Sociology Compass 5/2 (2011): 134–147, 10.1111/j.1751-9020.2010.00354.x

New Media, Web 2.0 and Surveillance

Christian Fuchs*
Uppsala University

Abstract

This article outlines some basic foundations and academic controversies about Web 2.0 surveillance. Contemporary web platforms, such as Google or Facebook store, process, analyse, and sell large amounts of personal data and user behaviour data. This phenomenon makes studying Internet surveillance and web 2.0 surveillance important. Surveillance can either be defined in a neutral or a negative way. Depending on which surveillance concept one chooses, Internet/web 2.0 surveillance will be defined in different ways. Web 2.0 surveillance studies are in an early stage of development. The debate thus far suggests that one might distinguish between a cultural studies approach and a critical political economy approach in studying web 2.0 surveillance. Web 2.0 surveillance is a form of surveillance that exerts power and domination by making use specific qualities of the contemporary Internet, such as user-generated content and permanent dynamic communication flows. It can be characterized as a system of panoptic sorting, mass self-surveillance and personal mass dataveillance. Facebook is a prototypical example of web 2.0 surveillance that serves economic ends. The problems of Facebook surveillance in particular and web 2.0 surveillance in general include: the complexity of the terms of use and privacy policies, digital inequality, lack of democracy, the commercialization of the Internet, the advancement of market concentration, the attempted manipulation of needs, limitation of the freedom to choose, unpaid value creation of users and intransparency.

Introduction

Facebook is the most popular social networking site (SNS). SNS are typical applications of what is termed web 2.0, they are web-based platforms that integrate different media, information and communication technologies, that allow at least the generation of profiles that display information that describes the users, the display of connections (connection list), the establishment of connections between users that are displayed on their connection lists and the communication between users (Fuchs 2009).

Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz and Chris Hughes, who were then Harvard students, founded Facebook in 2004. Facebook is the second most often accessed website in the world (data source: alexa.com, accessed on 9 October 2010); 34.8% of all Internet users have accessed Facebook in the 3-month period from 10 June to 10 September 2010 (data source: alexa.com, accessed on 9 October 2010). This means that more than 680 million individuals are Facebook users (data source for worldwide Internet users: http://www.internetworldstats.com/stats.htm, accessed on 9 October 2010). Facebook's revenues were more than $US 800 million in 2009 (Reuters: Facebook '09 revenue neared $800 million, http://www.reuters.com/article/idUSTRE65H01W20100618, accessed on 9 October 2010) and is likely to increase to more than $US 1 billion in 2010 (Mashable/Business: Facebook could surpass $1 billion in revenue this year, http://mashable.com/2010/03/02/facebook-could-surpass-1-billion-in-revenue-this-year, accessed on 9 October 2010).

The popularity of Facebook makes it an excellent example for explaining how Internet surveillance works. It will therefore be used throughout this paper as case that helps to apply theoretical categories to the real world of Internet surveillance in order to show how exactly surveillance works on the contemporary Internet.

The task of this paper is to discuss some foundations of web 2.0 surveillance and to show how this kind of surveillance works. In the section 'Theoretical Foundations of Surveillance Studies', I will discuss the notion of surveillance. In the section 'Web 2.0 Surveillance', aspects of web 2.0 surveillance are outlined.

Theoretical foundations of surveillance studies

'Living in ''surveillance societies'' may throw up challenges of a fundamental – ontological – kind' (Lyon 1994, 19). Social theory is a way of clarifying such ontological questions that concern the basic nature and reality of surveillance. An important ontological question is how to define surveillance. One can distinguish neutral concepts and negative concepts.

For Max Horkheimer, neutral theories 'define universal concepts under which all facts in the field in question are to be subsumed' (Horkheimer 1937/2002, 224). Neutral surveillance approaches define surveillance as the systematic collection of data about humans or non-humans. They argue that surveillance is a characteristic of all societies. An example for a well-known neutral concept of surveillance is the one of Anthony Giddens. For Giddens, surveillance is 'the coding of information relevant to the administration of subject populations, plus their direct supervision by officials and administrators of all sorts' (Giddens 1984, 183f). Surveillance means 'the collation and integration of information put to administrative purposes' (Giddens 1985, 46). For Giddens, all forms of organization are in need of surveillance in order to work. 'Who says surveillance says organisation' (Giddens 1981, xvii). As a consequence of his general surveillance concept, Giddens says that all modern societies are information societies (Giddens 1987, 27; see also: Lyon 1994, 27).

Basic assumptions of neutral surveillance concepts are:

- There are positive aspects of surveillance.
- Surveillance has two faces, it is enabling and constrainig.
- Surveillance is a fundamental aspect of all societies.
- Surveillance is necessary for organization.
- Any kind of systematic information gathering is surveillance.

Based on a neutral surveillance concept, all forms of online information storage, processing and usage in organizations are types of Internet surveillance. Examples include: the storage of company information on a company website, e-mail communication between employees in a governmental department, the storage of entries on Wikipedia, the online submission and storage of appointments in an e-health system run by a hospital or a general practitioner's office. The example shows that based on a neutral concept of surveillance, the notion of Internet surveillance is fairly broad.

Negative approaches see surveillance as a form of systematic information gathering that is connected to domination, coercion, the threat of using violence or the actual use of violence in order to attain certain goals and accumulate power, in many cases against the will of those who are under surveillance. Max Horkheimer (1947/1974) says that the 'method of negation' means 'the denunciation of everything that mutilates mankind and impedes its free development' (Horkheimer 1947/1974, 126). For Herbert Marcuse,

negative concepts 'are an indictment of the totality of the existing order' (Marcuse 1941, 258).

The best-known negative concept of surveillance is the one of Michel Foucault. For Foucault, surveillance is a form of disciplinary power. Disciplines are 'general formulas of domination' (Foucault 1977, 137). They enclose, normalize, punish, hierarchize, homogenize, differentiate and exclude (Foucault 1977, 183f). The 'means of coercion make those on whom they are applied clearly visible' (Foucault 1977, 171). A person that is under surveillance 'is seen, but he does not see; he is the object of information, never a subject in communication' (Foucault 1977, 200). The surveillant panopticon is a 'machine of power' (Foucault 2007, 93f).

In my opinion, there are important arguments speaking against defining surveillance in a neutral way:

1. Etymology: The French word *surveiller* means to oversee, to watch over. It implies a hierarchy and is therefore connected to notions, such as watcher, watchmen, overseer and officer. Surveillance should therefore be conceived as technique of coercion (Foucault 1977, 222), as 'power exercised over him [an individual] through supervision' (Foucault 1994, 84).
2. Theoretical conflationism: Neutral concepts of surveillance put certain phenomena, such as taking care of a baby or the electrocardiogram of a myocardial infarction patient, on one analytical level with very different phenomena, such as preemptive state-surveillance of personal data of citizens for fighting terrorism or the economic surveillance of private data or online behaviour by Internet companies (Facebook, Google, etc.) for accumulating capital with the help of targeted advertising. Neutral concepts might therefore be used for legitimatizing coercive forms of surveillance by arguing that surveillance is ubiquitous and therefore unproblematic.
3. Difference between information gathering and surveillance: If surveillance is conceived as systematic information gathering, then no difference can be drawn between surveillance studies and information society studies and between a surveillance society and an information society. Therefore, given these circumstances, there are no grounds for claiming the existence of surveillance studies as discipline or transdiscipline (as argued, for example, by Lyon 2007)
4. The normalization of surveillance: If everything is surveillance, it becomes difficult to criticize coercive surveillance politically.

Given these drawbacks of neutral surveillance concepts, I prefer to define surveillance as a negative concept: surveillance is the collection of data on individuals or groups that are used so that control and discipline of behaviour can be exercised by the threat of being targeted by violence. A negative concept of surveillance allows drawing a clear distinction of what is and what is not Internet surveillance. Here are, based on a negative surveillance concept, some examples for Internet surveillance processes (connected to: harm, coercion, violence, power, control, manipulation, domination, disciplinary power, involuntary observation):

- Teachers watching private activities of pupils via webcams at Harriton High School, Pennsylvania.
- The scanning of Internet and phone data by secret services with the help of the Echelon system and the Carnivore software.
- Usage of full body scanners at airports.

- The employment of the DoubleClick advertising system by Internet corporations for collecting data about users' online browsing behaviour and providing them with targeted advertising.
- Assessment of personal images and videos of applicants on Facebook by employers prior to a job interview.
- Watching the watchers: corporate watch systems, filming of the police beating of Rodney King (LA 1992), YouTube video of the police killing of Neda Soltan (Iran 2009).

There are other examples of information gathering that are oriented on care, benefits, solidarity, aid and co-operation. I term such processes monitoring. Some examples are:

- Consensual online video sex chat of adults.
- Parents observing their sleeping ill baby with a webcam that is connected to their PC in order to be alarmed when the baby needs their help.
- The voluntary sharing of personal videos and pictures from a trip undertaken with real life friends who participated in the trip by a user.
- A Skype video chat of two friends, who live in different countries and make use of this communication technology for staying in touch.

Web 2.0 surveillance

Tim O'Reilly introduced the notion of web 2.0 in 2005 (O'Reilly 2005). He stressed that many newer web platforms operate as platforms that support various communication functions and technologies and that they constitute an architecture of participation and rich user experience. On the one hand, one can criticize that web 2.0 is a marketing ideology, that the notion of participation underlying web 2.0 is only pseudo-participation, that web 2.0 is dominated by large corporations and commercial interests, that it is an advertising machine, that communication and community-building has also been supported by older Internet applications (Fuchs 2010d). But on the other hand, an empirical analysis of how the World Wide Web has changed in the past decade, shows that although the importance of information and communication on the web has not much changed, web platforms that support information sharing, community-building/maintenance and collaborative information productive have become more important (Fuchs 2010d). There are continuities and discontinuities in the development of the World Wide Web. In the research literature that web 2.0 is particularly characterized by user-generated content and more intensive and extended web-based communication and co-operation (see, e.g. Beer and Burrows 2007; Boyd 2007; Burg 2004; O'Hara and Shadbolt 2008; Shirky 2009; for a systematic theoretical discussion of web 2.0 definitions, see Fuchs 2010d).

The web is neither completely new, nor is it the same as 10 years ago. One important characteristic of many contemporary web platforms is that they store, process, assess and sell large amounts of personal information and usage behaviour data. It is therefore important to theorize web 2.0 surveillance and conduct empirical research about the surveillance and privacy implications of web 2.0.

Discussions about the surveillance and privacy implications of computing have resulted in the emergence of various theoretical concepts. Roger Clarke (1988) speaks of dataveillance, Mark Poster (1990) of the electronic superpanopticon, David Lyon (1994) of electronic surveillance, Gary T. Marx (2002) of the new surveillance or Graham and Wood (2003/2007) of digital surveillance. In relation to the surveillance capacities of the Internet, David Lyon (1998) has spoken of the World Wide Web of surveillance and Mark

Andrejevic (2007) of the virtual enclosure. Most of these accounts either refer to computing in general or the early phase of the World Wide Web in the 1990s. The surveillance implications of web 2.0 have thus far hardly been theorized. One of the tasks of the collected volume 'The Internet and Surveillance' (anonymized) that I edit together with Kees Boersma, Anders Albrechtslund and Marisol Sandoval in context of the EU COST action 'Living in Surveillance Societies' is to identify qualities of web 2.0 surveillance and to study example cases. Routledge will publish the book in 2011 (Fuchs, Boersma, Albrechtslund and Sandoval 2011). In the course of this paper, I can only introduce a few aspects of web 2.0 surveillance.

Clarke (1994) distinguishes between personal dataveillance that monitors the actions of one or more persons and mass dataveillance, where a group or large population is monitored in order to detect individuals of interest. On web 2.0, the boundaries between these two forms of surveillance become blurred: targeted advertising concerns the large mass of users of commercial web 2.0 platforms because by agreeing to terms of use they agree in most cases to the surveillance of their personal data and their usage behaviour, but this surveillance is fine-tuned in order to detect and store the individual differences and to target each user with a separate mass of advertisings. Web 2.0 surveillance is a form of personal mass dataveillance. Manuel Castells (2009) characterizes web 2.0 communication as mass self-communication. Web 2.0

> is mass communication because it can potentially reach a global audience, as in the posting of a video on YouTube, a blog with RSS links to a number of web sources, or a message to a massive e-mail list. At the same time, it is self-communication because the production of the message is self-generated, the definition of the potential receiver(s) is self-directed, and the retrieval of specific messages or content from the World Wide Web and electronic networks is self-selected. (Castells 2009, 55)

Web 2.0 surveillance is directed at large user groups who help to hegemonically produce and reproduce surveillance by providing user-generated (self-produced) content. We can therefore characterize web 2.0 surveillance as mass self-surveillance.

Facebook is a good example for how personal mass dataveillance/mass self-surveillance works on web 2.0: Facebook is a company, therefore its economic goal is to achieve money profit. It does so with the help of targeted personalized advertising, which means that it tailors advertisements to the consumption interests of the users. SNS are especially suited for targeted advertising because they store and communicate a vast amount of personal likes and dislikes of users so that surveillance of these data for economic purposes and finding out, which products the users are likely to buy, becomes possible. This explains why targeted advertising is the main source of income and the business model of most profit-oriented SNS. Facebook uses mass surveillance because it stores, compares, assesses and sells the personal data and usage behaviour of several 100 million users. But this mass surveillance is personalized and individualized at the same time because the detailed analysis of the interests and browsing behaviour of each user and the comparison to the online behaviour and interests of other users allows to sort the users into consumer interest groups and to provide each individual user with targeted advertisements. The underlying assumption is that algorithmic selection and comparison mechanisms can calculate the users' consumption interests. The combination of the economic surveillance of a large mass of users combined with personalized advertising can therefore be characterized as a form of personal mass dataveillance. For this form of Internet surveillance to work, permanent input and activity of the users are needed, which are guaranteed by the specific characteristics of web 2.0, especially the upload of user-generated content and

permanent communicative flows. This permanent activity is what Castells characterizes as 'self-activity' in mass self-communication. On Facebook and other commercial web 2.0 platforms, mass self-communication is used for the purpose of mass self-surveillance.

The use of targeted advertising and economic surveillance is legally guaranteed by Facebook's privacy policy, which, for example, says:

> We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment. (Facebook Privacy Policy, accessed on 15 September 2010)

Facebook also receives, stores and processes data about usage behaviour of Facebook users on other web platforms, with which Facebook has economic parternship:

> We may institute programs with advertising partners and other websites in which they share information with us. […] We may receive information about whether or not you've seen or interacted with certain ads on other sites in order to measure the effectiveness of those ads. (Facebook Privacy Policy, accessed on 15 September 2010)

This means that if I click on an advertisement on a website or buy a product in an onlineshop and Facebook has a business partnership with the company that runs this site, then I can expect that these data are passed on to Facebook and are used for a period of 180 days for targeting me with individualized advertisements.

Facebook's terms of use and its privacy policy are characteristic for the liberal US data protection policies that are strongly based on business self-regulation. As privacy self-regulation is voluntary, the number of organizations that have engaged in it is very small (Bennett and Raab 2006, 171). 'Self-regulation will always suffer from the perception that it is more symbolic than real because those who are responsible for implementation are those who have a vested interest in the processing of personal data' (Bennett and Raab 2006, 171).

Oscar Gandy has coined the notion of the panoptic sort. It is a form of surveillance that is very important in the age of web 2.0.

> The panoptic sort is a difference machine that sorts individuals into categories and classes on the basis of routine measurements. It is a discriminatory technology that allocates options and opportunities on the basis of those measures and the administrative models that they inform. (Gandy 1993, 15)

It is a system of power and disciplinary surveillance that identifies, classifies and assesses (Gandy 1993, 15). Produsage commodification on web 2.0 (see Fuchs 2010a,b) is a form of panoptic sorting (Gandy 1993): it identifies the interests of users by closely surveilling their personal data and usage behaviour, it classifies them into consumer groups and assesses their interests in comparison to other consumers and in comparison to available advertisements that are then targeted at the users.

Facebook is a panoptic sorting machine. It first *identifies* the interests of the users by requiring them to upload personal data for registering and allowing them to communicate in interests groups, with their friends, and to upload personal user-generated content. When registering a Facebook profile, users are required to input the following data: first name, family name, email, gender, date of birth. Other personal data that users can provide are: school, year of school leaving examination, universities attended, year of final

degree, programmes studied, employer, former employers, type of job, job description, place of employment, duration of employment, profile picture, place of residence, hometown, district of residence, family members including degree of kinship, relationship status, political attitude, religious belief, activities, interests, favourite music, favourite television programmes, favourite movies, favourite books, favourite quotations, self-description, Internet messenger usernames, mobile phone number, fixed line phone number, address, city, neighbourhood, zip code, website address (information as at 17 September 2010). According to the Facebook Privacy Policy (accessed on 17 September 2010), the company also stores the following data about users: type of computer, used browser, cookie data, data about the usage of Facebook applications, data about behaviour on other websites, browsing behaviour on other Facebook profiles, data about users that stems from other profiles. In a second step of the Facebook panoptic sort, all of these data are used for *classifying* users into consumer groups. In the third step, a comparative *assessment* of the interests of users and available advertisements is conducted, ads that match specific interests are selected and presented to the users. The description of this example process shows that surveillance on Facebook and other commercial web 2.0 platforms is a form of panoptic online sorting that is based on identification, classification and assessment.

Foucault characterized surveillance: 'He is seen, but he does not see; he is the object of information, never a subject in communication' (Foucault 1977, 200). With the rise of 'web 2.0', the Internet has become a universal communication system, which is shaped by privileged data control by corporations that own most of the communication-enabling web platforms and by the state that can gain access to personal data by law. On the Internet, the separation between 'objects of information' and 'subjects in communication' that Foucault (1977, 200) described for historical forms of surveillance no longer exists, by being subjects of communication on the Internet, users make available personal data to others and continuously communicate over the Internet. On Facebook, they, for example, frequently upload location information, status and mood messages, activity messages, comments to other profiles, videos and pictures. They are very active subjects in communication. This permanent, creative online activity becomes the object of surveillance. Facebook stands for the permanent active creativity of users that becomes instantly commodified, it is a machine that totally commodifies human creativity and communication. Web 2.0 communications are mainly mediated by corporate-owned platforms, therefore the subjects of communication become objects of information for corporations and the state in surveillance processes. Foucault argues that power relations are different from relationships of communication, although they are frequently connected (Foucault 1994, 337). 'Power relations are exercised, to an exceedingly important extent, through the production and exchange of signs', 'relationships of communication […] by modifying the field of information between partners, produce effects of power' (Foucault 1994, 338). On web 2.0, corporate and state power is exercised through the gathering, combination and assessment of personal data that users communicate over the web to others, and the global communication of millions within a heteronomous society that produces the interest of certain actors to exert control over these communications. On web 2.0, power relations and relationships of communication are interlinked. On web 2.0, the users are producers of information (produsers, prosumers), but this creative communicative activity enables the controllers of disciplinary power to closely gain insights into the lives, secrets and consumption preferences of the users.

Solove (2008, chapter 5) has worked out a model of different privacy violations that is based on a model of information processing. There is a data subject and a data holder.

Privacy violations can occur in relation to the data subject (invasion) or in relation to the data holder (information collection, processing or dissemination). Based on these four groups of harmful violations, Solove distinguishes 16 forms of privacy violations. Many of these forms can be found when analysing the economic operations of Facebook: Facebook watches and records usage behaviour and personal data uploaded and entered by users (surveillance), it aggregates information about users that is obtained from Facebook and other sites (aggregation), based on aggregation it identifies the consumer interests of users (identification), it is unclear to whom exactly the data are shared for economic purposes (exclusion from knowledge about data use, one can here also speak of the intransparency of data use), the data are exploited for profit generation and therefore for economic purposes (data appropriation, understood as 'the use of the data subject's identity to serve another's aims and interests', Solove 2008, 105). The surveillance, aggregation, identification, intransparency and appropriation of personal data and usage data are essential activities of Facebook that serve economic purposes. They are all part of Facebook's business model that is based on targeted personalized advertising. Solove defines secondary use as a privacy violation, where data are used for a purpose without the data subject's consent. Commercial SNS are primarily used because they allow users to communicate with their friends, colleagues and others, and to establish new relationships (Fuchs 2009, 2010c,e). Their privacy policies are complex and long. Although users formally agree to the commercial usage of their data, they do not automatically morally agree and express concerns about data appropriation for economic purposes (Fuchs 2009, 2010c,e). One can therefore here also speak of a secondary data use in a specific normative sense.

Some scholars have argued that there are primarily positive aspects of emancipation or resistance of web 2.0 surveillance: Albrechtslund (2008) speaks of participatory Internet surveillance; Whitaker (1999), Campbell and Carlson (2002) and Cascio (2005) describe the Internet as participatory panopticon; Dennis (2008) uses the notion of the participatory/social panopticon. These authors base their notions of Internet/web 2.0 surveillance on neutral surveillance concept. Other authors in contrast stress that web 2.0 surveillance is a process of exploitation and class formation (e.g. Andrejevic 2007; Fuchs 2010a,b). They understand Internet/web 2.0 surveillance as a negative process. In analogy to the debate between cultural studies scholars and representatives of the critical political economy of the media and communication (Garnham 1998; Grossberg 1998), one can say that in surveillance studies, there is a difference between cultural studies of web 2.0 surveillance-approaches and the critical political economy of web 2.0 surveillance-approach.

Based on a critical theory of technology, the Internet in contemporary society can be described and analysed as a dialectical system that contains both opportunities and risks that stand in contradiction to each other (Fuchs 2008). The Internet therefore is both a system of co-operation and competition (Fuchs 2008). In the context of surveillance, this means that power and counter-power, hegemony and counter-hegemony, surveillance and counter-surveillance are inherent potentialities of the Internet and web 2.0. But, we cannot assume that these potentials are symmetrically distributed because conducting surveillance requires resources (humans, money, technology, time, political influence, etc.). The two most powerful collective actors in capitalist societies are corporations and state institutions. It is therefore likely that companies and state institutions are dominant actors in Internet and web 2.0 surveillance and that there is an asymmetric dialectic of Internet/web 2.0 surveillance and counter-surveillance. Toshimaru Ogura (2006, 272) stresses that 'the common characteristics of surveillance are the management of population based on capitalism and the nation state'. Oscar Gandy points out that the 'panoptic sort is a technology that

has been designed and is being continually revised to serve the interests of decision makers within the government and the corporate bureaucracies' (Gandy 1993, 95). Both Ogura and Gandy argue based on critical political economy approaches that economic and political actors have particular power in modern surveillance. Counter-surveillance as form of protest politics and resistance against surveillance are possible, but are not so easy to organize due to power asymmetries. The actual distribution of power in web 2.0 surveillance relations can only be studied empirically. What is needed is a materialistic and critical theory of web 2.0 surveillance as well as critical empirical studies of web 2.0 surveillance that are theoretically grounded. The actual reality of the Internet and society shows the political importance of these academic endeavours.

Conclusion: the problems of web 2.0 surveillance

This article outlined some basic foundations and academic controversies about web 2.0 surveillance. Contemporary web platforms, such as Google or Facebook, store, process, analyse and sell large amounts of personal data and user behaviour data. This phenomenon makes studying Internet surveillance and web 2.0 surveillance important. Surveillance can either be defined in a neutral or a negative way. Depending on which surveillance concept one chooses, Internet/web 2.0 surveillance will be defined in different ways. Web 2.0 surveillance studies are in an early stage of development. The debate thus far suggests that one might distinguish between a cultural studies approach and a critical political economy approach in studying web 2.0 surveillance. The cultural studies-like approach stresses aspects of emancipation and resistance immanent in web 2.0, just like many cultural studies approaches stress resistant and oppositional forms of media reception and cultural practices. Critical political economy approaches either stress aspects of exploitation, class and domination that are connected to web 2.0 surveillance or the asymmetric dialectic of web 2.0 surveillance, just like the critical political economy of the media and communication-approach focuses on the power structure analysis and dialectical analysis of the media and communication. The first approach is closer to neutral and positive surveillance theories, whereas the second is closer to negative and dialectical surveillance theories.

An important question is, why corporate web 2.0 surveillance on Facebook and other profit-oriented web 2.0 platforms is harmful and problematic? There are several points that need to be taken into account.

Complexity of the terms of use and privacy policies

Such terms and policies are frequently very long and written in a complex, judicial language. Therefore, one can doubt that all users read the details and really agree with all rules. The current English version of the Facebook privacy policy (version from 5 October 2010) has 35 553 characters, which are approximately 11 single-spaced text pages. The current Facebook terms of use have 23 540 characters (version from 4 October 2010), which are approximately eight text pages. How likely is it that hundred of millions Facebook users study these rules thoroughly and completely, understand all details and agree to all rules?

Unequal Internet skills, digital inequality

Not all users have excellent Internet usage skills, which is an aspect of digital inequality. Therefore, we can assume that privacy mechanisms that need to be activated to work and the opt-out from advertising options are less likely to be used by those who have low

Internet skills. The common automatic full activation of advertising and the automatic large-scale sharing of data characteristic for Facebook and other commercial web 2.0 platforms therefore poses disadvantages for this user group.

Lack of democracy

Users generally have no right to participate in the formulation of the terms of use and privacy policies of Facebook and other corporate web 2.0 platforms. They, however, have to agree to these terms in order to be able to use the platforms. But creating a profile and logging into Facebook, which means automatic 'agreement' to the terms, does not mean that users really agree with the numerous clauses of the usage and privacy terms because when the users do not agree with certain rules, but need to use the service in order to stay in contact with their friends or professional contacts, then they are coerced into usage and to accept the terms that are defined by companies and thereby alienated from the users. On the corporate Internet, the understanding of democracy stops once economic purposes are involved. Users do not have a say in the exact design of corporate web 2.0 platforms. Facebook reacted to the protest of consumer protectionists about privacy violations by installing a forum, in which users can discuss Facebook's terms of use and privacy policy. But discussion possibilities are not a form of decision power, Facebook allows users to discuss, but not to decide. This is a strange understanding of democracy that is more oriented on trying to integrate, manipulate and forestall criticism without making actual improvements.

Commercialization of the Internet

If advertising interrupts my favourite television programme, I can refuse to consume this marketing information by switching to another channel. This is normally not automatically possible on the Internet. If I want to conduct certain tasks on a commercial platform (as, e.g. sending emails, writing blog entries, uploading images and videos, discussing in forums and interest groups, reading and commenting the guest books and profiles of my friends), I am in most cases permanently confronted with advertisements on the screen. Even if I do not click on them, I cannot simply switch off advertisements as on TV (except if I use an ad-blocker). Because of the Internet's domination by commercial interests and profit-oriented companies, it is an advertising machine that confronts users permanently with ads in order to motivate them to buy commodities and to surveil their usage behaviour in order to present even more targeted advertisements and to stimulate ever more commodity purchases. Commercial Internet platform operators therefore consider users primarily as the consumers of advertisements and commodities and reduce them to this status.

Market concentration and the manipulation of needs

Personalized advertising presents only certain commodities and services to users – those that are provided by companies that possess enough money for purchasing online ads. Large companies therefore here have advantages over smaller ones and non-commercial organizations. Their products and services are therefore much more present on web 2.0. As a result, targeted online advertising supports the concentration and monopolization of markets. Targeted online advertising is based on the false assumption that the real needs and desires of humans can be algorithmically calculated. That person A likes music of

band X does not automatically mean that s/he also likes the music of band Y because the persons B and C like the music of the bands X and Y. It is also a mistake to assume that users want to be provided with calculated advertising information and consider such information as credible. The attempt of manipulating and steering consumption behaviour by online surveillance assumes that needs and desires can be mathematically computed. But for many humans the development and realization of interests, desires and needs is an active, creative, self-determined search process, in which part of the desire and satisfaction is gained by the active self-discovery of novel interests. Individual discovery and active search are important elements of the development of individuality. Personalized online advertising that is based on the surveillance of online behaviour and personal user data in contrast wants to plan and control needs, which results in the attempted weakening of human creativity.

Coerced advertising and opt-out advertising solutions limit the freedom to choose

Many commercial web 2.0 platforms force their users to provide personal data and usage behaviour for economic surveillance processes that serve the purpose of targeted advertising and capital accumulation. In the case of Facebook, there is, for example, no option to deactivate targeted advertising. On some other platforms, there is the possibility to deactivate certain advertising features. This is a so-called opt-out option. Because one cannot assume that all users agree to personalized advertising, it would be much more democratic to base advertising and targeted advertising on web platforms on an opt-in solution, which means that these features are only activated if a user activates these options. But opt-in to a certain extent questions commercial interests of Internet companies, which explains why opt-in advertising solutions are hardly in use on the web today. This also shows the antagonism between democracy and commercial interests in the corporate Internet. Oscar Gandy has argued that opt-in solutions are democratic and opt-out solutions are undemocratic: If individuals

> wish information or an information-based service, they will seek it out. IT is not unreasonable to assume that individuals would be the best judge of when they are the most interested and therefore most receptive to information of a particular kind. Others with information to provide ought to assume that, unless requested, no information is desired. This would be the positive option. Through a variety of means, individuals would provide a positive indication that yes, I want to learn, hear, see more about this subject at this time. Individuals should be free to choose when they are ready to enter the market for information. (Gandy 1993, 220)

Opt-in solutions give the right of self-determination to individuals, who can decide themselves if and when they want to be confronted by advertisements. Opt-out advertising mechanisms and personalized advertising without opt-out/in (coerced advertising) violate according to Gandy the right to choose.

Unpaid value creation by the users

Personalized advertising means the creation of economic value by users, who are sold as a commodity to advertisers (Fuchs 2010b). The usage behaviour and personal user data are surveilled and transformed into a commodity that is sold on the advertising market. There is an inherent connection of economic surveillance and user commodification/exploitation on the corporate web 2.0 (Fuchs 2010b). If there is money profit, there must be creators of this economic value. In the case of web 2.0, the consumers are at the same time

consumers, so-called prosumers (Fuchs 2010b, Toffler 1980). One can speak of the existence of an Internet prosumer commodity – the users and their data are sold as commodities for advertising purposes (Fuchs 2010b). In contrast to slavery, in capitalist society productive labour is normally remunerated by wages (although the wage does not equal the created value so that unpaid surplus value exists as the source of profit). On corporate web 2.0, value creation by the users is unremunerated. Therefore, we can speak of the slave-like exploitation of Internet prosumers on the corporate web 2.0. Economic web 2.0 surveillance is inherently tied to user exploitation. It is a necessary element in the production and exploitation of value in the online world of web 2.0. User exploitation is part of the web 2.0 business model that also uses targeted advertising and economic data surveillance.

The intransparency of online surveillance

Online surveillance is a complex process, in which multiple data sources and databases are interconnected and permanently updated. The collection of personal data and usage behaviour by multiple platforms and the interconnection of these data make it almost impossible for the single user to know, which data about her/him are stored by whom and in which database and who exactly has access to these data. Web 2.0 surveillance is highly intransparent to the users.

Web 2.0 surveillance is a form of surveillance that exerts power and domination by making use specific qualities of the contemporary Internet, such as user-generated content and permanent dynamic communication flows. It can be characterized as a system of panoptic sorting, mass self-surveillance and personal mass dataveillance. Facebook is a prototypical example of web 2.0 surveillance that serves economic ends. The problems of Facebook surveillance in particular and web 2.0 surveillance in general include: the complexity of the terms of use and privacy policies, digital inequality, lack of democracy, the commercialization of the Internet, the advancement of market concentration, the attempted manipulation of needs, limitation of the freedom to choose, unpaid value creation of users and intransparency. Web 2.0 surveillance is a relatively novel phenomenon that has hardly been analysed and theorized. In order to limit the risks of this form of surveillance, more studies and theories are needed that show how web 2.0 surveillance works, what it risks are, and what actions can be taken at the political level.

Acknowledgement

The research presented in this paper was conducted in the project 'Social Networking Sites in the Surveillance Society', funded by the Austrian Science Fund (FWF): project number P 22445-G17. Project co-ordination: Dr Christian Fuchs.

Short Biography

Christian Fuchs holds the Chair in Media and Communication Studies at Uppsala University's Department of Informatics and Media. He is also board member of the Unified Theory of Information Research Group, Austria, and editor of tripleC (cognition, communication, co-operation): *Journal for a Global Sustainable Information Society*. He studied computer science at the Vienna University of Technology in the years 1994–2000. He completed his PhD in 2002 at the Vienna University of Technology. In 2000–2006, he was lecturer for information society studies at the Institute of Design and Technology

Assessment of the Vienna University of Technology. He was a research associate at the same department in the years 2002–2004. At the University of Salzburg, he was an assistant professor in the years 2005–2007 and associate professor from 2008 to 2010 in the field of ICTs and society. His main research fields are: social theory, critical theory, political economy of media, information, technology; information society studies, ICTs and society. He is author of more than 120 academic publications, including the books *Internet and Society: Social Theory in the Information Age* (New York: Routledge 2008; Paperback 2011) and *Foundations of Critical Media and Information Studies* (New York: Routledge, 2011). He is co-editor of *The Internet and Surveillance* (New York: Routledge 2011; edited together with Kees Boersma, Anders Albrechtslund and Marisol Sandoval). He is co-ordinator of the research project 'Social Networking Sites in the Surveillance Society' (2010–2013), which is funded by the Austrian Science Fund FWF.

Note

* Correspondence address: Christian Fuchs, Department of Informatics and Media Studies, Uppsala University, Kyrkogårdsgatan 10, Box 513, Uppsala 751 20, Sweden. E-mail: christian.fuchs@im.uu.se; Unified Theory of Information Research Group, Steinbrechergasse 15, 1220 Vienna, Austria. E-mail: christian.fuchs@uti.at

References

Albrechtslund, Anders. 2008. 'Online Social Networking as Participatory Surveillance.' *Firs Monday* **13**(3).
Andrejevic, Mark. 2007. *ISpy: Surveillance and Power in the Interactive Era*. Lawrence: University Press of Kansas.
Beer, David and Roger Burrows. 2007. 'Sociology and, of and in Web 2.0: Some Initital Considerations.' *Sociological Research Online* **12**(5).
Bennett, Colin and Charles Raab. 2006. *The Governance of Privacy*. Cambridge, MA: MIT Press.
Boyd, Danah. 2007. 'The Significance of Social Software.' Pp. 15–30 in *BlogTalks Reloaded*, edited by Thomas N. Burg. Norderstedt: Books on Demand.
Burg, Thomas N. 2004. 'Social Software – An Emancipation.' Pp. 7–14 in *BlogTalks 2.0*, edited by Thomas N. Burg. Norderstedt: Books on Demand.
Campbell, John E. and M. Matt Carlson. 2002. 'Panopticon.com: Online Surveillance and the Commodification of Privacy.' *Journal of Broadcasting & Electronic Media* **46**(4): 586–606.
Cascio, Jamais. 2005. *The Rise of the Digital Panopticon*. http://www.worldchanging.com/archives/002651.html (Last Accessed 5 September 2009).
Castells, Manuel. 2009. *Communication Power*. Oxford: Oxford University Press.
Clarke, Roger. 1988. 'Information Technology and Dataveillance.' *Communications of the ACM* **31**(5): 498–512.
Clarke, Roger. 1994. 'Dataveillance: Delivering '1984'.' Pp. 117–30 in *Framing Technology: Society, Choice and Change*, edited by Lelia Green and Roger Guinery. Sydney: Allen & Unwin.
Dennis, Kingsley. 2008. 'Keeping a Close Watch – The Rise of Self-Surveillance and the Threat of Digital Exposure.' *The Sociological Review* **56**(3): 347–57.
Foucault, Michel. 1977. *Discipline & Punish*. New York: Vintage.
Foucault, Michel. 1994. *Power*. New York: New Press.
Foucault, Michel. 2007. *Security, Territory, Population*. Basingstoke: Palgrave Macmillan.
Fuchs, Christian. 2008. *Internet and Society: Social Theory in the Information Age*. New York: Routledge.
Fuchs, Christian. 2009. *Social Networking Sites and the Surveillance Society*. Salzburg, Vienna: Unified Theory of Information Research Group.
Fuchs, Christian. 2010a. 'Class, Knowledge, and New Media.' *Media, Culture & Society* **32**(1): 141–50.
Fuchs, Christian. 2010b. 'Labour in Informational Capitalism.' *The Information Society* **26**(3): 179–96.
Fuchs, Christian. 2010c. 'Social Networking Sites and Complex Technology Assessment.' *International Journal of E-Politics* **1**(3): 19–38.
Fuchs, Christian. 2010d. 'Social Software and Web 2.0: Their Sociological Foundations and Implications.' Pp. 764–89 in *Handbook of Research on Web 2.0, 3.0, and X.0: Technologies, Business, and Social Applications*. Volume II, edited by S. Murugesan. Hershey, PA: IGI-Global.
Fuchs, Christian. 2010e. 'studiVZ: Social Networking Sites in the Surveillance Society.' *Ethics and Information Technology* **12**(2): 171–85.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds) 2011. *The Internet and Surveillance*. New York: Routledge.
Gandy, Oscar H. 1993. *The Panoptic Sort. A Political Economy of Personal Information*. Boulder: Westview Press.
Garnham, Nicholas. 1998. 'Political Economy and Cultural Studies. Reconciliation or Divorce.' Pp. 600–12 in *Cultural Theory and Popular Culture: A Reader*, edited by John Storey. Edinburgh: Pearson.
Giddens, Anthony. 1981. *A Contemporary Critique of Historical Aterialism. Vol. 1: Power, Property and the State*. London: Macmillan.
Giddens, Anthony. 1984. *The Constitution of Society. Outline of the Theory of Structuration*. Cambridge: Polity Press.
Giddens, Anthony. 1985. *A Contemporary Critique of Historical Materialism. Vol. 2: The Nation-State and Violence*. Cambridge: Polity Press.
Giddens, Anthony. 1987. *Social Theory and Modern Sociology*. Cambridge: Polity Press.
Graham, Stephen and David Wood. 2003/2007. 'Digitizing Surveillance: Categorization, Space, Inequality.' Pp. 218–30 in *The Surveillance Studies Reader*, edited by Sean P. Hier and Josh Greenberg. Berkshire: Open University Press.
Grossberg, Lawrence. 1998. 'Cultural Studies vs. Political Economy. Is Anybody Else Bored With This Debate?.' Pp. 613–24 in *Cultural Theory and Popular Culture: A Reader*, edited by John Storey. Edinburgh: Pearson.
Horkheimer, Max. 1937/2002. 'Traditional and Critical Theory.' Pp. 188–252 in *Critical Theory*. New York: Continuum.
Horkheimer, Max. 1947/1974. *Eclipse of Reason*. New York: Continuum.
Lyon, David. 1994. *The Electronic eye. The Rise of Surveillance Society*. Cambridge: Polity.
Lyon, David. 1998. 'The World Wide Web of Surveillance. The Internet and off-World Power-Flows.' *Information, Communication & Society* **1**(1): 91–105.
Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.
Marcuse, Herbert. 1941. *Reason and Revolution. Hegel and the Rise of Social Theory*. New York: Humanity Books.
Marx, Gary T. 2002. 'What's new About the ''new Surveillance''? Classifying for Change and Continuity.' *Surveillance & Society* **1**(1): 9–29.
Ogura, Toshimaru. 2006. 'Electronic Government and Surveillance-Oriented Society.' Pp. 270–95 in *Theorizing Surveillance*, edited by David Lyon. Portland, OR: Willan.
O'Hara, Kieron and Nigel Shadbolt. 2008. *The spy in the Coffee Machine*. Oxford: Oneworld.
O'Reilly, Tim. 2005. *What is web 2.0?* http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html?page=1 (Last Accessed 10 August 2009).
Poster, Mark. 1990. *The Mode of Information*. Cambridge: Polity.
Shirky, Clay. 2009. *Here Comes Everybody*. New York: Penguin.
Solove, Daniel J. 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.
Toffler, Alvin. 1980. *The Third Wave*. New York: Bantam.
Whitaker, Reginald. 1999. *The End of Privacy*. New York: New Press.