ROUTLEDGE STUDIES IN SCIENCE, TECHNOLOGY AND SOCIETY

Wind Power and Power Politics
International Perspectives
Edited by Peter A. Strachan, David Lal and David Toke

Global Public Health Vigilance
Creating a World on Alert
Lorna Weir and Eric Mykhalovskiy

Rethinking Disability
Bodies, Senses, and Things
Michael Schillmeier

Biometrics
Bodies, Technologies, Biopolitics
Joseph Pugliese

Wired and Mobilizing
Social Movements, New Technology, and Electoral Politics
Victoria Carty

The Politics of Bioethics
Alan Petersen

The Culture of Science
How the Public Relates to Science Across the Globe
Edited by Martin W. Bauer, Rajesh Shukla and Nick Allum

Internet and Surveillance
The Challenges of Web 2.0 and Social Media
Edited by Christian Fuchs, Kees Boersma,
Anders Albrechtslund and Marisol Sandoval

an **informa** business

Routledge
Taylor & Francis Group
www.routledge.com

ISBN 978-0-415-89160-8
9 780415 891608 80000

Internet and Surveillance
Edited by Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval

ROUTLEDGE

ROUTLEDGE STUDIES IN SCIENCE, TECHNOLOGY AND SOCIETY

Internet and Surveillance

The Challenges of Web 2.0 and Social Media

Edited by Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval

cost

ROUTLEDGE

Internet and Surveillance

The Challenges of Web 2.0 and Social Media

Edited by Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval

Routledge
Taylor & Francis Group
NEW YORK LONDON

First published 2011
by Routledge
270 Madison Ave, New York, NY 10016

Simultaneously published in the UK
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

Routledge is an imprint of the Taylor & Francis Group,
an informa business

Typeset in Sabon by IBT Global.
Printed and bound in the United States of America on acid-free paper by IBT Global.

Library of Congress Cataloging-in-Publication Data
A catalog record has been requested for this book.

ISBN: 978-0-415-89160-8 (hbk)
ISBN: 978-0-203-80643-2 (ebk)

About COST

COST—the acronym for European Cooperation in Science and Technology—is the oldest and widest European intergovernmental network for cooperation in research. Established by the Ministerial Conference in November 1971, COST is presently used by the scientific communities of 36 European countries to cooperate in common research projects supported by national funds.

The funds provided by COST—less than 1% of the total value of the projects—support the COST cooperation networks (COST Actions) through which, with EUR 30 million per year, more than 30 000 European scientists are involved in research having a total value which exceeds EUR 2 billion per year. This is the financial worth of the European added value which COST achieves.

A "bottom up approach" (the initiative of launching a COST Action comes from the European scientists themselves), "à la carte participation" (only countries interested in the Action participate), "equality of access" (participation is open also to the scientific communities of countries not belonging to the European Union) and "flexible structure" (easy implementation and light management of the research initiatives) are the main characteristics of COST.

As precursor of advanced multidisciplinary research COST has a very important role for the realisation of the European Research Area (ERA) anticipating and complementing the activities of the Framework Programmes, constituting a "bridge" towards the scientific communities of emerging countries, increasing the mobility of researchers across Europe and fostering the establishment of "Networks of Excellence" in many key scientific domains such as: Biomedicine and Molecular Biosciences; Food and Agriculture; Forests, their Products and Services; Materials, Physical and Nanosciences; Chemistry and Molecular Sciences and Technologies; Earth System Science and Environmental Management; Information and Communication Technologies; Transport and Urban Development; Individuals, Societies, Cultures and Health. It covers basic and more applied research and also addresses issues of pre-normative nature or of societal importance.

Web: http://www.cost.eu

Contents

PART III:
Conclusion

1 Introduction

Internet and Surveillance

Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval

1.1. COMPUTING AND SURVEILLANCE

Scholars in surveillance studies and information society studies have stressed the importance of computing for conducting surveillance for more than 20 years. This has resulted in a number of categories that describe the interconnection of computing and surveillance: for the new surveillance, dataveillance, the electronic (super)panopticon, electronic surveillance, or digital surveillance.

Gary T. Marx defines the new surveillance as "the use of technical means to extract or create personal data. This may be taken from individuals or contexts" (Marx 2002, 12; see also: Marx 1988, 217–219). He argues that in the old surveillance, it was more difficult to send data, whereas in the new surveillance this is easier. In traditional surveillance, "what the surveillant knows, the subject probably knows as well", whereas in the new surveillance the "surveillant knows things the subject doesn't" (Marx 2002, 29). He says that the new surveillance is not on scene, but remote, and that it is "less coercive" (28) and "more democratized" because some forms are more widely available (28). Computerized surveillance is an important form of new surveillance. "Computers qualitatively alter the nature of surveillance—routinizing, broadening, and deepening it. Organizational memories are extended over time and across space" (Marx 1988, 208).

Dataveillance is the "systematic monitoring of people's actions or communications through the application of information technology" (Clarke 1988, 500). 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. Bogard (2006) argues that the computer is a technology that simulates surveillance.

Gordon (1987) speaks of the electronic panopticon. Mark Poster (1990) has coined the notion of the electronic superpanopticon: "Today's 'circuits of communication' and the databases they generate constitute a Superpanopticon, a system of surveillance without walls, windows, towers or guards" (Poster 1990, 93). Mark Andrejevic has coined the notion of the digital enclosure (Andrejevic 2004, 2007), in which interactive technologies

generate "feedback about the transactions themselves", and he said that this feedback "becomes the property of private companies" (Andrejevic 2007, 3). Andrejevic (2007, 2) sees the Internet as a virtual digital enclosure. Commercial and state surveillance of consumers would be the result of the digital enclosure. They "foster asymmetrical and undemocratic power relations. Political and economic elites collect information that facilitates social Taylorism rather than fostering more democratic forms of shared control and participation" (Andrejevic 2007, 257). Nicole Cohen argues, based on Mark Andrejevic and Tiziana Terranova, that Facebook profits by the "valorization of surveillance" (Cohen 2008, 8). Parenti (2003, 78) stresses that by digital technology "surveillance becomes more ubiquitous, automatic, anonymous, decentralized, and self-reinforcing".

David Lyon has stressed the role of computers for contemporary surveillance and has used the notion of electronic surveillance: "Contemporary surveillance must be understood in the light of changed circumstances, especially the growing centrality of consumption and the adoption of information technologies" (Lyon 1994, 225). "Although computers are not necessarily used for all kinds of surveillance—some is still face to face and some, like most CCTV systems, still require human operators—most surveillance apparatuses in the wealthier, technological societies depend upon computers" (Lyon 2003, 22). "Electronic surveillance has to do with the ways that computer databases are used to store and process personal information on different kinds of populations" (Lyon 1994, 8). David Lyon (1998; 2001, 101) speaks of the worldwide web of surveillance in order to stress that "all uses of the Internet, the world wide web and email systems are traceable and this capacity is rapidly being exploited as these media are commercialized". He distinguishes three main forms of surveillance in cyberspace that are related to employment, security and policing, and marketing (Lyon 1998, 95). Lyon (1994, 51f) argues that digitalization and networking have changed surveillance: File size has grown, individuals can be more easily traced because databases are dispersed and easily accessed by central institutions, the speed of data flow has increased, and citizens are subjected to increasingly constant and profound monitoring.

Manuel Castells (2001, 172) defines Internet surveillance technologies as technologies that

> intercept messages, place markers that allow tracking of communication flows from a specific computer location, and monitor machine activity around the clock. Surveillance technologies may identify a given server at the origin of a message. Then, by persuasion or coercion, governments, companies, or courts may obtain from the Internet service provider the identity of the potential culprit by using identification technologies, or simply by looking up their listings when the information is available.

Castells considers Internet surveillance as a technology of control (Castells 2001, 171).

Graham and Wood (2003/2007) argue that monitoring across widening geographical distances and the active sorting of subject populations on a continuous, real-time basis are two central characteristics of digital surveillance. They say that under the given economic conditions, "digital surveillance is likely to be geared overwhelmingly towards supporting the processes of indvidualization, commodification, and consumerization" (Graham and Wood 2003/2007, 219).

Many of the discussions about the role of the Internet in surveillance started before the Internet became a popular mass medium in the mid-1990s. Large-scale Internet usage did not take off before 1995, when the Mosaic browser was made available to the public. The World Wide Web (WWW) was created in 1990 by Tim Berners-Lee and was released for the public in 1993. In December 1990, there was one website on the WWW, in September 1993 there were 204 sites, in June 1996, 252,000, in December 2000, 25,675,581, in November 2006, 101,435,253 (data source: Internet time line by Robert Zakon, http://www.zakon.org/robert/internet/timeline/#Growth).

The Internet enables a globally networked form of surveillance. Internet surveillance adds at least two dimensions to computer surveillance: global interaction and networking. The contributors to this book show that it is an important task to discuss how notions such as the new surveillance, dataveillance, the electronic panopticon, and electronic surveillance can be applied to the Internet and what commonalities and differences there are between computer surveillance and Internet surveillance.

1.2. WEB 2.0 AND SURVEILLANCE

Many observers claim that the Internet has been transformed in the past years from a system that is primarily oriented to information provision into a system that is more oriented to communication and community building. The notions of "web 2.0", "social media", "social software", and "social network(ing) sites" have emerged in this context. Web platforms such as Wikipedia, MySpace, Facebook, YouTube, Google, Blogger, Rapidshare, Wordpress, Hi5, Flickr, Photobucket, Orkut, Skyrock, Twitter, YouPorn, PornHub, Youku, Orkut, Redtube, Friendster, Adultfriendfinder, Megavideo, Tagged, Tube8, Mediafire, Megaupload, Mixi, Livejournal, LinkedIn, Netlog, ThePirateBay, Orkut, XVideos, Metacafe, Digg, StudiVZ, etc. are said to be typical for this transformation of the Internet. *Web 2.0/Social media platforms are web-based platforms that predominantly support online social networking, online community-building, and maintenance, collaborative information production and sharing, and user-generated content production, diffusion, and consumption.* No matter if we agree that important transformations of the Internet have taken place or not, it is clear that a principle that underlies such platforms is the massive provision and storage of personal data that are systematically evaluated, marketed, and used for targeting users with advertising. Therefore surveillance is an important topic in the context of web 2.0 studies.

> Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an 'architecture of participation', and going beyond the page metaphor of Web 1.0 to deliver rich user experiences. (O'Reilly 2005, online)

Some claim that the Internet has in recent years become more based on sharing, communication, and cooperation. Tapscott and Williams say that web 2.0 brings about "a new economic democracy [. . .] in which we all have a lead role" (Tapscott and Williams 2007). Manuel Castells characterizes social media and web 2.0 as media that enable mass-self communication: "people build their own networks of mass self-communication, thus empowering themselves" (Castells 2009, 421). For Clay Shirky, the central aspect of web 2.0 is "a remarkable increase in our ability to share, to cooperate with one another, and to take collective action" (Shirky 2008, 20f). Axel Bruns sees the rise of produsage—the "hybrid user/producer role which inextricably interweaves both forms of participation" (Bruns 2008, 21)—as the central characteristic of web 2.0. Henry Jenkins (2008) sees a participatory culture at work on web 2.0. Mark Deuze speaks in relation to web 2.0 of the "interactive, globally networked and increasingly participatory nature of new media" (Deuze 2007, 40). Shiffman (2008) sees the emergence of the "age of engage" as result of web 2.0. Yochai Benkler (2006) argues that the Internet advances the emergence of commons-based peer production systems (such as open source software or Wikipedia) that are "radically decentralized, collaborative, and nonproprietary; based on sharing resources and outputs among widely distributed, loosely connected individuals who cooperate with each other without relying on either market signals or managerial commands" (Benkler 2006, 60). Others have stressed for example that online advertising is a mechanism by which corporations exploit web 2.0 users who form an Internet prosumer/produser commodity and are part of a surplus-value generating class that produces the commons of society that are exploited by capital (Fuchs 2011; Fuchs 2010a, b; Fuchs 2009a, b, c; Fuchs 2008a, 195–209, Fuchs 2008b; Andrejevic 2002, 2004, 2007, 2009); that web 2.0 is based on the exploitation of free labour (Terranova 2004); that most web 2.0 users are part of a creative precarious underclass that needs economic models that assist them in making a living from their work (Lovink 2008); that blogging is mainly a self-centred, nihilistic, cynical activity (Lovink 2008); that the web 2.0 economy is still dominated by corporate media chains (Stanyer 2009); that web 2.0 is contradictory and therefore also serves dominative interests (Cammaerts 2008); that web 2.0 optimism is uncritical and an ideology that serves corporate interests (Fuchs 2008b, Scholz 2008, van Dijck and Nieborg 2009); that web 2.0 users are more passive users than active

creators (van Dijck 2009); that web 2.0 discourse advances a minimalist notion of participation (Carpentier and de Cleen 2008); or that corporations appropriate blogs and web 2.0 in the form of corporate blogs, advertising blogs, spam blogs, and fake blogs (Deuze 2008).

This short selective overview shows that web 2.0 is a contradictory phenomenon that, just like all techno-social systems, does not have a one-dimensional effect, but complex interconnected effects (Fuchs 2008a). The contributors to this book show the central importance of web 2.0 in the discussion and analysis of Internet surveillance. The working of web 2.0 is based on the collection, storage, usage, and analysis of a huge amount of personal data. Therefore discussing privacy- and surveillance-implications of web 2.0 and the political, economic, and cultural dimensions of privacy and surveillance on web 2.0 becomes an important task. The contributions in this book contribute to the clarification of the surveillance and privacy implications of web 2.0.

The term "web 2.0" can create the false impression that we are experiencing an entirely new Internet. But this is neither the case for the Internet's technological dimension nor for its organizational and institutional contexts. E-mail and information search are still the most popular online activities. In 2010, 61% of all people in the EU27 countries aged 15–74 used e-mail at least once during a three-month period, and 56% used the Internet to search for information about goods and services (data source: Eurostat). The change that has taken place in the past couple of years is that today World Wide Web platforms like Facebook (#2 in the list of most accessed websites, data source: alexa.com, top sites, accessed on January 2, 2011), YouTube (#3), Blogger (#7), Wikipedia (#8), and Twitter (#10) are among the ten most accessed and popular websites in the world. Sharing audiovisual content in public (user-generated content production and diffusion), writing online diaries (blogging), co-creating knowledge with others (wikis), staying in constant contact with friends and acquaintances (social networking sites), sending and sharing short messages online (microblogging, as on Twitter) are relatively new activities that in the 1990s were not supported by the World Wide Web. But there are also many Internet activities, applications, and platforms (like search engines, e-mail, online banking, online shopping, online newspapers, etc.) that have been around longer. The terms "web 2.0" and "social media" do not signify a new or radical transformation of the Internet, but the emergence of specific social qualities (sharing, online cooperation, etc.) supported by the World Wide Web that have become more important (Fuchs 2010b).

The Internet is a technology of cognition, communication, and cooperation (Fuchs 2008a, 2010b). All information is a Durkheimian social fact; it is generated in societal contexts and therefore reflects certain qualities of society and its production contexts. In this sense, we can say that the Internet is and has always been social because it is a vast collection of information and therefore of social facts (Fuchs 2010b). A second mode of sociality is the establishment and reproduction of social relationships (Fuchs 2010b).

Certain Internet applications and platforms support communication and thereby are social in a communicative sense. Cooperation is a third mode of sociality that is reflected in Ferdinand Tönnies' concept of community and Karl Marx's notion of cooperative labour (Fuchs 2010b). The terms web 2.0 and social media are in everyday life frequently employed for meaning that this third mode of sociality (cooperation) has to a certain degree become more supported by the World Wide Web (Fuchs 2010b). One should however bear in mind that this is a specific understanding and mode of sociality and that there are other ones as well (Fuchs 2010b).

One should neither be optimistic nor pessimistic about the transformation of power structures on the Internet. The Internet still is a tool that is used by powerful groups for trying to support their control and domination of other groups just like it is a tool that has potentials for being used in resistances against domination (Fuchs 2011). The difference today is that technologies and platforms like social networking sites, video sharing platforms, blogs, microblogs, wikis, user-generated content upload and sharing sites (like WikiLeaks), etc. have come to play a certain role in the exertion of and resistance against domination. The study of online surveillance and web 2.0 surveillance is situated in the context of the continuities and changes of the Internet, conflicts and contradictions, power structures and society.

1.3. THE ROLE OF THEORIES, FOUCAULT, AND THE PANOPTICON FOR ANALYZING INTERNET

Surveillance

Lyon (2006b, 10) argues that modern surveillance theories relate to nation-state, bureaucracy, techno-logic, political economy, whereas postmodern surveillance theories focus on digital technologies and their implications. The contributors to this book show that both modern and postmodern theories are important for discussing Internet surveillance and web 2.0 surveillance.

The notion of the panopticon was conceived by Jeremy Bentham as prison architecture in the nineteenth century and connected to academic discussions about the notions of surveillance and disciplinary power by Michel Foucault (1977, 1994). The concept of the panopticon has strongly influenced discussions about computer and Internet surveillance. On the one hand there are authors who find the metaphor suitable. Robins and Webster (1999) argue, for example, that in what they term cybernetic society "the computer has achieved [. . .] the extension and intensification of panoptic control; it has rendered social control more pervasive, more invasive, more total, but also more routine, mundane and inescapable" (Robins and Webster 1999, 180, see also 118–122). Webster (2002, 222) argues that computers result in a panopticon without physical walls. Oscar H. Gandy (1993) has introduced the notion of the panoptic sort: "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). David Lyon (2003) speaks based on Gandy's notion of the panoptic sort in relation to computers and the Internet of surveillance as social sorting. "The surveillance system obtains personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access, and so on" (Lyon 2003, 20). Gandy has analyzed data mining as a form of panoptic sorting (Gandy 2003) and has stressed the role of electronic systems in panoptic sorting: "Electronic systems promise the ultimate in narrowcasting or targeting, so it becomes possible to send an individualized message to each individual on the network" (Gandy 1993, 90). Mathiesen (1997) has introduced the notion of the synopticon as user-oriented correlate to the panopticon and has argued that the Internet is a silencing synopticon (Mathiesen 2004). James Boyle (1997) argues that the works of Foucault allow an alternative to the assumption of Internet libertarians that cyberspace cannot be controlled in order to provide "suggestive insights into the ways in which power can be exercised on the Internet" (Boyle 1997, 184). Gordon (1987) speaks of the electronic panopticon; Zuboff (1988) of the information panopticon; Poster (1990) of the electronic superpanopticon; Elmer (2003, 2004) of diagrammatic panoptic surveillance; and Rämö and Edenius (2008) speak of the mobile panopticon.

On the other hand, there are authors who want to demolish the metaphor of the panopticon (for example Haggerty 2006) and do not find it useful for explaining contemporary surveillance and networked forms of surveillance. They argue that surveillance systems such as the Internet are decentralized forms of surveillance, whereas the notion of the panopticon assumes centralized data collection and control. "Certainly, surveillance today is more decentralized, less subject to spatial and temporal constraints (location, time of day, etc.), and less organized than ever before by the dualisms of observer and observed, subject and object, individual and mass. The system of control is deterritorializing" (Bogard 2006, 102). Haggerty and Ericson (2000/2007) have introduced the notion of the surveillant assemblage and argue that contemporary surveillance is heterogeneous, involves humans and non-humans, state and extra-state institutions, and "allows for the scrutiny of the powerful by both institutions and the general population" (Haggerty and Ericson 2000/2007, 112). Lyon (1994, 26, 67) argues that Foucault's notion of the panopticon does not give attention to two central features of contemporary surveillance: information technologies and consumerism. Connected to this critique of Foucault is the claim that the contemporary Internet makes surveillance more democratic or participatory (for example: Albechtslund 2008; Campbell and Carlson 2002; Cascio 2005; Dennis 2008; Haggerty 2006; Whitaker 1999).

There is no ultimate solution to the question of whether Foucault and the notion of the panopticon are suited for analyzing contemporary surveillance and Internet surveillance; it is an open controversial issue. The contributions in this volume show that the role of Foucault, the panopticon, and George Orwell's Big Brother for surveillance studies continues to be discussed in a controversial manner and that this controversy is also important for Internet studies and web 2.0 studies.

For Gandy, especially, corporations and the state conduct surveillance: "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). Toshimaru Ogura (2006, 272) argues that "the common characteristics of surveillance are the management of population based on capitalism and the nation state". Because of the importance of political actors and economic actors in surveillance, we give special attention to aspects of economic and political surveillance on the Internet in this book.

1.4. ECONOMIC IMPLICATIONS OF INTERNET SURVEILLANCE

The production, distribution, and consumption of commodities is one of the defining features of contemporary societies. If the claim that surveillance has become a central quality of contemporary society is true, then this means that surveillance shapes and is shaped by economic production, circulation, and consumption. The economy therefore constitutes an important realm of Internet surveillance that needs to be studied.

Historically, the surveillance of workplaces, the workforce, and production has been the central aspect of economic surveillance. Zuboff (1988) has stressed that computers advance workplace panopticism. As workplaces have become connected to cyberspace, employees tend to produce, receive, transmit, and process more data in less time. They leave digital traces in digital networks that allow the reconstruction and documentation of their activities. The Internet therefore poses new potentials and threats for workplace and workforce surveillance.

Commodities are not only produced, they also circulate in markets and are consumed. Without consumption there is no realization of profit and therefore no growth of the economic operations of firms. The rise of Fordist mass production and mass consumption after 1945 has extended and intensified the interest of corporations to know details about the consumption patterns of citizens. This has not only resulted in the rise of the advertising industry, but also in the intensification of consumer research and consumer surveillance. The rise of flexible accumulation strategies in the 1980s (Harvey 1989) has brought about an individualization and personalization of commodities and advertising. The Internet poses new opportunities for consumer surveillance and new risks for consumers. Technologies such as cookies, data mining, collaborative filtering, ambient intelligence,

clickstream analysis, spyware, web crawlers, log file analysis, etc. allow an extension and intensification of consumer surveillance with the help of the Internet. It therefore becomes a central task to analyze how consumer surveillance works on the Internet and which policy implications this phenomenon brings about. Targeted advertising, spam mail, the collection and marketing of e-mail addresses and user data for commercial purposes, detailed consumer profiling, privacy policies, terms of use, the role of opt-in and opt-out solutions, and fair information practices on the Internet are just some of the important and pressing research topics (see for example Andrejevic 2002; Bellman et al. 2004; Campbell and Carlson 2002; Caudill and Murphy 2000; Culnan and Bies 2003; Fernback and Papacharissi 2007; Lauer 2008; Milne, Rohm, and Bahl 2004; Miyaziki and Krishnamurthy 2002; Ryker et al. 2002; Sheehan and Hoy 2000; Solove 2004b; Turow 2006; Wall 2006; Wang, Lee, and Wang 1998).

Only a few randomly selected opinions about the economic dimension of Internet surveillance can be briefly mentioned in this short introduction. "The effectiveness of targeted marketing depends upon data, and the challenge is to obtain as much of it as possible" (Solove 2004b, 19). "Moreover, companies such as Microsoft and Yahoo are beginning to select ads for people based on combining the tracking of individuals' search or web activities with huge amounts of demographic and psychographic data they are collecting about them. Privacy advocates worry that people know little about how data are collected online, or about the factors that lead such firms to reach out to them with certain materials and not others" (Turow 2006, 299). David Wall argues that surveillant technologies of the Internet such as spyware, cookies, spam spider boots, peer-to-peer technologies, and computer-based profiling "make possible the accumulation and exploitation of valuable personal information" (Wall 2006, 341) and "have facilitated the growth in information capital(ism)" (Wall 2006, 340). "The tremendous technical resources of information technology find a vast new field in identifying, tracking, and attempting to channel the consumption activities of householders in the advanced societies. The data gleaned from available records of purchasing patterns and purchasing power are combined both to allure consumers into further specific styles of spending and also to limit the choices of those whose records indicate that at some point they have failed to conform to proper consuming norms, or have transgressed their spending abilities and accrued unacceptable debts" (Lyon 1994, 137). Mathiesen (2004) uses the notion of the synopticon in order to stress that corporations dominate the Internet and manipulate users in order to establish a system of silencing. "Progress in information processing caused the advancement of the segmentation of mass consumers into many categories of consumers" (Ogura 2006, 275).

Economic surveillance includes aspects such as workplace surveillance, consumer surveillance, industrial espionage, or the surveillance of competition. A frequent concern of web 2.0 users is that employers or potential employers could spy on them with the help of Google or social networking sites and could thereby gain access to personal information that could

cause job-related disadvantages (Fuchs 2009b). This phenomenon shows that web 2.0 has dramatic implications for economic surveillance that need to be understood and analyzed.

Studying the role of the Internet in economic surveillance is an important task. The contributions in this book contribute to this task.

1.5. POLITICAL IMPLICATIONS OF INTERNET SURVEILLANCE

Internet surveillance has important implications for political regulation, state power, and civil society.

E-government has in recent years emerged as an important phenomenon of online politics. Toshimaru Ogura (2006) argues that e-government is an ideology and advances surveillance by governments.

> E-government creates another route for making consensus with the public by using ICT. ICT allows government to access the constituency online, and monitor their political needs. As public comments online exemplify the case, the government tries to make any interactive discourse with people who want to participate in the policy-making process. This looks more democratic and more effective than the representative decision-making system. However, online democracy only has a narrow basis of permissible scope for discussion because it is based on an 'if/and/or' feedback system of cybernetics. It cannot raise concerns about the fundamental preconditions and essential alternatives or transformation of regime. It ignores the opposition forces outside of partnership strategies that refuse the feedback system itself. (Ogura 2006, 288)

There are different regulatory regimes and options at the policy level that governments and civil society can pursue in dealing with Internet surveillance and its privacy implications at the political level. The US approach in privacy regulation relies on the free market and self-regulation by corporations. It makes some exceptions from the self-regulation rule such as data held by financial institutions and data relating to children (Children's Online Privacy Protection Act 1998). It conceives privacy primarily as a commodity. The EU approach defines privacy as a fundamental right that needs to be protected by the state (Data Protection Directive 95/46/EC of the European Parliament 1995) (Ashworth and Free 2006; Caudill and Murphy 2000).

The terrorist attacks of September 11, 2001, and the subsequent wars in Iraq and Afghanistan have brought about important privacy- and surveillance-policy changes that have implications for Internet surveillance. We can only mention a few examples here. The EU's 2006 Data Retention Directive requires the member states to pass laws that require communication service providers to store identification and connection data for phone calls and Internet communication for at least six months. The USA Patriot Act of 2001 (*U*niting and *S*trengthening *A*merica by *P*roviding *A*ppropriate *T*ools

*R*equired to *I*ntercept and *O*bstruct *T*errorism Act of 2001) in section 210 widened the scope of data that the government can obtain from Internet service providers with subpoenas (besides name, address, and identity, data such as session times and durations, used services, device address information, payment method, bank account, and credit card number can also be obtained). The Act extended wiretapping from phones to e-mail and the Web. The use of roving wiretaps was extended from the law enforcement context to the foreign intelligence context, and government no longer has to show that the targeted person is using the communication line in order to obtain surveillance permission from a court. The regulation that surveillance of communications for foreign intelligence requires proof that intelligence gathering is the primary purpose has been changed to the formulation that it must only be a significant purpose. Pen/trap surveillance allows law enforcement to obtain information on all connections that are made from one line. Prior to the Patriot Act, law enforcement agencies had to show to the court that the device had been used for contacting a foreign power in order to gain the permission to monitor the line. The Patriot Act changed the formulation in the law so that law enforcement agencies only have to prove to the court that the information that is likely to be obtained is relevant to an ongoing criminal investigation. This amendment made it much easier for law enforcement agencies to engage in Internet surveillance. Section 505, which allowed the FBI to obtain data on any user from Internet service providers, was declared unconstitutional in 2004. The Combating Terrorism Act that was passed in September 2001 legalized the installation of Carnivore Internet filtering systems by intelligence services at Internet service providers without a judge's permission. The Patriot Act confirmed this rule.

There is a significant debate about the question of whether these regulatory changes bring about conditions that advance a total or maximum surveillance society (see for example Kerr 2003 and Solove 2004a for two opposing views). Such debates show that discussing the continuities and discontinuities of Internet surveillance before and after 9/11 is important. The contributions in this book make a significant contribution to these debates.

Some scholars have argued that the post-9/11 condition is characterized by the ideological normalization of surveillance. "It is also likely that the use of data mining in the so-called 'war against terrorists' will soften the public up for its use in a now quiescent war against global competitors, and the threat to shrinking profits" (Gandy 2003, 41). Bigo argues that surveillance technologies have become so ubiquitous and "are considered so banal [. . .] that nobody (including the judges) asks for their legitimacy and their efficiency after a certain period of time" (Bigo 2006, 49). He speaks in this context of the ban-opticon, which results in the normalization of emergency. "My hypothesis is that surveillance [. . .] is easily accepted because all sorts of watching have become commonplace within a 'viewer society', encouraged by the culture of TV and cinema. [. . .] It is not too much of stretch to suggest that part of the enthusiasm for adopting new surveillance technologies, especially after 9/11, relates to the fact that in the

global north (and possibly elsewhere too) the voyeur gaze is a commonplace of contemporary culture" (Lyon 2006a, 36, 49).

Naomi Klein has stressed the connection between corporate and political interests in fostering surveillance in general and Internet surveillance in particular after 9/11.

> In the nineties, tech companies endlessly trumpeted the wonders of the borderless world and the power of information technology to topple authoritarian regimes and bring down walls. Today, inside the disaster capitalism complex, the tools of the information revolution have been flipped to serve the opposite purpose. In the process, cell phones and Web surfing have been turned into powerful tools of mass state surveillance by increasingly authoritarian regimes, with the full cooperation of privatized phone companies and search engines. [. . .] Many technologies in use today as part of the War on Terror—biometric identification, video surveillance, Web tracking, data mining, sold by companies like Verint Systems and Scisint, Accenture and ChoicePoint—had been developed by the private sector before September 11 as a way to build detailed customer profiles, opening up new vistas for micromarketing. [. . .] September 11 loosened this logjam in the market: suddenly the fear of terror was greater than the fear of living in a surveillance society. (Klein 2008, 302f)

The operators of Facebook, the most popular social networking sites, have continuously witnessed user protests against changes of the privacy policy and the terms of use that are perceived to bring about privacy threats and more surveillance. Such protests show the potential of the Internet for the global networked initiation, coordination, and support of protests. Various scholars have in this context coined terms such as cyberprotest and cyberactivism (see for example McCaughey and Ayers 2003; van de Donk et al. 2004). Fuchs (2008a, 277–289) has distinguished between cognitive, communicative, and cooperative cyberprotest as three forms of protest on the Internet. Cyberprotest is an expression of civil society- and social movement-activism. Surveillance as political phenomenon has always been connected to the rise and the activities of citizen groups. The Internet in general and web 2.0 in particular bring about specific conditions for social movement activities that relate to the political topic of surveillance. It is an important task for contemporary Internet studies and surveillance studies to conduct research on the relationship of Internet, surveillance, and social movements.

The Los Angeles Police Department (LAPD) stopped the African-American Rodney King in his car on March 3, 1991, after a freeway chase. King resisted arrest, which resulted in a brutal beating by the police from which he suffered a fracture of a leg and of a facial bone. The four police officers, Briseno, Koon, Powell, and Wind, were tried for police brutality and acquitted by a LA court in April 1992. George Holiday filmed the beating of King with a low technology home video camera. When the news of the acquittal of the officers and the video made their way to the mass media,

outrage spread, and many observers came to hold the view that both the LAPD and the justice system engaged in racism against African-Americans. The event triggered riots in Los Angeles in April 2002. John Fiske (1996) discusses the role of video cameras in the Rodney King example and other cases in order to show that the miniaturization, cheapening, and mass availability of video cameras changes surveillance. "Videotechnology extends the panoptic eye of power [. . .], but it also enables those who are normally the object of surveillance to turn the lens and reverse its power" (Fiske 1996, 127). "The videolow allows the weak one of their few opportunities to intervene effectively in the power of surveillance, and to reverse its flow. [. . .] The uses of videolow to extend disciplinary surveillance can be countered [. . .] by those who turn the cameras back upon the surveillers" (Fiske 1996, 224f). Today, we live in an age where the Internet shapes the lives of many of us. The Internet has become a new key medium of information, communication, and co-production. Therefore, paraphrasing Fiske, we can say that the Internet extends the panoptic eye of power, but it also enables those who are normally objects of surveillance to turn the eyes, the ears, and the voice on the powerful and reverse the power of surveillance. We can in such cases speak of Internet counter-surveillance.

Neda Agha-Soltan, a 27-year-old Iranian woman, was shot on June 20, 2009, by Iranian police forces during a demonstration against irregularities at the Iranian presidential election. Her death was filmed with a cellphone video camera and uploaded to YouTube. It reached the mass media and caused worldwide outrage over Iranian police brutality. Discussions about her death were extremely popular on Twitter following the event. The protestors used social media such as Twitter, social networking platforms, or the site Anonymous Iran for coordinating and organizing protests. The Facebook profile image of another Iranian woman, Neda Soltani, was mistakenly taken for being a picture of the killed woman. It made its way to the mass media and caused threats to Ms. Soltani, who as a result had to flee from Iran to Germany. This example on the one hand shows the potential for counter-power that the Internet poses, but also the problems that can be created by information confusion in large information spaces. The newspaper vendor Ian Tomlinson died after being beaten to the ground by British police forces when he watched the G-20 London summit protests as a bystander on April 1, 2009. The police claimed first that he died of natural causes after suffering a heart attack. But a video showing police forces pushing Tomlinson to the ground surfaced on the Internet, made its way to the mass media, and resulted in investigations against police officers.

These examples show that the Internet not only is a surveillance tool that allows the state and corporations to watch citizens and to create political profiles, criminal profiles, and consumer profiles, but that it also poses the potential for citizens to conduct surveillance of the powerful and to try to exert counter-power that tries to create public attention for injustices committed by the powerful against the weak. The Internet is therefore a surveillance power and potentially a counter-surveillance power. There are ways

of watching the watchers and surveilling the surveillers. After the Rodney King incident, copwatch initiatives that watch police forces in order to stop police brutality became popular in the US and Canada. Since the turn of the millennium, scepticism against the power of corporations has intensified and has been supported by Internet communication. Corporate watch sites have emerged on the Internet. They document corporate crimes and injustices caused by corporations. Large corporations have huge financial power and have influence so that they are enabled to frequently hide the details, size, nature, and consequences of their operations. Economic and political power tries to remain invisible at those points where it is connected to injustices. Watch sites are attempts to visualize the injustices connected to power; they try to exert a counter-hegemonic power that makes use of the Internet. Alternative online media try to make available critical information that questions power structures that normally remain unquestioned and invisible. The most popular alternative online medium is Indymedia. Indymedia Centres are seen by John Downing (2003, 254; see also 2002) as practices of social anarchism because "their openness, their blend of internationalism and localism, their use of hyperlinks, their self-management, represent a development entirely consonant with the best in the socialist anarchist tradition". For Dorothy Kidd (2003, 64) the Indymedia Centres are "a vibrant commons" among "the monocultural enclosures of the .coms and media giants". Atton (2004, 26f) argues that radical online journalism like Indymedia is "opposed to hierarchical, elite-centred notions of journalism as business" and places "power into the hands of those who are more intimately involved in those stories" so that "activists become journalists". The power of alternative online media derives partly from their open character, which allows citizens to become journalists. WikiLeaks became part of the world news in 2010 because it leaked secret documents about the US wars in Afghanistan and Iraq to the public. Its task is to use the "power of principled leaking to embarrass governments, corporations and institutions"; it is "a buttress against unaccountable and abusive power" (self-description, http://www.wikileaks.org/wiki/WikiLeaks:About, accessed on August 13, 2010). Leaking secret information is understood as a way of watching the powerful and holding them accountable.

But in a stratified society, resources are distributed asymmetrically. Alternative media and watchdog projects are mainly civil society projects that are operated by voluntary labour and are not supported by corporations and governments. They therefore tend to be confronted with a lack of resources such as money, activists, time, infrastructure, or influence. Visibility on the Internet can be purchased and centralized. This situation poses advantages for powerful actors such as states and large corporations and disadvantages for civil society and social movement organizations. It is therefore no surprise that Indymedia is only ranked number 4147 in the list of the most accessed websites, whereas BBC Online is ranked number 44, CNN Online number 52, the *New York Times* Online number 115, Spiegel Online number 152, Bildzeitung Online number 246, or Fox News Online number 250 (data

source: alexa.com, top 1,000,000,000 sites, August 2, 2009). Similarly, concerning the example of Neda Soltan, the Iranian government controls technology that allows them to monitor and censor the Internet and mobile phones, which has resulted in the surveillance of political activists. The surveillance technologies are provided or developed by Western corporations such as Nokia Siemens Networks or Secure Computing.

Power and counter-power, hegemony and counter-hegemony, surveillance and counter-surveillance are inherent potentialities of the Internet. But these potentials are asymmetrically distributed. The Internet in a stratified society involves an asymmetric dialectic that privileges the powerful. It has a power to make visible the invisible, which can be the personal lives of citizens, but also the operations of the powerful. But attention is a scare resource on the Internet, although each citizen can easily produce information, not all information can easily gain similar attention by users. There is an Internet attention economy that is dominated by powerful actors: "Surveillance is not democratic and applied equally to all" (Fiske 1996, 246).

The contributors to this volume show that the political dimension of Internet surveillance is an important realm of analysis and that Internet surveillance has practical political consequences that affect civil society, social movements, citizens, governments, and policies.

1.6. DIMENSIONS AND QUALITIES OF INTERNET SURVEILLANCE

Information technology enables surveillance at a distance, whereas non-technological surveillance, for example when a person is tailed by a detective, is unmediated, does not automatically result in data gathering and requires the copresence, closeness, or proximity of surveiller and the surveilled in one space. Internet surveillance operates in real time over networks at high transmission speed. Digital data doubles can with the help of the Internet be copied and manipulated endlessly, easily, and cheaply. Table 1.1 identifies fourteen dimensions of the Internet and summarizes how these dimensions shape the conditions for Internet surveillance and resistance against Internet surveillance or counter-surveillance. It should be noted that Table 1.1 presents an asymmetric dialectic where resistance is only a precarious potential that is less powerful than the surveillance reality. On the Internet we find an unequal resource distribution, unequal technological innovation diffusion, an unequal distribution of power, etc. (see Fuchs 2008a). The contributions in this book all relate to one or more of these 14 dimensions and show that Internet surveillance is embedded into processes of power and counter-power.

Starke-Meyerring and Gurak (2007) distinguish among three kinds of Internet surveillance technologies: 1) surveillance of personal data captured from general Internet use, 2) surveillance of personal data captured by using specialized Internet services, 3) technologies and practices designed to access data from Internet users. Data can be collected, stored, analyzed, transferred,

Table 1.1 Dimensions and Qualities of Internet Surveillance

Dimension	*Quality of the Internet*	*Internet surveillance*	*Potentials for resisting 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	**data storage switching** data can be transferred from one virtual position to another and deleted at the original points, which makes it harder to detect data, but powerful actors possess powerful surveillance tools (e.g., Echelon), and deleted data might still persist in copies at other places
(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	**real-time activism** coordination of social movements in real time and asynchronous time (cyberactivism)
(3) Speed	**high-speed data transmission**	**high-speed surveillance** availability of high-speed surveillance systems	**increased surveillance complexity** high-speed transmission enlarges the volume of global data transfer and makes surveillance more complex; but state institutions and corporations due to resource advantages frequently have more efficient and powerful systems than users

(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	**increased surveillance complexity** users store more data, which makes surveillance more complex; new storage media develop rapidly so that the transfer of surveillance data becomes more complex, which favours surveillance data loss; but powerful institutions benefit from technological advances much earlier than the everyday user (unequal innovation diffusion)
(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 is easier to find	**data manipulation** data can be consciously manipulated in order to set wrong tracks
(6) Sensory Modality	**multimedia** digital combination of text, sound, image, animation, and video in one integrated medium	**multimodal surveillance** surveillance of multisensory data over one medium	**increased surveillance complexity** messages that are encoded into images, sounds, or videos are difficult to detect (steganography), but there is unequal innovation diffusion
(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	**networked cyberprotest** easy and fast coordination of social movements and protests (cyberprotest), protest communication can quickly intensify and spread over the Internet; but political and corporate actors control huge amounts of resources and therefore visibility on the Internet

(*continued*)

Table 1.1 (*continued*)

Dimension	*Quality of the Internet*	*Internet surveillance*	*Potentials for resisting surveillance*
(8) Information Structure	**hypertext** networked, interlinked, and hypertextual information structures	**linked surveillance** the links between persons can be more easily observed	**networked individualism in cyber-protest** protest can be easier linked and networked; but protest reduces itself frequently to simple isolated point-and-click activities that do not have the same visual power as mass action protests with physical presence
(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	**critical produsage** critical information can be easily produced; but visibility is largely controlled by powerful corporations that dominate the Internet
(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	**creation of digital commons** copy left; open content; intellectual property rights can easily be undermined if many users engage in sharing and cooperation; but control of property rights and attempts to enclose the digital commons are inherent to capitalism and therefore ubiquitous

(11) Context	**decontextualization** decontextualized information and anonymity (authorship, time and place of production, etc. might be unclear)	**intensification of surveillance** decontextualization advances speculative and pre-emptive surveillance	**data anonymity** anonymous data and encrypted messages are harder to trace; but there is an unequal innovation diffusion in this area
(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	**data fakes** fake data might be spread consciously, which makes surveillance more complex, but can also make surveillance more total
(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	**fake identities** fake or anonymous online identities make surveillance more difficult; but also allow the intensification of surveillance based on the argument that anonymity is dangerous, might foster antisocial behaviour, and therefore needs to be controlled
(14) Availability	**ubiquitous Internet** the Internet has become ubiquitous in all spheres of everyday 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	**intensified and extended protest capacities** in everyday life, the Internet is likely to attract a large number of users who increase their e-literacy over time; this increases the mobilization potentials for protests; but the violent and ideological policing of protest and the Internet are profound interests of powerful, resource-intensive actors

accessed, monitored, and solicited. Information privacy intrusion is an improper processing of data that reflects one or more of these seven activities and is unwanted by the users (Wang, Lee, and Wang 1998). Table 1.2 presents a classification scheme for Internet surveillance technologies and techniques.

Privacy-enhancing technologies have been defined as "technical and organizational concepts that aim at protecting personal identity" (Burkert 1998, 125). Privacy-enhancing Internet techniques and technologies are, for example: encryption technologies, virus protection, spyware protection tools, firewall, opt-out mechanisms, reading privacy policies, disabling of cookies, spam filters, cookie busters, or anonymizers/anonymous proxy. Dwayne Winseck (2003) cautions that the focus on privacy-enhancing technologies as an answer to surveillance technologies advances "a technocratic approach to managing personal information" and "fails to grasp how power shapes the agenda and overall context in which struggles over technological design occur" (Winseck 2003, 188). Formulated in another way: Privacy-enhancing technologies advance a techno-deterministic ideology that does not question power structures and advances the idea that there is a technological fix to societal problems. Nonetheless it is an important task for Internet studies and surveillance studies to explore ways that privacy-enhancing Internet technologies can be used for minimizing threats. This will not pose solutions to societal problems, but could to a certain extent empower citizens. It is therefore important to take into account that the implementation of privacy-enhancing Internet technologies "forces us to return to social innovation in oreder to successfully implement them" (Burkert 1998, 140).

Classifying privacy-threatening and privacy-enhancing technologies is an important aspect of studying the Internet and surveillance. The contributors to this volume help advance this task.

1.7. CONCLUSION

Howard Rheingold argues that the new network technologies available today that open "new vistas of cooperation also make[s] possible a universal surveillance economy and empower[s] the bloodthirsty as well as the altruistic" (Rheingold 2002, xviii). This book, *The Internet and Surveillance* explores the two sides of the information society that Rheingold mentions. It shows that information technology has a dark and a bright side and that Internet surveillance is deeply enmeshed into the power relations that shape contemporary society.

This book has two parts: Theoretical Foundations of Internet Surveillance Studies (Part I); Case Studies, Applications, and Empirical Perspectives of Internet Surveillance Studies (Part II). The first part predominantly focuses on defining Internet surveillance and web 2.0 surveillance and on identifying its key qualities. The second part presents more applied research, analyses of specific examples of Internet/web 2.0 studies; it is more empirical in character.

Table 1.2 A Classification of Internet Surveillance Techniques (based on Wang, Lee, and Wang 1998)

	Improper data acquisition			*Improper data use*		*Privacy invasion*	
Technology, practices	*Improper collection*	*Improper access (to stored data that is only available to single individuals or a small group)*	*Improper monitoring*	*Improper analysis*	*Improper transfer*	*Unwanted solicitation*	*Improper storage*
spam mail	X					X	X
consumer profiling (including cookies, storage of click-stream data)	X		X	X	X	X	X
online eaves-dropping by state institutions	X	X	X	X	X		X
spyware	X	X	X	X	X		X
selling or transfer of personal data to third parties				X	X	X	X
no opt-out			X	X	X	X	X
digital rights man-agement tools	X		X	X	X		X

(*continued*)

Table 1.2 (*continued*)

	Improper data acquisition			*Improper data use*		*Privacy invasion*	
Technology, practices	*Improper collection*	*Improper access (to stored data that is only available to single individuals or a small group)*	*Improper monitoring*	*Improper analysis*	*Improper transfer*	*Unwanted solicitation*	*Improper storage*
web bugs	X		X	X	X		X
web crawlers, bots	X		X	X	X	X	X
e-mail and Internet usage surveillance of employees by employers		X	X	X			
targeted online advertising	X		X	X	X	X	X
ISP log file access by government institutions	X	X	X	X	X		X
packet sniffers (e.g., Carnivore)			X	X	X		
phishing, pharming	X	X	X		X	X	X

The theory part of this book has five chapters. *Christian Fuchs* focuses on analyzing and criticizing the political economy of web 2.0 surveillance. Fuchs situates the commercial web 2.0 in the Marxian analysis of capital accumulation and connects this analysis with notions like Dallas Smythe's audience commodity, Oscar Gandy's panoptic sort, Thomas Mathiesen's silent silencing, and Manuel Castells's mass self-communication. *Mark Andrejevic* connects the concept of online surveillance with an analysis of power and control. Andrejevic reminds us that there is a power asymmetry between those engaging in surveillance and those who are the objects of surveillance in the Internet economy. He makes use of Karl Marx's concepts of exploitation and alienation. *Daniel Trottier and David Lyon* provide an empirically grounded identification of five qualities of what they term social media surveillance. These qualities are: (a) collaborative identity construction, (b) lateral ties, (c) the visibility, measurability and searchability of social ties, (d) the dynamic change of social media interfaces and contents, (e) the recontextualization of social media content. *David Hill* connects the notion of Internet surveillance with a detailed interpretation of Jean-François book *The Inhuman*. Hill argues that this inhumanity takes on two predominant forms: the error-prone fetish of algorithmic calculation that can easily advance injustices, and the extension of the capitalist performance principle and consumer culture into all realms of life. *Thomas Allmer* discusses panoptic-oriented and non-panoptic ways of defining Internet surveillance. He points out the importance of economic surveillance in capitalist society and of economic Internet surveillance in contemporary capitalist society. He argues for a critical approach that is grounded in Marxist theory.

The part on case studies, applications, and empirical perspectives of this book consists of eight chapters. *Marisol Sandoval* analyzes the privacy policies and terms of use of more than fifty of the most popular web 2.0 platforms. Her approach is an empirical application of critical political economy to web 2.0 surveillance. The analysis shows that web 2.0 is dominated by corporations that monitor user data in order to accumulate capital by selling user data to advertising companies that provide targeted advertising to the users. The study also shows that commodification tends to be ideologically masked in the privacy policies and the terms of use. *David Arditi* discusses the role of surveillance in the realm of file sharing. He shows that the culture industry tries to use surveillance for on the one hand forestalling music sharing on the Internet and on the other hand for analyzing and exploiting data about music consumption preferences that are commodified. Arditi's chapter is based on a critical understanding of the culture industry that questions corporations' domination of the Internet and culture. *Anders Albrechtslund* analyzes the role of information sharing in web 2.0. He is particularly interested in how such sharing practices shape urban spaces. He interprets online sharing as a form of social, participatory surveillance. He gives particular attention to location-based information sharing, as enabled by applications like Foursquare and Facebook places that are mainly used on mobile phones

that support mobile Internet access. *Iván Székély* reports results from an empirical study that analyzed the knowledge, opinion, values, attitudes and self-reported behaviour of IT professionals in the area of handling personal data in Hungary and the Netherlands. Studying the attitudes of IT professionals on privacy and surveillance is crucial because they are the ones who design surveillance systems. The study shows that IT professional tend to have a rather instrumental view of privacy and surveillance in their work practices. *Miyase Christensen and André Jansson* conceptually combine surveillance theory, the concept of transnationalism, and the Bourdieuian notion of the field. They apply this approach for conducting two case studies: The first study deals with transnational migrants of Turkish/Kurdish origin residing in urban Sweden; the second with a Scandinavian expatriate community in Nicaragua, linked to the global development business. *Kent Wayland, Roberto Armengol, and Deborah Johnson* make a conceptual differentiation between surveillance and transparency. They discuss issues of online transparency in relation to the online disclosure of donations in electoral campaigns. They introduce in this context the notion of the house of mirrors. *Monika Taddicken* presents results from a study of attitudes of social web users towards privacy and surveillance, in which focus group interviews were conducted. The study shows a high general concern about online privacy violations and surveillance, a lack of concrete knowledge about online surveillance mechanisms, and the importance of the social and communicative motive of web 2.0 users. *Rolf Weber* discusses legal aspects of online privacy and online surveillance. The chapter shows the importance of discussing which legal understandings of privacy are required in an age where our communication is increasingly taking place online and is mediated by online surveillance systems. The contribution also points out the problems of politically and legally regulating a global space like the Internet with policy frameworks that are primarily national in character.

This book is introduced by a preface written by *Thomas Mathiesen*, who is one of the most frequently cited and influential scholars in surveillance studies, and concluded by a postface written by *Kees Boersma* that identifies the key issues and approaches represented in this book.

ACKNOWLEDGMENTS

This publication is supported by COST—European Cooperation in Science and Technology. It is a result of the COST Action "Living in Surveillance Societies" (IS0807, chair: Dr. William Webster, University of Stirling).

The Living in Surveillance Societies (LiSS) COST Action is a European research programme designed to increase and deepen knowledge about living and working in the surveillance age, in order to better understand the consequences and impacts of enhanced surveillance, and subsequently to make recommendations about its future governance and practice. Further information about LiSS can be found at, URL: http://www.liss-cost.eu/

This publication has emerged from Working Group 2 'Surveillance Technologies in Practice' of the Living in Surveillance Societies COST Action and a number of the contributions were presented and discussed at Working Group meetings and at the Living in Surveillance Societies Annual Conference in London in April 2010. The editors would like to thank the members of LiSS Working Group 2 for their constructive feedback and support.

REFERENCES

Albrechtslund, Anders. 2008. Online social networking as participatory surveillance. *First Monday* 13 (3).

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.

———. 2004. *Reality TV: The work of being watched*. Lanham, MD: Rowman & Littlefield.

———. 2007. *iSpy: Surveillance and power in the interactive era*. Lawrence: University Press of Kansas.

———. 2009. Critical media studies 2.0: an interactive upgrade. *Interactions: Studies in Communication and Culture* 1 (1): 35–51.

Ashworth, Laurence and Clinton Free. 2006. Marketing dataveillance and digital privacy. *Journal of Business Ethics* 67 (2): 107–123.

Atton, Chris. 2004. *An alternative internet*. Edinburgh: Edinburgh University Press.

Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. International differences in information privacy concerns: a global survey of consumers. *The Information Society* 20 (5): 313–324.

Benkler, Yochai. 2006. *The wealth of networks*. New Haven: Yale University Press.

Bigo, Didier. 2006. Security, exception, ban and surveillance. In *In Theorizing surveillance*, ed. David Lyon, 46–68. Portland, OR: Willan.

Bogard, William. 2006. Surveillance assemblage and lines of flight. In *Theorizing surveillance*, ed. David Lyon, 97–122. Portland, OR: Willan.

Boyle, James. 1997. Foucault in cyberspace. *University of Cincinnati Law Review* 66 (1): 177–205.

Bruns, Axel. 2008. *Blogs, wikipedia, second life, and beyond: From production to produsage*. New York: Peter Lang.

Burkert, Herbert. 1998. Privacy-enhancing technologies. In *Technology and privacy*, ed. Philip E. Agre and Marc Rotenberg, 125–142. Cambridge: MIT Press.

Cammaerts, Bart. 2008. Critiques on the participatory potentials of web 2.0. *Communication, Culture & Critique* 1 (4): 358–377.

Campbell John E. and Matt Carlson M. 2002. Panopticon.com: online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media* 46 (4): 586–606.

Carpentier, Nico and Benjamin de Cleen. 2008. Introduction: blurring participations and convergences. In *Participation and media production*, ed. Nico Carpentier and Benjamin de Cleen, 1–12. Newcastle: Cambridge Scholars.

Cascio, Jamais. 2005. The rise of the digital panopticon. http://www.worldchanging.com/archives/002651.html (accessed September 5, 2009).

Castells, Manuel. 2001. *The Internet galaxy*. Oxford: Oxford University Press.

———. 2009. *Communication power*. Oxford: Oxford University Press.

Caudill, Eve M. and Patrick E. Murphy. 2000. Consumer online privacy: legal and ethical issues. *Journal of Public Policy & Marketing* 19 (1): 7–19.

Clarke, Roger. 1988. Information technology and dataveillance. *Communications of the ACM* 31 (5): 498–512.
———. 1994. Dataveillance: delivering '1984'. In *Framing technology: Society, choice and change*, ed. Lelia Green and Roger Guinery, 117–130. Sydney: Allen & Unwin.
Cohen, Nicole S. 2008. The valorization of surveillance: towards a political economy of Facebook. *Democratic Communique* 22 (1): 5–22.
Culnan, Mary J. and Robert J. Bies. 2003. Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues* 59 (2): 323–342.
Dennis, Kingsley. 2008. Keeping a close watch—the rise of self-surveillance and the threat of digital exposure. *The Sociological Review* 56 (3): 347–357.
Deuze, Mark. 2007. *Media work*. Cambridge: Polity.
———. 2008. Corporate appropriation of participatory culture. In *Participation and media production*, ed. Nico Carpentier and Benjamin de Cleen, 27–40. Newcastle: Cambridge Scholars.
Downing, John H. 2002. Independent media centres: a multi-local, multi-media challenge to neoliberalism. In *Global media policy in the new millennium*, ed. Marc Raboy, 215–232. Luton: University of Luton Press.
———. 2003. The independent media center movement and the anarchist socialist tradition. In *Contesting media power: Alternative media in a networked world*, ed. Nick Couldry and James Curran, 243–257. Lanham: Rowman & Littlefield.
Elmer, Greg. 2003. A diagram of panoptic surveillance. *New Media & Society* 5 (2): 231–247.
———. 2004. *Profiling machines*. Cambridge: MIT Press.
Fiske, John. 1996. *Media matters*. Minneapolis: University of Minnesota Press.
Foucault, Michel. 1977. *Discipline & punish*. New York: Vintage.
———. 1994. *Power*. New York: New Press.
Fuchs, Christian. 2008a. *Internet and society: Social theory in the information age*. New York: Routledge.
———. 2008b. Book review. Don Tapscott and Anthony D. Williams: *Wikinomics*. *International Journal of Communication* 2 (2008): 1–11.
———. 2009a. Information and communication technologies and society: a contribution to the critique of the political economy of the Internet. *European Journal of Communication* 24 (1): 69–87.
———. 2009b. *Social networking sites and the surveillance society: A critical case study of the usage of studiVZ, Facebook, and MySpace by students in Salzburg in the context of electronic surveillance*. Salzburg/Vienna: Research Group UTI.
———. 2009c. Some reflections on Manuel Castells' book *Communication Power*. *tripleC* 7 (1): 94–108.
———. 2010a. Class and knowledge labour in informational capitalism and on the Internet. *The Information Society* 26 (3): 179–196.
———. 2010b. Social software and web 2.0: their sociological foundations and implications. In *Handbook of research on web 2.0, 3.0, and X.0: Technologies, business and social applications*, ed. San Murugesan, 764–789. Hershey, PA: IGI-Global.
———. 2011. *Foundations of critical media and information studies*. New York: Routledge.
Gandy, Oscar H. 1993. *The panoptic sort: A political economy of personal information*. Boulder: Westview.
———. 2003. Data mining and surveillance in the post-9/11 environment. In *The intensification of surveillance*, ed. Kirstie Ball and Frank Webster, 26–41. London: Pluto.
Gordon, Diana. 1987. The electronic panopticon. *Politics and Society* 15 (4): 483–511.
Graham, Stephen and David Wood. 2003/2007. Digitizing surveillance: categorization, space, inequality. In *The surveillance studies reader*, ed. Sean P. Hier and Josh Greenberg, 218–230. Berkshire: Open University Press.

Haggerty Kevin. 2006. Tear down the walls: on demolishing the panopticon. In *Theorizing surveillance*, ed. David Lyon, 23–45. Portland, OR: Willan.
Haggerty, Kevin and Richard Ericson. 2000/2007. The surveillant assemblage. In *The surveillance studies reader*, ed. Sean P. Hier and Josh Greenberg, 104–116. Berkshire: Open University Press.
Harvey, David. 1989. *The condition of postmodernity*. London: Blackwell.
Jenkins, Henry. 2008. *Convergence culture*. New York: New York University Press.
Kerr, Orin S. 2003. Internet surveillance law after the USA Patriot Act: the big brother that isn't. *Northwestern University Law Review* 97 (2): 607–673.
Kidd, Dorothy. 2003. Indymedia.org: a new communications common. In *Cyber-activism*, ed. Martha McCaughey and Michael D. Ayers, 47–69. New York: Routledge.
Klein, Naomi. 2008. *The shock doctrine: The rise of disaster capitalism*. London: Penguin.
Lauer, Josh. 2008. Alienation in the information economy: toward a Marxist critique of consumer surveillance. In *Participation and media production*, ed. Nico Carpentier and Benjamin De Cleen, 41–53. Newcastle: Cambridge Scholars.
Lovink, Geert. 2008. *Zero comments: Blogging and critical internet culture*. New York: Routledge.
Lyon, David. 1994. *The electronic eye: The rise of surveillance society*. Cambridge: Polity.
———. 1998. The world wide web of surveillance: the Internet and off-world power-flows. *Information, Communication & Society* 1 (1): 91–105.
———. 2001. *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.
———. 2003. Surveillance as social sorting: computer codes and mobile bodies. In *Surveillance as social sorting*, ed. David Lyon, 13–30. New York: Routledge.
———. 2006a. 9/11, synopticon, and scopophilia: watching and being watched. In *Surveillance and visibility*, ed. Kevin Haggerty and Richard Ericson, 35–54. Toronto: University of Toronto Press.
———. 2006b. The search for surveillance theories. In *Theorizing surveillance*, ed. David Lyon, 3–20. Portland, OR: Willan.
Marx, Gary T. 1988. *Undercover: Police surveillance in America*. Berkeley: University of California Press.
———. 2002. What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society* 1 (1): 9–29.
Mathiesen, Thomas. 1997. The viewer society: Michel Foucault's 'panopticon' revisited. *Theoretical Criminology* 1 (2): 215–234.
———. 2004. Panopticon and synopticon as silencing systems. In *Silently silenced: Essays on the creation of acquiesence in modern society*, 98–102. Winchester: Waterside.
Milne, George R., Andrew J. Rohm, and Shalini Bahl. 2004. Consumers' protection of online privacy and identity. *Journal of Consumer Affairs* 38 (2): 217–232.
McCaughey, Martha and Michael D. Ayers, ed. 2003. *Cyberactivism*. New York: Routledge.
Miyazaki, Anthony and Sandeep Krishnamurthy. 2002. Internet seals of approval: effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs* 36 (1): 28–49.
Ogura, Toshimaru. 2006. Electronic government and surveillance-oriented society. In *Theorizing surveillance*, ed. David Lyon, 270–295. Portland, OR: Willan.
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 (accessed August 10, 2009).
Parenti, Christian. 2003. *The soft cage*. New York: Basic Books.
Poster, Mark. 1990. *The mode of information*. Cambridge: Polity.

Rämö, Hans and Mats Edenius. 2008. Time constraints in new mobile communication. *KronoScope* 8 (2): 147–157.
Rheingold, Howard. 2002. *Smart mobs: The next social revolution*. New York: Basic Books.
Robins, Kevin and Frank Webster. 1999. *Times of the technoculture*. New York: Routledge.
Ryker, Randy, Elizabeth Lafleur, Chris Cox, and Bruce Mcmanis. 2002. Online privacy policies: an assessment of the fortune E-50. *Journal of Computer Information Systems* 42 (4): 15–20.
Scholz, Trebor. 2008. Market ideology and the myths of web 2.0. *First Monday* 13 (3).
Sheehan, Kim Bartel and Mariea Grubbs Hoy. 2000. Dimensions of privacy among online consumers. *Journal of Public Policy & Marketing* 19 (1): 62–73.
Shiffman, Denise. 2008. *The age of engage*. Ladera Ranch, CA: Hunt Street Press.
Shirky, Clay. 2008. *Here comes everybody*. London: Penguin.
Solove, Daniel J. 2004a. Reconstructing electronic surveillance law. *George Washington Law Review* 72 (6): 1264–1305.
———. 2004b. *The digital person: Technology and privacy in the information age*. New York: New York University Press.
Stanyer, James. 2009. Web 2.0 and the transformation of news and journalism. *In Routledge Handbook of Internet Politics*, ed. Andrew Chadwick and Philip N. Howard, 201–213. New York: Routledge.
Starke-Meyerring, Doreen and Laura Gurak. 2007. Internet. In *Encyclopedia of privacy*, ed. William G. Staples, 297–310. Westport, CT: Greenwood.
Terranova, Tiziana. 2004. *Network culture*. London: Pluto.
Tapscott, Don and Anthony D. Williams. 2006. *Wikinomics: How mass collaboration changes everything*. London: Penguin.
Turow, Joseph. 2006. Cracking the consumer code: advertisers, anxiety, and surveillance in the digital age. In *Surveillance and visibility*, ed. Kevin Haggerty and Richard Ericson, 279–307. Toronto: University of Toronto Press.
van de Donk, Wim, Brian Loader, Paul Nixon, and Dieter Rucht, ed. 2004. *Cyberprotest: New media, citizens and social movements*. New York: Routledge.
van Dijck, José. 2009. Users like you? theorizing agency in user-generated content. *Media, Culture & Society* 31 (1): 41–58.
van Dijck, José and David Nieborg. 2009. Wikinomics and its discontents: a critical analysis of web 2.0 business manifestors. *New Media & Society* 11 (5): 855–874.
van Dijk, Jan. 2000. Models of democracy and concepts of communication. In *Digital democracy*, ed. Kenneth L. Hacker and Jan van Dijk, 30–53. London: Sage.
Wall, David S. 2006. Surveillant Internet technologies and the growth in information capitalism: spams and public trust in the information society. In *Surveillance and visibility*, ed. Kevin Haggerty and Richard Ericson, 340–362. Toronto: University of Toronto Press.
Wang Huaiqing, Matthew K.O. Lee, and Chen Wang. 1998. Consumer privacy concerns about Internet marketing. *Communications of the ACM* 41 (3): 63–70.
Webster, Frank. 2002. *Theories of the information society*. New York: Routledge.
Whitaker, Reginald. 1999. *The end of privacy*. New York: New Press.
Winseck, Dwayne. 2003. Netscapes of power: convergence, network design, walled gardens, and other strategies of control in the information age. In *Surveillance as social sorting*, ed. David Lyon, 176–198. New York: Routledge.
Zuboff, Shoshana. 1988. *In the age of the smart machine*. New York: Basic Books.