22. Social media surveillance

Christian Fuchs

INTRODUCTION

Privacy is not a phenomenon specific to digital media like the Internet. Modern thinking about privacy and surveillance has for a long time been bound up with the media: Warren and Brandeis defined privacy as a right to be left alone and situated this understanding in the context of the tabloid press:

> The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. (Warren and Brandeis, 1890: 196)

Privacy has been defined either as the right to be left alone or as the right to determine for oneself which areas of life should be accessible to others – or as a combination of the two (Tavani, 2008). In the context of information processing, privacy plays a role because information about the lives of humans can become publicly available and the question arises: which rules shall regulate the becoming public of such information?

Some scholars have defined surveillance as the systematic gathering and processing of personal data for the management of individuals or groups. Others stress that surveillance tries to bring about or to prevent certain behaviours in groups or individuals by gathering, storing, processing, diffusing, assessing and using data (Fuchs, 2011c). Just like privacy, surveillance is also not a phenomenon specific to digital media, which becomes clear in Foucault's (1977) work, which has shown that surveillance is bound up with the history of control, the prison system, the state and the class-structured economies.

There is a debate between scholars studying privacy and surveillance about the relevance of these two concepts. Whereas some argue that privacy is a liberal and individualistic concept and that surveillance is a more critical concept that can focus on the structural implications of data collection in society, others argue that although privacy advocates may not always be successful in preventing the negative effects of state and corporate surveillance, they at least try to bring about political intervention (Bennett, 2011a, 2011b; Boyd, 2011; Gilliom, 2001; Regan, 1995; Stalder, 2011).

Although privacy and surveillance are not new, the rise of the computer in society has brought about special public concern for both phenomena. The first national data protection Act was passed in 1973 in Sweden and subsequent laws followed in other countries. It is no accident that this happened in the early 1970s, a time when large-scale computer-based data processing took broader effect in society. The rise of computing and an information society is the context for the establishment of data protection and explains the connection of data protection with informational privacy and surveillance.

Scholars have been aware of the privacy and surveillance implications of computing for quite some time and have in this context coined notions such as the 'new surveillance' (Marx, 1988, 2002), 'dataveillance' (Clarke, 1988, 1994), the 'electronic (super)panopticon' (Poster, 1990), 'electronic surveillance' (Lyon, 1994), 'digital surveillance' (Graham and Wood, 2007), the 'world-wide web of surveillance' (Lyon, 1998), and the 'digital enclosure' (Andrejevic, 2004, 2007).

The rise of the Internet took a quantum leap in the mid-1990s when the World Wide Web (WWW) became popular and commercialized. The early 1990s until after the new millennium were times of a general and scholarly Internet optimism, spurred by neoliberalism and the new entrepreneurialism of the Internet economy. Issues relating to privacy, surveillance and data protection were often considered as outmoded and old-fashioned. Typical books of neoliberal 1990s Internet gurus such as Nicholas Negroponte's (1996) *Being Digital* or Kevin Kelly's (1999) *New Rules for the New Economy* do not contain terms such as 'surveillance' or 'data protection'. Internet optimism suffered a drawback when the dot.com crisis took effect in 2000 and resulted in the bankruptcy of many Internet companies that had been founded on venture capital investments that could not be translated into actual profits. The rise of what was somewhat mistakenly called social media – blogs, social networking sites, microblogs, content sharing sites and wikis – spurred new hopes (and foundations of another financial bubble) that have been represented by Google and Facebook, among others. At the same time, a new neoliberal and techno-deterministic round of techno-optimism emerged. At the same time, 9/11 sparked new wars, a new surveillance offensive and an intensification of conservative law-and-order politics. In this context of heightened state and commercial surveillance, new discussions of about the societal and ethical implications of online media, and especially social media, emerged.

This chapter gives special focus to debates on social media privacy and surveillance. The next section focuses on the discussion of key characteristics of social media surveillance. The chapter then discusses the economic, political and cultural implications of social media surveillance; and the final section draws some conclusions.

WHAT IS SOCIAL MEDIA SURVEILLANCE?

Is the 'social web' a real change in the WWW or a piece of jargon and marketing ideology? Although Tim O'Reilly surely thinks that Web 2.0 denotes actual changes and says that the crucial fact about it is that users as a collective intelligence co-create the value of platforms like Google, Amazon, Wikipedia and Craigslist (O'Reilly and Battelle, 2009: 1), he admits that the term was mainly created for identifying the need of new economic strategies of Internet companies after the dot.com crisis. So he says in a paper published five years after the creation of the term Web 2.0 that this category was 'a statement about the second coming of the Web after the dotcom bust' at a conference that was 'designed to restore confidence in an industry that had lost its way' (O'Reilly and Battelle, 2009: 1).

The question of how social the web is or has become depends on a profoundly social-theoretical question: what does it mean to be social? Are human beings always social, or only if they interact with others? In sociological theory, there are different concepts of the social, such as Émile Durkheim's social facts, Max Weber's social action, Karl Marx's notion of collaborative work (as for example also employed in the concept of computer-supported collaborative work – CSCW), or Ferdinand Tönnies' notion of community (Fuchs, 2010). Depending on which concept of sociality one employs, one gets different answers to the questions of whether the web is social or not, and whether sociality is a new quality of the web or not. Community aspects of the web certainly did not start with Facebook in 2004, but had been used in the 1980s to describe bulletin board systems like the Whole Earth 'Lectronic Link (WELL) (Rheingold, 1993). Collaborative work, for example the cooperative editing of articles performed on Wikipedia, is rather new as a dominant phenomenon on the WWW, but not new in computing (where the concept of CSCW was already the subject of a conference series that started in December 1986 with the 1st ACM Conference on CSCW in Austin, Texas). Neither is the wiki concept new: the WikiWikiWeb was introduced by Ward Cunningham in 1984. All computing systems, and therefore all web applications, can be considered as social because they store and transmit human knowledge that originates in social relations in society. They are objectifications of society and human social relations. Whenever a human uses a computing system or another medium such as a book (even if they do so alone in a room), they interact with an objectification of knowledge, that is, ideas that are stored as objects in media forms. They are the outcomes of social relations. But not all computing systems and web applications support direct communication in which at least two humans mutually exchange symbols that are interpreted as being meaningful. Amazon, for example, mainly provides information about books and other goods one can buy. It is not primarily a tool of communication, but rather a tool of information. In contrast, Facebook has inbuilt communication features that facilitate direct communication between people (mail system, walls for comments, forums, and so on).

The above discussion shows that it is not a simple question to decide whether and how social the WWW actually is. Therefore a theory of Internet and society is needed that identifies multiple dimensions of sociality (such as cognition, communication and cooperation; see Fuchs, 2008, 2010), based on which the continuities and discontinuities of the development of the Internet can be empirically studied. An important theoretical question is: what are the basic characteristics of online and social media surveillance? Fuchs et al. (2012) identify 14 qualities of Internet surveillance based on more general qualities of Internet communication, that are displayed in Table 22.1.

Daniel Trottier and David Lyon (2012) argue that there are five key features of social media surveillance:

- Collaborative identity construction: with the help of image tagging and wall comments, users contribute to the identity construction of others. Users monitor what others say about their friends, contacts and themselves.
- Social media enable the monitoring of individuals' social networks.
- Social media surveillance makes use of social ties that are visible, measurable and searchable.
- Social media surveillance is confronted with continuously changing interfaces and contents.
- Social media surveillance is surveillance of profiles that hold information from many different social contexts, that is, of 'social convergence'. (Trottier and Lyon, 2012: 102)

Daniel Trottier (2012) argues that social media augments surveillance. 'By sharing not only the same body of information, but also the same interface used to access that information, formerly discrete surveillance practices feed off one another' (Trottier, 2012). On social media, there are:

Table 22.1 Qualities of Internet surveillance

Dimension	Quality of Internet communication	Quality of Internet surveillance
1. Space	*Global communication* Global communication at a distance, global information space	*Global surveillance* Surveillance at a distance is possible from all nodes in the network, not just from a single point; combination and collection of many data items about certain individuals from a global information space
2. Time	*Real-time (synchronous) or asynchronous global communication*	*Real-time surveillance* Surveillance of real time communication, surveillance of stored asynchronous communication, surveillance of communication protocols and multiple data traces
3. Speed	*High-speed data transmission*	*High-speed surveillance* Availability of high-speed surveillance systems
4. Size	*Miniaturization* Storage capacity per chip increases rapidly (Moore's law)	*Surveillance data growth* Ever more data on individuals can be stored for surveillance purposes on storage devices that become smaller and cheaper over time
5. Reproduction	*Data multiplicity* Digital data can copied easily, cheaply and endlessly; copying does not destroy the original data	*Surveillance data multiplicity* Surveillance becomes easy and cheap; if multiple copies of data exist, specific data are easier to find
6. Sensual modality	*Multimedia* Digital combination of text, sound, image, animation and video in one integrated medium	*Multimodal surveillance* Surveillance of multi-sensual data over one medium
7. Communication flow	*Many-to-many communication*	*Social network surveillance* The multiple personal and professional social networks of individuals become visible and can be traced

Table 22.1 (continued)

Dimension	Quality of Internet communication	Quality of Internet surveillance
8. Information structure	*Hypertext* Networked, interlinked and hypertextual information structures	*Linked surveillance* The links between persons can be easier observed
9. Reception	*Online produsage* Recipients become producers of information (produsers, prosumers)	*Economic exploitation of produsage* Economic exploitation of produsage, new capital accumulation strategies based on active, creative users that are sold to advertisers as produsage commodity, targeted advertising based on continuous surveillance of user-generated content
10. Mode of interaction and sociality	*Online cooperation* Cooperative information production at a distance, information sharing at a distance	*Enclosure of digital commons* Laws that enable the surveillance of sharing and cooperation, intellectual property rights
11. Context	*Decontextualization* Decontextualized information and anonymity (for example, authorship, time and place of production might be unclear)	*Intensification of surveillance* Decontextualization advances speculative and pre-emptive surveillance
12. Reality	*Derealization* The boundaries between actuality and fiction can be blurred	*Intensification of surveillance* Fictive reality might be taken for actual reality by surveillers, which puts people at risk and intensifies surveillance
13. Identity and emotions	*Emotive Internet* The Internet is a very expressive medium that allows identity construction and representation online	*Personalized surveillance* Surveillance of very personal characteristics of individuals and their emotions becomes possible

Table 22.1 (continued)

Dimension	Quality of Internet communication	Quality of Internet surveillance
14. Availability	*Ubiquitous Internet* The Internet has become ubiquitous in all spheres of everyd ay life	*Ubiquitous surveillance* In a heteronomous society, there is constant and profound surveillance of Internet information and communication for economic, political, judicial and other aims

Source: Fuchs et al. (2012: 16–19).

> individuals watching over one another, institutions watching over a key population, businesses watching over their market and investigators watching over populations . . . Individual, institutional, market and investigative scrutiny all rely on the same interface. Thus, familiarity with the site as an interpersonal user facilitates other uses. In addition to relying on the same interface, these practices also rely on the same body of information. This means that personal information that has been uploaded for any particular purpose will potentially be used for several kinds of surveillance. (Trottier, 2012)

Fuchs and Trottier (2013) argue that one feature of social media is that they integrate forms of sociality as well as integrated social roles. Based on a dialectical model, we can identify three levels or stages of social life that form the 'triple C' process model of information: cognition, communication and cooperation (Fuchs, 2008, 2010). Cognition refers to the status and processes of human thought that create and reproduce knowledge. Humans are not isolated monads, but social beings: they exist in and through their relations with other humans. Communication is a social relation between at least two human beings in which there is a mutual exchange of symbols that are interpreted so that the interaction partners give meaning to them. Communication is the social dimension of human existence. It is based on cognition because communication changes the states of knowledge of the participating communication partners. Based on communication, humans can collaborate. Many communication processes do not result in cooperation, but some do. Collaboration or cooperation means that humans create new qualities of social systems or new social systems together. Cooperation is based on communication and cognition: every cooperation process is also a communication and cognition process; every communication process involves also cognition processes.

An important characteristic of social media is the convergence of the three spheres of sociality. Social media are simultaneously media of cognition, communication and cooperation. The publication of content or an idea on a social networking site, a wiki or a blog can become the foundation of communication, which in turn can spur collaboration.

In modern society, human beings act in different capacities in different social roles. Consider the modern middle-class office worker, who also has roles as a husband, father, lover, friend, voter, citizen, child, fan, neighbour, to say nothing of the various associations to which he may belong. In these different roles, humans are expected to behave according to specific rules that govern the various social systems of which modern society is composed (such as the company, the schools, the family, the Church, fan clubs, political parties, and so on). Habermas mentions the following social roles that are constitutive for modern society: employee, consumer, client, citizen (Habermas, 1987: 320). Other roles, such as for example wife, husband, houseworker, immigrant, convict, and so on, can certainly be added. What is constitutive for modern society is not just the separation of spheres and roles, but also the creation of power structures, in which roles are constituted by power relations (as for example employer–employee, state bureaucracy–citizen, citizen of a nation state–immigrant, manager–assistant, dominant gender roles – marginalized gender roles).

Based on these theoretical foundations, Fuchs and Trottier (2013) argue that integrated and converging surveillance is a specific feature of social media surveillance: On social media such as Facebook, various social activities (cognition, communication, cooperation) in different social roles that belong to our behaviour in systems (economy, state) and the lifeworld (political public, civic spheres, private life) are mapped to single profiles. In this mapping process, data about social activities within social roles are generated. This means that a Facebook profile holds: (1) personal data; (2) communicative data; and (3) social network and community data, in relation to: (1) personal roles (friend, lover, relative, father, mother, child, and so on); (2) civic roles (political public: activist, citizens; civic cultures: audience members, fans, association members, neighbours); and (3) systemic roles (in politics: voter, citizen, client, politician, bureaucrat; in the economy: worker, manager, owner, purchaser or consumer, and so on). The different social roles and activities tend to converge, as for example in situations where the workplace is also a playground, where friendships and intimate relations are formed and where leisure activities are conducted. This means that social media surveillance is an integrated form of surveillance, in which one finds surveillance of different partly converging activities with the help of profiles that hold a complex, networked multitude of data about humans.

This discussion shows that the question of how to understand online and social media's implications for society is a complex one. Basic theoretical questions that arise in this context are: What is social about social media and the Internet? What is privacy? What is surveillance? What are key features and qualities of Internet privacy and Internet surveillance? What are the key features and qualities of privacy and surveillance on newer Internet platforms such as Facebook and Google? Giving answers to such questions requires profound knowledge and application of social theory to the study of online privacy and surveillance. Based on social theory, empirical social research is needed for studying the implications of privacy and surveillance in the online world. The next section gives an overview of some empirical results.

EMPIRICAL STUDIES OF THREE REALMS OF ONLINE PRIVACY AND SURVEILLANCE: THE ECONOMY, POLITICS AND CULTURE

This section presents results from studies of privacy and surveillance in three realms of the online world: the online economy, online politics and everyday culture online.

A First Realm that Concerns Online Privacy and Surveillance is the Economy

Fuchs (2013b) argues that social media constitute spaces where job applicant surveillance, workplace and workforce surveillance, property surveillance, consumer surveillance and surveillance of competitors converge. Dallas Smythe (1977) argued that in commercial media that are funded by advertising (broadcasting, newspapers), the audience is sold as a commodity to advertisers, who pay for access to audiences. He spoke therefore of audience commodification. Fuchs (2013b, 2011) argues that in social media, the audience has turned into 'prosumers', the social media business model is based on Internet prosumer commodification, and that prosumer surveillance that monitors all user data generated on certain platforms like Facebook (and beyond) is built into this business model. As a consequence, advertising becomes targeted and personalized to user activities and interests.

In an analysis based on Smythe (1977), Sut Jhally and Bill Livant (1986) argued that watching is working and that the living room has become a factory for the production of economic value. Andrejevic (2002) argues that in commercial interactive media, surveillance becomes part of the work of watching that as a consequence turns into the work of being watched. He stresses that users of commercial social media create economic value and that their activity is exploited for economic purposes. Users' conscious communication and creation of content creates unintentional information – data about user behaviour captured by the (commercial) platform in surveillance processes (Andrejevic, 2012: 85) – that they do not control and that is turned into profit via targeted advertising. As a result, they are alienated from their activities and products. The users become separated from the 'means of socialization' (Andrejevic, 2012: 88) that are controlled by commercial companies such as Facebook.

Both Fuchs and Andrejevic stress that usage of commercial social media platforms is a form of value-generating labour. Trebor Scholz (2010) therefore argues that Facebook and the commercial Internet are playgrounds and factories, on which users' play becomes digital labour (play labour = 'playbour'). Production and consumption, labour and play, the public and the private, tend to converge on social media. Consumer surveillance on social media tends at the same time to be producer surveillance.

Social media surveillance also relates to traditional wage labour, especially the hiring process and the monitoring of employees' Internet use. A UK survey conducted by Reppler (N = 300) found that 91 per cent of the surveyed companies use social networking sites to screen prospective employees in the hiring process, and 69 per cent say they have rejected a candidate because what they saw about them on a social networking site (SNS) (http://www.thedrum.co.uk/news/2011/10/24/91-employers-use-social-media-screen-applicants). Forty-nine per cent conduct such screening after they have received applications, 27 per cent after an initial conversation, and 15 per cent after a detailed job interview.

A study conducted by the American Management Association and the ePolicy Institute in 2007 found that more than 28 per cent of the surveyed US companies had fired workers for the misuse of e-mail at work, and almost one-third for the misuse of the Internet; 66 per cent said that they monitor employees' Internet use, and more than 40 per cent that they monitor employees' e-mails.

> The 28% of employers who have fired workers for e-mail misuse did so for the following reasons: violation of any company policy (64%); inappropriate or offensive language (62%); excessive personal use (26%); breach of confidentiality rules (22%); other (12%). The 30% of bosses who have fired workers for Internet misuse cite the following reasons: viewing, downloading, or uploading inappropriate/offensive content (84%); violation of any company policy (48%); excessive personal use (34%); other (9%) . . . Computer monitoring takes many forms, with 45% of employers tracking content, keystrokes, and time spent at the keyboard. Another 43% store and review computer files. In addition, 12%

> monitor the blogosphere to see what is being written about the company, and another 10% monitor social networking sites. Of the 43% of companies that monitor e-mail, 73% use technology tools to automatically monitor e-mail and 40% assign an individual to manually read and review e-mail.[1]

The use of social media as tools of applicant and workforce surveillance is a relatively new area of research and concern (Sánchez Abril et al., 2012; Clark and Roberts, 2010; Davison et al., 2012; Davison et al., 2011). The published works on this topic tend to agree that this issue is legally relatively unregulated and that more social scientific and legal research is needed in this area. Sánchez Abril et al. (2012: 69) argue that 'employer intrusion into an employee's personal life threatens the employee's freedom, dignity, and privacy – and may lead to discriminatory practices'. They conducted a survey of 2500 undergraduate students and found that 71 per cent agreed that the following scenario could result in physical, economic or reputational injury in the offline world (p. 104f):

> You called in sick to work because you really wanted to go to your friend's all day graduation party. The next day you see several pictures of you having a great time at the party. Because the pictures are dated you start to worry about whether you might be caught in your lie about being sick. You contact the developers of the social network and ask that the pictures be taken down because the tagging goes so far, it would take you too long to find all the pictures. There was no response from the network. You are stunned to be called in by your supervisor a week later to be advised that you were being 'written up' for taking advantage of sick leave and put on notice that if it happened again you would be terminated (Sánchez Abril et al., 2012: 104)

Clark and Roberts (2010) argue that notwithstanding all legal debates, employers' monitoring of employees' or applicants' social networking sites profiles is a socially irresponsible practice because such practices allow 'employers to be undetectable voyeurs to very personal information and make employment decisions based on that information' (Clark and Roberts, 2010: 518). Due to the persistence of online information, such monitoring can have negative career effects that persist for years. Also, employers can make inappropriate decisions based on very sensitive information ('she is too conservative or too liberal'; Clark and Roberts, 2010: 51).

Protecting employees and job applicants from decisions based on information derived from social media is important because there is an asymmetrical power relationship between employers or managers and employees or applicants. The existence of this asymmetrical power relationship, in which employers have relative power to decide if employees are hired and fired, requires special protection of workers and applicants.

A Second Realm of Online Privacy and Surveillance has to do with the State, especially the Police

Trottier (2011) observes that the police make use of social media in investigations by accessing publicly available profile information, befriending suspects and obtaining personal information from platforms using warrants. One can add to this the targeted surveillance of suspects with the help of communication surveillance technologies in order to try to prevent terrorism. The result is 'an enhanced police presence in – and scrutiny of – everyday life' (Trottier, 2011). The topic of state, police and secret service surveillance of social media has gained special attention since Edward Snowden revealed in 2011 that the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) have direct surveillance access to the personal data processed by AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype and Yahoo!. It shows the existence of a surveillance–industrial complex, in which online corporations, state agencies and private security companies collaborate in order to establish and maintain a political-economic control system (Fuchs, 2014).

Crime on social media is a topic that is often presented by the news media in a sensationalistic manner and by presenting single examples:

> Sex-trio abused schoolgirl (16) . . . and wanted to make her walk the streets . . .
>
> Sex-trap Internet! For a 16-year-old student a flirt on the network 'Facebook' had obviously terrible consequences. The prosecutor is certain: The girl was raped by three men – and was compelled to walk the streets![2] (*Bild Zeitung*, 9 December 2011)
>
> Paedo groomed Facebook girls . . . A 19-YEAR-OLD man who police said was part of a paedophile gang has admitted having sex with girls as young as 13 . . . The group used Facebook to groom schoolgirls before meeting up with them, plying them with drink and drugs and sexually abusing them. (*Sun Online*, 27 May 2011[3])

The reality is, however, fairly different than such sensationalistic news reports suggest. The European Union (EU) Kids Online II Survey studied the behaviour of children online in the EU27 countries.[4] Eighty-six per cent of surveyed children (9–16 years old) in the EU27 countries say they never sent a photo or video of themselves to somebody they have not met face-to-face, and 85 per cent say they never sent personal information to somebody they have not met face-to-face (p. 43). Twelve per cent say they have been bothered by something online, and 8 per cent of parents say their children have been bothered by something online (p. 46). Eighty-one per cent say that they have never been bullied online or offline (p. 61), while 19 per cent were bullied at least once (p. 61). Six per cent had been bullied online (in the past 12 months), 3 per cent on a social networking site (p. 63), which shows that bullying primarily takes place offline and that online bullying is a relatively rare phenomenon. Two per cent said that they had been asked on the Internet to show photos or videos of themselves nude (within the past 12 months), and 2 per cent had been asked to talk about sexual acts (p. 75). Nine per cent of all survey children said that they met an online contact offline, and 1 per cent reported being bothered by this (p. 92). Seven per cent said that somebody other than themselves used their password to access their account (p. 100). Overall these results show that the crime that children experience online is of a relatively minor extent. Majid Yar (2010) argues that mass media reports of individual incidents of violent online pornography or the raping or killing of children by strangers they first met online often function as 'signal crimes' that result in moral panics and calls for law-and-order policies, Internet policing and surveillance. Statistics show that such panics do not reflect the actual low level of online crime. According to the Special Eurobarometer Study 371 'Internal Security' of 2011,[5] 46 per cent say that the EU is doing enough to fight cybercrime, whereas 36 per cent think it is not doing enough.

A Third Realm of Online Privacy and Surveillance Concerns Everyday Life, Civil Society and the Lifeworld

Based on John B. Thompson's (2005) argument that there is a mediated new visibility, in which those who hold power are made visible to the many, Goldsmith (2010) argues that social media, especially YouTube and Facebook, make police misconduct more visible in the public. So on the one hand the police have powerful surveillance technologies at hand for monitoring citizens, but on the other hand citizens also use less sophisticated technologies with less reach (mobile phone cameras, video live streams, and so on) in aiming to make police power and violence transparent. There is an asymmetry involved in this usage because the police have more resources, capacities, access possibilities and time for conducting surveillance. Goldsmith discusses the example of YouTube videos of the death of Ian Tomlinson in the London G9 protests in 2009, and of the death of Robert Dziekanski at Vancouver Airport in 2009. In both cases, police violence was involved. Other examples that can be mentioned are the YouTube video of the killing of Neda Soltan by police forces in the 2009 Iranian protests, and two 2011YouTube videos that show how police officers pepper-sprayed unarmed protestors of the Occupy movement (one filmed in New York, the other at the University of California Davis campus). On the one hand one can argue that these are acts of counter-power and counter-surveillance. On the other hand, visibility on the

Internet is not equally distributed; there is 'an Internet attention economy that is dominated by powerful actors' (Fuchs et al., 2012b: 15).

Acquisti and Gross conducted an online survey of SNS users at Carnegie Mellon University in the USA (N = 294; Acquisti and Gross, 2006) and data mining of 7000 social networking site profiles (Gross et al., 2005). They found that although users are highly concerned about privacy, the amount of personal information they include in their SNS profiles is high: for example, 78 per cent revealed their full name and 99.94 per cent of the profiles were publicly accessible. Barnes (2006) called this phenomenon the 'privacy paradox'. Nosko et al. (2010) analysed 400 Facebook profiles. They conclude that there is a high level of information revelation: mini-feed, profile pictures, birth date, friends, college or university, wall postings, gender, used applications, groups, photos, tagged photos and photo albums were disclosed to the public by 70 per cent or more of the studied profiles.

These results to a certain extent imply that social media users deal carelessly with private data and put themselves at risk. They are however to a certain degree questioned by studies that found that Facebook users feel highly confident in managing Facebook privacy settings. According to Boyd and Hargittai (2010), 51 per cent of the respondents in a study of 18–19-year-old SNS users had changed their privacy settings four or more times, 38 per cent two or three times, 9 per cent once, and only 2 per cent never (N2 = 495, survey conducted in 2010). The Special Eurobarometer Study 359 'Attitudes on Data Protection and Electronic Identity in the European Union' (2011)[6] shows that 51 per cent of European social networking site users have changed the privacy settings of Facebook and other sites (p. 164). Eighty-two per cent find it easy to change privacy settings; 18 per cent find it difficult (p. 166). These data show that most users seem to be aware of how to change the privacy settings. Fuchs (2009) and Beer (2008) argue that many of these studies are too focused on individual users' behaviour and neglect macro contexts such as advertising culture, political economy, surveillance or the 'War on Terror'. They stress that revealing information on social media is a means of communication and is not a problem in itself. Rather, the problem is power structures (for example, companies that spy on their employees or applicants) that make use of such data for negatively impacting upon individuals.

Albrechtslund argues that people's practice of watching each other on social networking sites is 'participatory surveillance': it '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 . . . participatory surveillance is a way of maintaining friendships by checking up on information other people share' (Albrechtslund, 2008). Andrejevic (2005) speaks of lateral surveillance as 'do-it-yourself monitoring' (p. 487) or 'peer-to-peer monitoring', 'the use of surveillance tools by individuals, rather than by agents of institutions public or private, to keep track of one another', for example in relation to romances, family, friends and acquaintances (p. 488). In contrast to Albrechtslund, Andrejevic does not think that lateral surveillance democratizes surveillance, but argues that it reinforces and replicates 'the imperatives of security and productivity' (Andrejevic, 2005: 487) and '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' (p. 494). Thomas Mathiesen argues that everyday life monitoring today also takes on the form of a synopticon, which is 'an extensive system enabling the many to see and contemplate the few', whereas in the panopticon the few 'see and supervise the many' (Mathiesen, 1997: 219). There is a difference between seeing and supervising: in Mathiesen's concept the many do not have the power to supervise the few, but the few have the power to supervise the many.

CONCLUSION

Many questions regarding online privacy and surveillance are largely unanswered and require theory construction, empirical research and ethical reasoning:

- What are the key features and qualities of online privacy and surveillance?
- What are social media and how do privacy and surveillance shape social media?
- How do contemporary societal contexts, such as the new imperialism, capitalism, neoliberalism, global wars and conflicts, the political economy of the surveillance–industrial complex, and so on, shape online privacy and surveillance?
- What is the role of privacy and surveillance in the context of the online economy? That is, what are key features and empirical realities of phenomena such as digital labour, targeted advertising, online marketing, online business models and value creation, class relations and exploitation online, consumer surveillance online, workforce and workplace surveillance online, and so on.

- What are the implications and empirical realities of the online realm for state surveillance, crime, policing and political activism?
- What are the features and empirical realities of online privacy and surveillance in everyday life and relationships?
- How can online surveillance be resisted and what power asymmetries do counter-surveillance projects that make use of the Internet face (for example WikiLeaks, corporate watchdog projects)? Are there ways of overcoming these asymmetries?
- What are philosophical foundations and principles of computer ethics and how do they relate to the study of online privacy and surveillance?
- What is the difference between privacy impact assessments and societal and ethical impact assessments of information and communication technologies (ICTs)? How can societal and ethical impact assessments be best integrated into research and research projects (for example by requiring all research projects that develop or study ICTs and are funded by national research councils, the European Union, and so on to include a work package about societal and ethical impact assessment)?

Scholars studying online privacy and surveillance often situate themselves and their work in either 'Internet studies' (Consalvo and Ess, 2011; Hunsinger et al., 2010) or 'surveillance studies' (Ball et al., 2012), which reflects two sides of the conceptual integration of the concepts of 'online' and of 'privacy' and 'surveillance'. Both of these new fields claim that they are not disciplines, but interdisciplinary or transdisciplinary fields. Nonetheless each displays the habitus, identity and discipline-making behaviour of a discipline. There are a lot of new interdisciplines and transdisciplines today that claim to be new and unique. In making claims that their fields of studies are unique they, however, separate themselves from other academic communities, fields, scholars and institutions and contribute to academic fragmentation. They also imitate the behaviour of established disciplines, so that 'interdisciplines' and 'transdisciplines' may one day simply become the new disciplines.

I am neither arguing for or arguing against established disciplines or new interdisciplines, but instead think that such categorizations are rather meaningless, and pure expressions of academic power struggles. I therefore contend that the study of online privacy and surveillance should neither be situated in the realm of 'Internet studies' nor in the realm of 'surveillance studies'. I rather think that it is today necessary to invoke another distinction in the social sciences and humanities: namely the one between administrative and critical research. Administrative social research describes reality merely as it is by employing empirical social research that follows basic inductive or deductive schemes, and is instrumental in the legitimatization of powerful institutions. In contrast, Horkheimer (2002) stresses that the goal of a critical theory of society is the transformation of society as a whole (p. 219) so that a ‘society without injustice’ (p. 221) emerges that is shaped by ‘reasonableness, and striving for peace, freedom, and happiness’ (p. 222). Horkheimer argues that critical theory wants to enhance the realization of all human potentialities (p. 248); it ‘never simply aims at an increase of knowledge as such’. Its goal is man’s ‘emancipation from slavery’ (p. 249) and ‘the happiness of all individuals’ (p. 248).

Online privacy and surveillance happen in societal contexts that are shaped by fundamental socio-economic inequalities, global crises, global wars and conflicts. Therefore it matters not just that we study the Internet, digital politics, online privacy and surveillance, but that we do so in a non-administrative and critical way.

ACKNOWLEDGEMENT

This chapter is an outcome of the EU FP7 project PACT – Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action, grant agreement number 285635, http://www.projectpact.eu/.

NOTES

[1] http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey.

[2] Source: http://www.bild.de/regional/hamburg/vergewaltigung/sex-trio-missbrauchte-schuelerin-21460618.bild.html. Translation from German: ‘Sex-Trio missbrauchte Schülerin (16) . . . und wollte sie auf den Strich schicken . . . Sex-Falle Internet! Für eine 16-jährige Schülerin hatte ein Flirt im Netzwerk “Facebook” offenbar schreckliche Folgen. Der Staatsanwalt ist sicher: Das Mädchen wurde von drei Männern vergewaltigt – und sollte auf dem Straßenstrich landen!’.

[3] http://www.thesun.co.uk/sol/homepage/news/3605422/Man-in-paedophile-gang-admits-grooming-girls-on-Facebook.html.

[4] ‘European Union Kids Online: enhancing knowledge regarding European children’s use, risk and safety online, 2010’, http://www.esds.ac.uk/doc/6885%5Cmrdoc%5Cpdf%5C6885_reports.pdf.

[5] http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf.

[6] http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

FURTHER READING

Allmer, Thomas (2012), *Towards a Critical Theory of Surveillance in Informational Capitalism*, Frankfurt am Main: Peter Lang.

Andrejevic, Mark (2007), *iSpy: Surveillance and Power in the Interactive Era*, Lawrence, KS: University Press of Kansas.

Fuchs, Christian (2008), *Internet and Society. Social Theory in the Information Age*, New York: Routledge.

Fuchs, Christian (2011a), 'New media, web 2.0 and surveillance', *Sociology Compass*, 5 (2), 134–147.

Fuchs, Christian (2011b), 'Teaching and learning guide for new media, web 2.0 and surveillance', *Sociology Compass*, 5 (6), 480–487.

Fuchs, Christian (2013a), *Social Media. A Critical Introduction*, London: Sage.

Fuchs, Christian (2014), 'Social media and the public sphere', *tripleC: Communication, Capitalism and Critique*, 12 (1), 57–101.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds) (2012a), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, New York: Routledge.

Gandy, Oscar H. (1993), *The Panoptic Sort. A Political Economy of Personal Information*, Boulder, CO: Westview Press.

Gandy, Oscar H. (2009), *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*, Farnham: Ashgate.

Kelly, Kevin (1999), *New Rules for the New Economy*, New York: Penguin.

Negroponte, Nicholas (1996), *Being Digital*, New York: Vintage Books.

Trottier, Daniel (2012), *Social Media as Surveillance*, Farnham: Ashgate.

REFERENCES

Acquisti, Alessandro and Ralph Gross (2006), 'Imagined communities: awareness, information sharing, and privacy on the Facebook', in Phillipe Golle and George Danezis (eds), *Proceedings of 6th Workshop on Privacy Enhancing Technologies*, Cambridge: Robinson College, pp. 36–58.

Albrechtslund, A. (2008), 'Online social networking as participatory surveillance', *First Monday*, 13 (3). http:l/firstmonday.orglarticlelviewl2142/1949.

Andrejevic, Mark (2002), 'The work of being watched: interactive media and the exploitation of self-disclosure', *Critical Studies in Media Communication*, 19 (2), 230–248.

Andrejevic, Mark (2004), *Reality TV: The Work of Being Watched*, Lanham, MD: Rowman & Littlefield.

Andrejevic, M. (2005), 'The work of watching one another: lateral surveillance, risk, and governance', *Surveillance and Society*, 2 (4), 479–497.

Andrejevic, M. (2007), *iSpy: Surveillance and Power in the Interactive Era*, Lawrence, KS: University Press of Kansas.

Andrejevic, Mark (2012), 'Exploitation in the data mine', in Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, New York: Routledge, pp. 71–88.

Ball, Kirstie, Kevin Haggerty and David Lyon (eds) (2012), *Routledge Handbook of Surveillance Studies*, New York: Routledge

Barnes, S. (2006), 'A privacy paradox: social networking in the United States', *First Monday*, 11 (9). http://www.firstmonday.org/issues/issue11_9/barnes/index.html.

Beer, D. (2008), 'Social network(ing) sites revisiting the story so far: a response to Danah Boyd and Nicole Ellison', *Journal of Computer-Mediated Communication*, 13 (2), 516–529.

Bennett, C. (2011a), 'In defence of privacy: the concept and the regime', *Surveillance and Society*, 8 (4), 485–496.

Bennett, C. (2011b), 'In further defence of privacy', *Surveillance and Society*, 8 (4), 513–516.

Boyd, D. (2011), Social Network Sites as Networked Publics: affordances, dynamics and implications. In *A Networked Self: identity, community and culture on social network sites*, edited by Zizi Papacharissi, 39–58. London: Routledge.

Boyd, D. and Hargittai, E. (2010), 'Facebook privacy settings: Who cares?', *First Monday*, 15 (8).

Clark, Leigh A. and Sherry J. Roberts (2010), 'Employer's use of social networking sites: a socially irresponsible practice', *Journal of Business Ethics*, 95 (4), 507–525.

Clarke, R. (1988), Information technology and dataveillance, *Communications of the ACM*, 31 (5), 498–512.

Clarke, Roger (1994), 'Dataveillance: delivering "1984"', in Lelia Green and Roger Guinery (eds), *Framing Technology: Society, Choice and Change*, Sydney: Allen & Unwin, pp. 117–130.

Consalvo, Mia and Charles Ess (eds) (2011), *The Handbook of Internet Studies*, Chicester: Wiley-Blackwell.

Davison, Kristl H., Catherine Maraist and Mark N. Bing (2011), 'Fiend or foe? The promise and pitfalls of using social networking sites for HR decisions', *Journal of Business and Psychology*, 26 (2), 153–159.

Davison, Kristl H., Catherine Maraist, R.H. Hamilton and Mark N. Bing (2012), 'To screen or not to screen? Using the Internet for selection decisions', *Employee Responsibilities and Rights Journal*, 24 (1), 1–21.

Foucault, Michel (1977), *Discipline and Punish*, New York: Vintage.

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: Forschungsgruppe UTI.

Fuchs, Christian (2010), 'Social software and Web 2.0: their sociological foundations and implications', in San Murugesan (ed.), *Handbook of Research on Web 2.0, 3.0, and X.0: Technologies, Business, and Social Applications. Volume II*, Hershey, PA: IGI-Global, pp. 764–789.

Fuchs, C. (2011c), 'How to define surveillance?', *MATRIZes*, 5 (1), 109–133.

Fuchs, Christian (2013b), 'Political economy and surveillance theory', *Critical Sociology* 39 (5), 671–687.

Fuchs, Christian (2014), 'Social media and the public sphere', *tripleC: Communication, Capitalism and Critique*, 12 (1), 57–101.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (2012b), 'Introduction: Internet and surveillance', in Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, New York: Routledge, pp. 1–28.

Fuchs, Christian and Daniel Trottier (2013), 'The Internet as surveilled workplayplace and factory', in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *European Data Protection. Coming of Age*, Dordrecht: Springer, pp. 33–57.

Gilliom, John (2001), *Overseers of the Poor*, Chicago, IL: University of Chicago Press.

Goldsmith, Andrew John (2010), 'Policing's new visibility', *British Journal of Criminology*, 50 (5), 914–934.

Graham, Stephen and David Wood (2007), 'Digitizing surveillance: categorization, space, inequality', in Sean P. Her and Josh Greenberg (eds), *The Surveillance Studies Reader*, Maidenhead: Open University Press, pp. 218–230.

Gross, Ralph, Alessandro Acquisti and H. John Heinz III (2005), 'Information revelation and privacy in online social networks', in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, New York: ACM Press, pp. 71–80.

Habermas, Jürgen (1987), *The Theory of Communicative Action. Volume 2: Lifeworld and System: A Critique of Functionalist Reason*, Boston, MA: Beacon Press.

Horkheimer, Max (2002), 'Traditional and critical theory', *Critical Theory*, New York: Continuum, pp. 188–252.

Hunsinger, Jeremy, Klastrup, Listrup and Matthew Allen (eds) (2010), *International Handbook of Internet Research*, Dordrecht: Springer.

Jhally, S. and B. Livant (1986), 'Watching as working: the valorization of audience consciousness', *Journal of communication*, 36 (3), 124–143.

Kelly, Kevin (1999), *New Rules for the New Economy*, New York: Penguin.

Lyon, David (1994), *The Electronic Eye: The Rise of Surveillance Society*, Cambridge: Polity.

Lyon, D. (1998), 'The world wide web of surveillance: the Internet and off-world powerflows', *Information, Communication and Society*, 1 (1), 91–105.

Marx, Gary T. (1988), *Undercover: Police Surveillance in America*, Berkeley, CA: University of California Press.

Marx, Gary T. (2002), 'What's new about the "new surveillance"? Classifying for change and continuity', *Surveillance and Society*, 1 (1), 9–29.

Mathiesen, Thomas (1997), 'The viewer society: Michel Foucault's "panopticon" revisited', *Theoretical Criminology*, 1 (2), 215–234.

Negroponte, Nicholas. (1996), *Being Digital*, New York: Vintage Books.

Nosko, A., E. Wood and S. Molema (2010), 'All about me. Disclosure in online social networking profiles. The case of Facebook', *Computers in Human Behavior*, 26 (3), 406–418.

O'Reilly, T. and N. Battelle, (2009), 'Web squared. Web 2.0 five years on. Special report', available at http://assets.en.oreilly.com/1/event/28/web2009_websquared-whitepaper.pdf (accessed 30 January 2013).

Poster, Mark (1990), *The Mode of Information*, Cambridge: Polity.

Regan, Priscilla (1995), *Legislating Privacy*, Chapel Hill, NC: University of North Carolina Press.

Rheingold, Howard (1993), *The Virtual Community. Homesteading on the Electronic Frontier*, Cambridge, MA: MIT Press.

Sánchez Abril, Patricia, Avner Levin and Alissa Del Riego (2012), 'Blurred boundaries: social media privacy and the twenty-first-century employee', *American Business Law Journal*, 49 (1), 63–124.

Scholz, Trebor (2010), 'Facebook as playground and factory', in Dylan E. Wittkower (ed.), *Facebook and Philosophy: What's on Your Mind?*, Chicago, IL: Open Court, pp. 241–252.

Smythe, Dallas W. (1977), 'Communications: blindspot of Western Marxism', *Canadian Journal of Political and Social Theory*, 1 (3), 1–27.

Stalder, F. (2011), 'Autonomy beyond privacy? A rejoinder to Colin Bennett', *Surveillance and Society*, 8 (4), 508–512.

Tavani, Herman T. (2008), 'Informational privacy: concepts, theories, and controversies', in Kenneth E. Himma and Herman T. Tavani (eds), *The Handbook of Information and Computer Ethics*, Hoboken, NJ: Wiley, pp. 131–164.

Thompson, John B. (2005), 'The new visibility', *Theory, Culture and Society*, 22 (6), 31–51.

Trottier, Daniel (2011), 'A research agenda for social media surveillance', *Fast Capitalism*, 8 (1).

Trottier, Daniel (2012), *Social Media as Surveillance*, Farnham: Ashgate.

Trottier, Daniel and David Lyon (2012), 'Key features of social media surveillance', in Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, New York: Routledge, pp. 89–105.

Warren, S. and L. Brandeis (1890), 'The right to privacy', *Harvard Law Review*, 4 (5), 193–220.

Yar, Majid (2010), 'Public perceptions and public opinion about Internet crime', in Yvonne Jewkes and Majid Yar (eds), *Handbook of Internet Crime*, Cullompton: Willan, pp. 104–119.