison, Charles Steinfield and Cliff Lampe, 2007. "The benefits of Facebook 'friends': Social capital and college students' use of online social network sites," *Journal of Computer–Mediated Communication*, volume 12, number 4, at http://jcmc.indiana.edu/vol12/issue4/ellison.html, 30 January 2008.

Michel Foucault, 1975. *Surveiller et punir: Naissance de la prison*. Paris: Gallimard.

Christian Fuchs, 2005. "The Internet as a self–organizing socio–technological system," *Cybernetics & Human Knowing*, volume 12, number 3, pp. 37–81.

William Gibson, 1984. *Neuromancer*. New York: Ace Books.

Stephen Graham, 1998. "The end of geography or the explosion of place? Conceptualizing space, place and information technology," *Progress in Human Geography*, volume 22, number 2, pp. 165–185.

Matt Greenop, 2007. "Facebook — The CIA conspiracy," *new Zealand Herald* (8 August), at http://www.nzherald.co.nz/section/story.cfm?c_id=5&objectid=10456534, accessed 30 January 2008.

Ralph Gross and Alessandro Acquisti, 2005. "Information revelation and privacy in online social networks," In: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (Alexandria, Va.). New York: ACM, pp. 71–80, and at http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf, accessed 28 February 2008.

Gertrude Himmelfarb, 1968. "The haunted house of Jeremy Bentham," In: Gertrude Himmelfarb (editor). *Victorian minds*. New York: Knopf, pp. 32–81.

Alice van der Klei, 2002. "Repeating the Rhizome," *SubStance*, volume 31, number 1, pp. 48–55.

Hille Koskela, 2004. "Webcams, TV shows and mobile phones: Empowering exhibitionism," *Surveillance & Society*, volume 2, numbers 2/3, pp. 199-215, and at http://www.surveillance-and-society.org/articles2(2)/webcams.pdf, accessed 28 February 2008.

Amanda Lenhart and Mary Madden, 2007. *Teens, privacy & online social networks: How teens manage their online identities and personal information in the age of MySpace*. Washington, D.C.: Pew Internet & American Life Project, at http://www.pewinternet.org/PPF/r/211/report_display.asp, accessed 28 February 2008.

David Lyon, 2006. *Theorizing surveillance: The panopticon and beyond*. Cullompton, Devon: Willan Publishing.

David Lyon, 2001. *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

David Lyon, 1994. *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

David Lyon, 1991. "Bentham's Panopticon: From moral architecture to electronic surveillance," *Queen's Quarterly*, volume 98, number 3, pp. 596–617.

Paul Marks, 2006. "Pentagon sets its sights on social networking websites," *NewScientist* (9 June), at http://www.newscientist.com/article/mg19025556.200, accessed 14 July 2007.

Chris Maxcer, 2007. "Cops nab crooks using YouTube," *TechNewsWorld* (6 March), at http://www.technewsworld.com/story/56108.html, accessed 30 January 2008.

John E. McGrath, 2004. *Loving big brother: Performance, privacy and surveillance space*. London: Routledge.

Joyce Y.M. Nip, 2004. "The relationship between online and offline communities: The case of the queer sisters," *Media, Culture & Society*, volume 26, number 3, pp. 409–428.

George Orwell, 1949. *Nineteen eighty–four, a novel*. London: Secker & Warburg.

Malcolm R. Parks and Kory Floyd, 1996. "Making friends in cyberspace," *Journal of Computer–Mediated Communication*, volume 1, number 4, at http://jcmc.indiana.edu/vol1/issue4/parks.html, accessed 30 January 2008.

Mark Poster, 1990. *The mode of information: Poststructuralism and social context*. Chicago: University of Chicago Press.

Mark Poster, 1996. "Databases as discourse; or, Electronic interpellations," In David Lyon and Elia Zureik (editors). *Computers, surveillance, and privacy*. Minneapolis: University of Minnesota Press, pp. 175–192.

Wade Roush, 2006. "The moral panic over social–networking sites," *Technology Review* (7 August), at http://www.technologyreview.com/Infotech/17266/, accessed 30 January 2008.

Clay Shirky, 2005. "Ontology is overrated: Categories, links, and tags," at http://www.shirky.com/writings/ontology_overrated.html, accessed 30 January 2008.

T.L. Taylor, 2006. "Does WoW change everything? How a PvP server, multinational player base, and surveillance mod scene caused me pause," *Games & Culture*, volume 1, number 4, pp. 318–337.

Ivan Tribble, 2005a. "Bloggers need not apply," *Chronicle of Higher Education* (8 July), at http://chronicle.com/jobs/2005/07/2005070801c.htm, accessed 30 January 2008.

Ivan Tribble, 2005b. "They shoot messengers, don't they?" *Chronicle of Higher Education* (2 September), at http://chronicle.com/jobs/2005/09/2005090201c.htm, accessed 30 January 2008.

Online Social networking as participatory surveillance
by Anders Albrechtslund
First Monday, Volume 13, Number 3 - 3 March 2008
https://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/2142/1949