The Internet & Surveillance - Research Paper Series

Edited by the Unified Theory of Information Research Group,
Vienna, Austria (http://www.uti.at)

Critical Internet Surveillance Studies and Economic Surveillance

Thomas Allmer

Abstract: *The overall aim of Critical Internet Surveillance Studies and Economic Surveillance is to clarify how we can theorize and systemize economic surveillance on the Internet. Surveillance studies scholars like David Lyon (1998, 95; 2003b, 163) accentuates that economic surveillance on the Internet such as monitoring consumers or the workplace are central aspects of modern surveillance societies. The approach that is advanced in this work recognizes the importance of the role of the economy in contemporary surveillance societies. This contribution constructs theoretically founded typologies in order to systemize the existing literature of Internet surveillance studies and to analyze examples of surveillance. Therefore, it mainly is a theoretical approach combined with illustrative examples, advancing from the abstract to the concrete level. This paper contains a systematic discussion of the state of the art of Internet surveillance and clarifies how different notions treat economic aspects of Internet surveillance. In this work it is argued that the existing literature is insufficient for studying economic surveillance on the Internet. In contrast, a typology of surveillance in the modern economy, which is based on foundations of a political economy approach, allows to systemize economic surveillance and to analyze surveillance in the spheres of production, circulation, and consumption. Constructing a theoretically founded typology of economic surveillance is important in order to undertake a systematic analysis of online surveillance in the modern economy. Finally, some political recommendations are drawn in order to overcome economic online surveillance. This contribution can be fruitful for scholars who want to undertake a systematic analysis of Internet surveillance in the modern economy and who want to study the field of surveillance critically.*

Keywords: surveillance society, Panopticon, Internet, political economy, economic surveillance, workplace surveillance, pre-employment screening, consumer surveillance

Short biography of the author/s: Thomas Allmer has studied media and communication at the University of Salzburg and the Victoria University of Melbourne. He currently is PhD student at the University of Salzburg and research associate of the project "Social Networking Sites in the Surveillance Society". He is member of the Unified Theory of Information Research Group and of the working group "Living in the Surveillance Age" of the European Cooperation in Science and Technology Action "Living in Surveillance Societies". Thomas is member of the editorial team of tripleC: Journal for a Global Sustainable Information Society.

1. Introduction

Surveillance has notably increased in the last decades of modern society. Surveillance studies scholars like David Lyon (1994) or Clive Norris and Gary Armstrong (1999) stress that we live in a surveillance society. Although there are a lot of other features in contemporary society, such as information, neoliberalism, globalization, or capitalism, surveillance in general and Internet surveillance in particular are crucial phenomena. For instance, web 2.0 activities, such as creating profiles and sharing ideas on Facebook, announcing personal messages on Twitter, uploading or watching videos on YouTube, and writing personal entries on Blogger, enables the collection, analyzes, and sale of personal data by commercial web platforms.

The overall aim of this chapter is to clarify how we can theorize and systemize such phenomena. Lyon (1998, 95; 2003b, 163) accentuates that economic surveillance on the Internet such as monitoring consumers or the workplace, are central aspects of modern surveillance societies. The approach that is advanced in this chapter recognizes the importance of the role of the economy in contemporary surveillance societies. For doing so, the following thematically grouped research questions are subject to this contribution:

Foundations of Internet surveillance studies

- How is Internet surveillance defined in the existing literature?
- What are commonalties and differences of various notions of Internet surveillance?
- What are advantages and disadvantages of such definitions?

Critical Internet surveillance studies

- Which theory provides a typology in order to systemize Internet surveillance in the modern economy?
- What are examples of Internet surveillance in the spheres of production, circulation, and consumption?

This paper wants to undertake a systematic analysis of surveillance in general and Internet surveillance in particular in the modern economy and wants to study the field of surveillance critically. It deals with surveillance in the modern economy and is a critical contribution to surveillance studies insofar as it is based on the foundations of a critical political economy approach. The term Internet refers to the global system of computer networks that use the Internet Protocol Suite (TCP/IP). Emerged in the 1970s, the Internet is a network of networks which includes systems such as the world wide web (WWW) and the infrastructure of electronic mail. According to The Oxford Dictionary of English, the term surveillance originated from the French sur-"over" + veiller "watch" and from the Latin vigilare "keep watch" in the early 19th century (Soanes and Stevenson 2005). The term modern economy refers to the capitalistic economy of modern societies. Modern society is the historical period, which has begun with the Enlightenment and lasts up to today.

This contribution constructs theoretically founded typologies in order to systemize the existing literature of Internet surveillance studies and to analyze examples of sur-

veillance. Therefore, it mainly is a theoretical approach combined with illustrative examples, advancing from the abstract to the concrete level. Based on the research questions and the described methodology, the following structure can be outlined:

Section two analyzes how Internet surveillance is defined in the existing literature, what commonalties and differences of various notions of online surveillance exist, and what advantages and disadvantages such definitions have. Furthermore, section two describes how different notions deal with economic surveillance on the Internet and makes clear if there is a gap in the existing literature in order to study Internet surveillance in the modern economy. The specific economic mode of Internet surveillance is studied in section three. Based on the foundations of a critical political economy approach and the distinction of surveillance in the economy into the spheres of production, circulation, and consumption, a typology of online surveillance in the economy can be constructed. Constructing a theoretically founded typology of economic surveillance is important in order to undertake a systematic analysis of surveillance in the modern economy. Economic surveillance on the Internet in the spheres of production, circulation, and consumption will be outlined. Section four concludes with a summary and makes some political recommendations in order to overcome Internet surveillance in the modern economy.

2. Foundations of Internet Surveillance Studies

Since Michel Foucault has published his book Surveiller et punir in French in 1975 and in English in 1977, the amount of literature on surveillance has increased enormously and represents a diffuse and complex field of research. Lyon (1994, 6-7) stresses: "Michel Foucault's celebrated, and contentious, historical studies of surveillance and discipline had appeared that mainstream social theorists began to take surveillance seriously in its own right". David Murakami Wood (2003, 235) emphasizes that "for Surveillance Studies, Foucault is a foundational thinker and his work on the development of the modern subject, in particular Surveillir et Punir (translated as Discipline and Punish), remains a touchstone for this nascent transdisciplinary field". According to Google Scholar, Foucault's book Discipline and Punish (1977) is cited more than 17 thousand times (scholar.google.com, accessed on September 10, 2010). According to the Encyclopedia of Philosophy (Pryor 2006, 898) and to the Routledge Encyclopedia of Philosophy (Gutting 1998, 708-713), Foucault is one of the most important historians and philosophers of the 20th century with wide influence in different disciplines.

The overall aim of this section is to elucidate how Internet surveillance is defined in the existing literature, what commonalties and differences of various notions of online surveillance exist, and what advantages and disadvantages such definitions have. For doing so, Foucault's understanding of surveillance and the idea of the panopticon are introduced (subsection one). Based on these findings, subsections two and three of this section contain a systematic discussion of the state of the art of Internet surveillance by establishing a typology of the existing literature and discussing commonalties and differences. For analyzing the existing literature on a more ab-

stract level and identifying advantages and disadvantages, it is essential to discuss commonalties and differences and to find certain typologies. Finally, subsection four gives a summary, discusses how different notions deal with Internet surveillance in the modern economy and makes clear if there is a gap in the existing literature.

2.1. Foucault's Notion of Surveillance and the Panopticon

Foucault (1995; 2002; 2003; 2007) analyzes surveillance in the context of the emergence of disciplinary societies. He stresses an evolution from feudal societies of torture, to reformed societies of punishment, and on to modern disciplinary societies. In the age of torture, arbitrary penalties and public spectacles of the scaffold took place in order to exterminate bodies. Afterwards, in the age of punishment, defendants were punished and exterminated. In the age of disciplines, direct violence has been replaced with softer forms of power in order to discipline, control, and normalize people in respect of drilling docile bodies and "political puppets" (Foucault 1995, 136).

For Foucault (1995, 195-210), Jeremy Bentham's panopticon is a symbol for modern disciplinary society. "On the whole, therefore, one can speak of the formation of a disciplinary society in this movement that stretches from the enclosed disciplines, a sort of social 'quarantine', to an indefinitely generalizable mechanism of 'panopticism'" (Foucault 1995, 216). The panopticon is an ideal architectural figure of modern disciplinary power. It exists of an annular building divided in different cells and a huge tower with windows in the middle. Prisoners, workers, pupils, as well as patients stay in the cells and a supervisor occupies the middle tower. The architecture allows the supervisor to observe all individuals in the cells without being seen. Not every inmate is observed at every moment, but no one knows if she or he is monitored. Observation is possible anytime. As a result, everyone acts as if kept under surveillance all the time – individuals discipline themselves out of fear of surveillance. The panopticon creates a consciousness of permanent visibility as a form of power, where no bars, chains, and heavy locks are necessary for domination any more. Foucault (1995, 228) finally asks: "Is it surprising that prisons resemble factories, schools, barracks, hospitals, which all resemble prisons?"

In summary, Foucault analyzes surveillance in the context of the emergence of modern disciplinary societies. He understands disciplines as forms of operational power relations and technologies of domination in order to discipline, control, and normalize people. For Foucault, the panopticon is an ideal symbol of modern surveillance societies. Foucault's understanding of surveillance and the panopticon allows to distinguish panoptic (affirmation of Foucault's notion) and non-panoptic (rejection of Foucault's notion) approaches of defining Internet surveillance that can be used for constructing a typology of existing surveillance literature and for discussing commonalties and differences of definitions of Internet surveillance: The task of the following two subsections is to give a representative, but still eclectic overview about different definitions of online surveillance.

2.2.   Non-Panoptic Notions of Internet Surveillance

Lyon understands the "world wide web of surveillance" (Lyon 1998) as a neutral concept that identifies positive consequences such as protection and security as well as negative consequences such as control. Computerization of surveillance makes bureaucratic administration easier (Lyon 2003b, 164) and surveillance in cyberspace permits "greater efficiency and speed, and may well result in increased benefits for citizens and consumers, who experience them as enhancing their comfort, convenience, and safety" (Lyon 2003a, 69). Nevertheless, Lyon says that the nation-state and the capitalist workplace are the main sites of surveillance on the Internet (1998, 95; 2003a, 69; 2003b, 163) and argues that surveillance technologies such as the Internet reinforce asymmetrical power relations on an extensive and intensive level (Lyon 1998, 92). "So surveillance spreads, becoming constantly more routine, more intensive (profiles) and extensive (populations), driven by economic, bureaucratic and now technological forces" (Lyon 1998, 99). The Internet has become a multi-billion dollar industry, because it is primarily corporations that are interested in collecting, analyzing and assessing a huge amount of personal consumer data in order to target personalized advertisement (Lyon 2003b, 162).

Similarly to Lyon's notion of Internet surveillance that assumes there are enabling and constraining effects, Seumas Miller and John Weckert (2000) articulate advantages and disadvantages of being monitored. Their paper examines monitoring at the workplace in general and observing of email and the Internet usage in particular. Although the authors claim that privacy is a moral right (Miller and Weckert 2000, 256) and criticize existing approaches that stress benefits of workplace monitoring for both employers and employees (Miller and Weckert 2000, 258-259), they argue that "surveillance and monitoring can be justified in some circumstances" (Miller and Weckert 2000, 255) and reason: "The proposition must be rejected that the extent and nature of the enjoyment of rights to individual privacy is something to be determined by the most powerful forces of the day, be they market or bureaucratic forces." (Miller and Weckert 2000, 256)

For Anders Albrechtslund (2008), positive aspects of being under surveillance are worth mentioning and he argues that online surveillance also empowers the users, constructs subjectivity, and is playful. Internet surveillance as social and participatory act involves mutuality and sharing.

Online social networking can also be empowering for the user, as the monitoring and registration facilitates new ways of constructing identity, meeting friends and colleagues as well as socializing with strangers. This changes the role of the user from passive to active, since surveillance in this context offers opportunities to take action, seek information and communicate. Online social networking therefore illustrates that surveillance – as a mutual, empowering and subjectivity building practice – is fundamentally social (Albrechtslund 2008).

Hille Koskela (2004; 006) emphasizes individuals' active role in the context of surveillance in general and online surveillance in particular. For instance, reality shows are based on viewer participation, mobile phones with cameras create an active subject, and home webcams generate new subjectivities. Koskela wants to analyze "the other side of surveillance", which has resistant and liberating elements. "Webcams can also be argued to contribute to the 'democratization' of surveillance" (Koskela 2006, 175). In addition, Koskela (2004, 204) argues that webcams have an empowering role and that the active role of individuals with surveillance equipment shows that the lines of control are blurred.

In conclusion, non-panoptic notions of Internet surveillance either use a neutral concept that assumes there are enabling effects such as protection and security as well as constraining effects such as control or a positive concept that identifies comical, playful, amusing, and even enjoyable characteristics of surveillance and where everyone has the opportunity to surveil. In addition, these approaches tend to reject the proposition that surveillance mechanisms are dominated by political and economic actors and see monitoring not necessarily as annoying and disturbing. In non-panoptic notions, Internet surveillance is understood as a useful and effective management tool and as fair methods and procedures of monitoring individuals online. Now, we move on to panoptic notions of Internet surveillance.

2.3.   Panoptic Notions of Internet Surveillance

Based on a diagrammatic understanding of panoptic surveillance, Greg Elmer (1997) predominantly understands the Internet as a powerful space of economic surveillance. "The Internet is first mapped, through indexical search engines, and then diagnosed, via 'spiders' and 'cookies', to actively monitor, survey, solicit and subsequently profile users' online behavior" (Elmer 1997, 182). Corporations map consumer profiles including demographic and psychographic data in order to target advertising and to accumulate profit (Elmer 1997, 186; 189-190).

Likewise, in The Internet Galaxy, Manuel Castells (2001, 168-187) describes the Internet not only as a space full of opportunities, but also as a technology of control, which has primarily emerged from the interests of economic and political actors such as corporations and state institutions. He argues that these institutions make use of such technologies in order to locate individual users. State institutions such as governments and corporations like Microsoft and Google use special surveillance technologies that allow the monitoring of online behaviour in one central database.

Surveillance technologies ... often rely on identification technologies to be able to locate the individual user ... These technologies operate their controls under two basic conditions. First, the controllers know the codes of the network, the controlled do not. Software is confidential, and proprietary, and cannot be modified except by its owner. Once on the network, the average user is the prisoner of an architecture he or she does not know. Secondly, controls are exercised on the basis of a space de-

fined on the network, for instance, the network around an Internet service provider, or the intra-network in a company, a university, or a government agency. (Castells 2001, 171-173)

Castells understands the rise of the Internet as an emergence of a powerful electronic surveillance system and concludes: "If this system of surveillance and control of the Internet develops fully, we will not be able to do as we please. We may have no liberty, and no place to hide" (Castells 2001, 181). Castells (2001, 171-173) considers, just like Foucault, surveillance to be negative and centralized and being connected to control and power. Hence, although Castells does not refer to the concept of the panopticon directly, his contribution to online surveillance can be considered as being a panoptic notion of Internet surveillance.

Michael Levi and David Wall (2004, 201-203) emphasize the new politics of surveillance in a post 9/11 European information society and the increase of the panoptic power of the EU member states mediated through surveillance techniques such as identity/entitlement cards, asylum seekers' smartcards, data sharing schemes, and smart passports in order to create a suspect population. Wall (2003; 2006) analyzes the growth of surveillant Internet technologies in the information society. He draws on Foucault's understanding of panoptic power relations (Wall 2006, 344) and distinguishes between personal and mass surveillance (Wall 2006, 342). For Wall, the Internet as a multidirectional information flow has brought new opportunities for individuals in the context of surveillance. Techniques such as spyware, spam spider bots, and cookies allow a synoptic effect where the surveilled can surveil the surveillers (Wall 2006, 342-343).

The Internet is not simply a 'super' (Poster, 1995), 'virtual' (Engberg, 1996) or 'electronic' (Lyon, 1994, ch. 4) Panopticon: an extension of Foucault's conceptualization of Bentham's prison design – 'seeing without being seen' (Foucault, 1983, p. 223), as has become the conventional wisdom. It is important to emphasize that Internet information flows are simultaneously panoptic and synoptic – not only can the few watch the many, but the many can watch the few (Mathiesen, 1997, p. 215) (Wall 2003, 112).

Wall argues that the balance between personal surveillance on the one hand and mass surveillance on the other hand is "rarely even" (Wall 2006, 346) and lists powerful corporations such as DoubleClick and Engage that are able to undertake large-scale surveillance (Wall 2006, 343). In addition, he emphasizes the growth of surveillance and privacy threats as tradeable commodities in information capitalism (Wall 2003, 135) and presents an empirical case study of the spam industry such as e-mail list compilation and unsolicited bulk e-mails (Wall 2006, 350-352).

Joseph Turow (2005; 2006) speaks about marketing and consumer surveillance in the digital age of media. He stresses that online media are interested in collecting data about their audience in order to sell these data to advertisers. In a next step, the advertisers use these data in order to increase the efficiency of marketing (Turow 2005,

103-104; 2006, 280). Furthermore, customer relationship management constructs audiences and produces a surveillance-driven culture, where consumers understand surveillance as a cost-benefit calculation and willing to the data collection of media and advertisers (Turow 2005, 105, 119-120). Turow's understanding of surveillance can be seen in the context of Foucault's notion of panoptic surveillance. He considers, just like Foucault, surveillance to be negative and centralized and being connected to discipline, control, and power (Turow 2005, 115). Similarly to Foucault, Turow (2005, 116-117) stresses that surveillance is predominately undertaken by powerful institutions such as corporations. Also interesting in this context is the national survey of Internet privacy and institutional trust by Joseph Turow and Michael Hennessy (2007). In 2003, they undertook 1200 quantitative telephone interviews in the United States with adults (18 years and older), who go online at home (Turow and Hennessy 2007, 304). The authors tried to analyze what US citizens think about institutional surveillance and conclude "that a substantial percentage of Internet users believes that major corporate or government institutions will both help them to protect information privacy and take that privacy away by disclosing information to other parties without permission" (Turow and Hennessy 2007, 301).

Mark Andrejevic (2002; 2007b; also 2007a 135-160) wants to offer an alternative approach of online privacy in the era of new media. Andrejevic studies the economic surveillance of interactive media such as interactive TV (2002) and Google's business model of free wireless Internet access (2007b) and analyzes interactive surveillance in the digital enclosure: "the model of enclosure traces the relationship between a material, spatial process – the construction of networked, interactive environments – and the private expropriation of information" (Andrejevic 2007b, 297). The author argues that Foucault's approach of the panopticon is suitable in order to study surveillance and hierarchical power asymmetries in the online economy and speaks about a "digital form of disciplinary panopticism" (Andrejevic 2007b, 237). Andrejevic argues that just like workplace surveillance rationalized production in the era of scientific management, online surveillance rationalizes and stimulates consumption (Andrejevic 2007b, 232; 244), produces customized commodities and the crucial capital of the economy (Andrejevic 2007b, 234). "Viewers are monitored so advertisers can be ensured that this work is being done as efficiently as possible. Ratings, in this context, are informational commodities that generate value because they help to rationalize the viewing process" (Andrejevic 2007b, 236).

Also in the context of economic surveillance, John Edward Campbell and Matt Carlson (2002) revisit Foucault's idea of the panopticon as well as Gandy's notion of the panoptic sort. They apply these notions to online surveillance and the commodification of privacy on the Internet:

The Panopticon was seen as a way of organizing social institutions to ensure a more orderly society by producing disciplined and 'rational' (read predictable) citizens. With Internet ad servers, the goal is to provide marketers with the personal

information necessary to determine if an individual constitutes an economically vi-
able consumer. The enhanced consumer profiling offered by these third-party ad
servers increases the effectiveness and efficiency of advertisers' efforts, reducing the
uncertainty faced by producers introducing their goods and services into the mar-
ketplace (Campbell and Carlson 2002, 587).

Summing up, panoptic notions of Internet surveillance argue that power, control, and surveillance have increased in the era of the Internet. Furthermore, the rise of the Internet has brought a space of electronic surveillance, where the powerful will appropriate the Internet as a technology of control for their own instrumental advantage. These approaches consider online surveillance to be negative and being connected to coercion, repression, discipline, power, and domination. For these authors, power is primarily centralized and society tends to be repressive and controlled.

2.4. Discussion

The overall aim of this section was to clarify how Internet surveillance has been defined in the existing literature, what the different notions of online surveillance have in common, and what distinguishes them from one another. Based on the distinction of panoptic and non-panoptic notions of surveillance, a systematic discussion of the state of the art of Internet surveillance by establishing a typology of the existing literature and a discussion of commonalties and differences were introduced. The following table summarizes the results:

Foundations of Internet surveillance studies			
		Non-panoptic notions of Internet surveillance	Panoptic notions of Internet surveillance
Non-panoptic notions of Internet surveillance	Non-panoptic notions of Internet surveillance either use a neutral concept that assumes there are enabling as well as constraining effects or a positive concept that identifies comical, playful, amusing, and even enjoyable characteristics of online surveillance.	David Lyon (1998; 2003a; 2003b), Seumas Miller and John Weckert (2000), Anders Albrechtslund (2008), Hille Koskela (2004; 2006)	
Panoptic notions of Internet surveillance	Panoptic notions of Internet surveillance consider online surveillance to be negative. These approaches argue that power, domination, coercion, control, discipline, and surveillance have increased in the era of the Internet.		Greg Elmer (1997), Manuel Castells (2001), David Wall (2003; 2006), Joseph Turow (2005; 2006), Mark Andrejevic (2002; 2007a; 2007b), John Edward Campbell and Matt Carlson (2002)

Table 1: Foundations of Internet surveillance studies

In conclusion, non-panoptic notions of Internet surveillance use either a neutral concept that assumes there are enabling as well as constraining effects or a positive concept that identifies comical, playful, amusing, and even enjoyable characteristics; they are represented by scholars such as David Lyon and Hille Koskela. In contrast, panoptic notions of Internet surveillance consider online surveillance to be negative. These approaches argue that power, domination, coercion, control, discipline, and surveillance have increased in the era of the Internet; they are represented by scholars such as Greg Elmer, Manuel Castells, and Joseph Turow.

Although private actors monitor and watch over other individuals in everyday life experiences (for example parents taking care of their children, providing personal information on weblogs, and using social networking sites on the Internet), these acts are processes to which people agree and which involve no violence, coercion, or repression. In comparison, economical and political actors use surveillance and exercise violence in order to control certain behaviour of people and in most cases people do not know that they are surveilled. Corporations control the economic behaviour of people and coerce individuals in order to produce or buy specific commodities for accumulating profit and for guaranteeing the production of surplus value. Corporations and state institutions are the most powerful actors in society and are able to undertake mass-surveillance extensively and intensively (such as for example the collection and gathering of information on Internet user profiles in order to implement targeted advertising), because the amount of available resources shapes the intensity and extension of surveillance. In the modern production process, primarily electronic surveillance is used to document and control workers' behaviour and communication for guaranteeing the production of surplus value. The commodification of privacy is important to target advertising for accumulating profit. State institutions have intensified and extended state surveillance of citizens in order to combat the threat of terrorism (see: Gandy 2003; Lyon 2003c) Therefore, one can assume that corporations and state institutions are the main actors in modern surveillance societies and surveillance is a crucial element for modern societies.

Non-panoptic notions of Internet surveillance understand surveillance in cyberspace in a non-hierarchical and decentralized way, where everyone has the opportunity to surveil. This argument overlooks the fact that corporations and state institutions are the most powerful actors in society and are able to undertake mass-surveillance online, what private actors are not able to do. Neutral concepts of surveillance on the Internet tend to overlook power asymmetries of contemporary society and therefore tend to convey the image that private actors are equally powerful as corporations and state institutions. Hence, a general and neutral understanding of surveillance in cyberspace is not fruitful for studying online surveillance as it does not take asymmetrical power relations and repressive aspects of society into consideration. Approaches that stress that everyone today has the opportunity to surveil, that online surveillance is a useful and effective management tool, and that Internet surveillance has playful, amusing, and even enjoyable characteristics are typical for

postmodern scholars and disguise the fact of power and domination in contemporary surveillance societies.

Surveillance studies scholars like Lyon (1998, 95; 2003b, 163) argue that economic surveillance on the Internet such as monitoring consumers or the workplace are central aspects of modern surveillance societies. The following explanations indicate that most of the panoptic notions of Internet surveillance recognize the importance of economic aspects of surveillance in cyberspace: So for example Elmer (1997, 186; 189-190) investigates economic Internet surveillance predominantly in the sphere of consumption and analyzes how corporations map consumer profiles in order to target advertising and to accumulate profit. In contrast, Castells (2001, 173-174) mentions economic Internet surveillance in the sphere of production and in the sphere of consumption. When Wall (2006, 350-352) presents an empirical case study of the spam industry such as e-mail list compilation and unsolicited bulk e-mails, he solely emphasizes surveillance in the sphere of consumption. Turow (2006, 114-118) analyzes consumer surveillance in the digital age and marks a development from customized media of one-to-one marketing to walled gardens as an online environment to interactive television such as video-on-demand. Andrejevic (2007b, 242-243) is primarily interested in analyzing consumer surveillance. In addition, Campbell and Carlson (2002, 587) understand online surveillance in the context of the commodification of privacy, consumer profiling, and advertising. In conclusion, panoptic notions of Internet surveillance primarily analyze economic aspects of surveillance on the Internet in the context of consumption. The following table summarizes these example approaches:

Economic aspects in panoptic notions of Internet surveillance		
Internet surveillance in the sphere of production	Internet surveillance in the sphere of circulation	Internet surveillance in the sphere of consumption
Manuel Castells (2001)		Greg Elmer (1997)
		Manuel Castells (2001)
		David Wall (2003; 2006)
		Joseph Turow (2005; 2006)
		Mark Andrejevic (2002; 2007a; 2007b)
		John Edward Campbell and Matt Carlson (2002)

Table 2: Economic aspects in panoptic notions of Internet surveillance

Athough panoptic notions of Internet surveillance recognize the importance of the economy, they tend to focus on the sphere of consumption and to overlook online

surveillance in the spheres of production and circulation as important aspects of contemporary surveillance societies. Furthermore, panoptic notions of Internet surveillance claim that there are particular forms of economic surveillance without a theoretical criterion for a certain typology. In contrast, a typology of Internet surveillance in the modern economy, which is based on Marx' theory and critique of the political economy, allows to systemize economic surveillance on the Internet and to distinguish between online surveillance in the spheres of production, circulation, and consumption. A theoretically founded typology of economic Internet surveillance is important in order to undertake a theoretical analysis of online surveillance in the modern economy. Therefore, in the next section, a distinction of Internet surveillance in the economy into the spheres of production, circulation, and consumption will be outlined.

3. Critical Internet Surveillance Studies

The overall aim of this section is to analyze the specific economic mode of Internet surveillance. Based on the foundations of a political economy approach, the distinction of production, circulation, and consumption within the economy is introduced (subsection one) in order to establish a typology of online surveillance in the economy and to study Internet surveillance in the spheres of production, circulation, and consumption (subsection two).

3.1.   The Spheres of the Economy

In the Introduction to a Contribution to the Critique of Political Economy, Karl Marx (MECW 28, 26-37) distinguishes between (a) production, (b) circulation (distribution and exchange), and (c) consumption as dialectically mediated spheres of the capitalistic economy (a). The sphere of production appears as the point of departure. In the capitalist mode of production, entrepreneurs consume purchased commodities (means of production and labour power) in order to produce new commodities and surplus value. (b) Circulation is the "mediation between production and consumption" (MECW 28, 27). In the process of circulation, consumers purchase commodities for daily life and proprietors sell the produced commodities to realize profit. (c) In the sphere of consumption as the final point of the process, "the product drops out of this social movement, becomes the direct object and servant of an individual need, which its use satisfies" (MECW 28, 26). While in production the person receives an objective aspect, in consumption the object receives a subjective aspect. The "consumption, as the concluding act, … reacts on the point of departure thus once again initiating the whole process" (MECW 28, 27). Although production, circulation, and consumption are separated spheres, they correlate in an interconnected relationship (see figure 1):
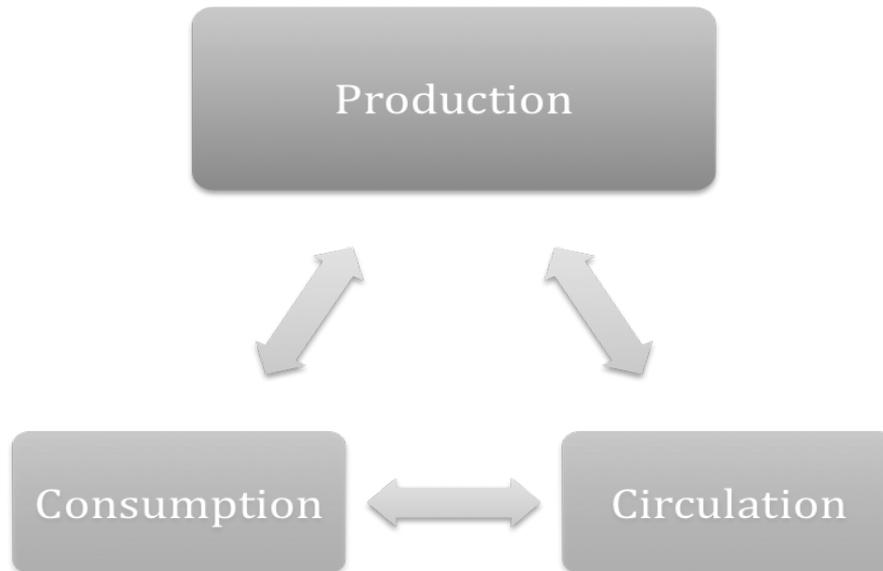
Figure 1: Production, circulation, and consumption as dialectically mediated spheres of the modern economy

In the sphere of production, means of production are consumed and in the sphere of consumption, labour power is (re)produced. "Production is consumption; consumption is production. Consumptive production. Productive consumption" (MECW 28, 30). Production is not possible without demand and consumption does not take place without material. "No consumption without production; no production without consumption" (MECW 28, 30). Moreover, the process of production is determined by circulation of labour power as well as means of production, whereas circulation itself is a product of production. Production, circulation, and consumption are not "identical, but that they are all elements of a totality, differences within a unity … There is an interaction between the different moments" (MECW 28, 36-37). Nevertheless, production, circulation, and consumption are not equal spheres in the economy; production is rather "the dominant moment, both with regard to itself in the contradictory determination of production and with regard to the other moments. The process always starts afresh with production … A definite [mode of; TA] production thus determines a definite [mode of; TA] consumption, distribution, exchange and definite relations of these different moments to one another. Production in its one-sided form, however, is in its turn also determined by the other moments" (MECW 28, 36).

Based on the distinction of production, circulation, and consumption, a typology of surveillance in the economy can be constructed. Such a typology will be outlined in the next subsection.

3.2. Internet Surveillance in the Spheres of the Economy

Illustrative examples of economic online surveillance in the spheres of production, circulation, and consumption will be presented. The following three parts are therefore structured according to this distinction.

3.2.1. Internet Surveillance in the Sphere of Production

The Electronic Monitoring and Surveillance Survey (American Management Association and the ePolicy Institute 2008) offers interesting examples of Internet surveillance in the sphere of production: according to the American Management Association and the ePolicy Institute (2008) that undertake an annual quantitative survey about electronic monitoring and surveillance with approximately 300 US companies, "more than one fourth of employers have fired workers for misusing e-mail and nearly one third have fired employees for misusing the Internet". More than 40% of the studied companies monitor e-mail traffic of their workers, and 66% of the corporations monitor Internet connections. In addition, most companies use software to block non-work related websites such as sexual or pornographic sites, game sites, social networking sites, entertainment sites, shopping sites, and sport sites. The American Management Association and the ePolicy Institute (2008) also stress that companies track "content, keystrokes, and time spent at the keyboard … store and review computer files … monitor the blogosphere to see what is being written about the company, and … monitor social networking sites". Furthermore, about 30% of the companies were also firing employees for non-work related email and Internet usage such as "inappropriate or offensive language" and "viewing, downloading, or uploading inappropriate/offensive content" (American Management Association and the ePolicy Institute 2008).

3.2.2. Internet Surveillance in the Sphere of Circulation

An interesting phenomenon of surveillance in the sphere of circulation is applicant surveillance: Rosalind Searle (2006, 343) states in this context that "checking procedures are increasingly utilised to authenticate candidates' data. In several countries financial services authorities have sanctioned formal vetting, often outsourcing it to external contractors … such as Kroll and Carratu International". The corporate investigation company Carratu International is headquartered in London. The company operates around the world with national and multi-national corporations, insurance companies, law firms, and financial institutions, which are primarily found in the Fortune 500 and the Financial Times Top 100 rankings (Carratu International). Carratu International argues that pre-employment screening is crucial, because up to 80% of new job candidates give incorrect information about themselves (see brochure of employee screening services in figure 2).

Do you really know who you employ?

How do you know that the information provided is complete and honest?

CV fraud is a serious and growing problem. Details provided by a potential employee on their application form are a mixture of facts and representations. The facts, such as sex and height are difficult to alter. Almost everything else can be overstated, falsified or omitted. Personal history can be falsified, qualifications fabricated, identities assumed and references faked. Research has shown that up to eighty percent of applicants provided false or misleading information or omitted important facts about themselves. Whilst some falsehoods put on applications may be treated as innocuous, the consequences of employing someone who has not been honest can be disastrous.

Regular surveys have shown that most employee frauds are carried out by individuals who - if screened at the time of their original application - would not have been employed because of the discrepancies uncovered. By screening applicants, organisations greatly reduce the risk of financial loss, fraudulent use of material or information, the misuse of staff time and harm to their reputation. Organisations need to ensure that the people they employ are really who they say they are and have the experience and qualifications that made them want to employ them in the first place.

The need for efficient employee screening does not end with protection from dishonesty or harm to reputation.

Many companies and financial institutions are required by regulation to ensure that the people they employ are suitable for the role they are given. For example the Financial Services Authority requires regulated firms to ensure that their regulated staff are "fit and proper persons" for the role they perform. British Standard 7858 gives recommendations for the security screening of people to be employed in a security environment.

The only reliable way to ensure that representations are real facts is to validate them utilising an objective third party who has not been involved in the recruitment and interview process.

The types of information which should be checked include:

- Personal Data: to confirm that the applicant is who he/she says they are
- Judicial/Legal Data: civil litigation, credit history, bankruptcy and the like
- Employment History: this is particularly important as previous employers are usually only willing to supply the barest of references
- Credentials: educational achievements, professional qualifications, professional or occupational licensing.

We have seen instances where:

- An applicant who used a fraudulently altered copy of his son's birth certificate
- An applicant who had severe current financial problems including numerous County Court judgements
- An applicant who had omitted his time in prison from his application for a senior management role
- An applicant who had various well publicised convictions and lengthy jail sentences for financial fraud

But possibly more importantly we have investigated thousands of cases where there was no employee vetting system present and staff have gone on to steal large amounts of cash, commit fraud or steal proprietary information.

We are able to provide a discreet, cost efficient employee validation service tailored to both your objectives and timescales. Each of our clients has a different focus when vetting their staff and we provide precisely tailored solutions to meet these objectives. However, in general our validations are at three levels, each with a fixed price.

Level One

Our basic service includes:

- Confirmation of address and other contact details
- Credit referencing and history including a bankruptcy search
- Confirmation of employment history and references
- Validation of relevant educational qualifications and membership of professional bodies

Level Two

Our intermediate service includes:

- Confirmation of address and other contact details
- Credit referencing and history including a bankruptcy search
- Confirmation of employment history and references
- Validation of relevant educational qualifications and membership of professional bodies
- Property ownership search
- Search of judicial and legal data
- Company directorship search
- Full media/database search

Level Three

At this level we are normally dealing with appointments to senior management grade and/or to a very sensitive position/business area. We aim to validate all details contained on the application document, carry out all checks as detailed in Level Two validations, together with additional relevant research and investigations to confirm the probity and standing of the applicant.

In addition we have the experience and resources to administer both high level vetting of board level appointments and the validation of large volumes of applicants. We are also pleased to assist you with advice on recruitment procedures and the information which needs to be collected on application forms.

Fig. 2. Carratu International brochure of employee screening services (Carratu International)

According to Carratu International, the only opportunity to "know that the information provided is complete and honest" is to undertake a systematic off- and online check of information such as personal data and information on civil litigation, credit history, bankruptcy, employment history, educational achievements, professional qualifications, and professional or occupational licensing. In addition, Carratu International provides three levels of off- and online pre-employment screening at different prices: the basic service includes data analyzes of items such as address, educational qualification, and employment history. The intermediate service includes the basic service plus searches of the media, ownership records, company directorship and judicial data. Finally, the professional level includes an investigation of "all details contained on the application document, carry[ing; TA] out all checks as detailed in Level Two validations, together with additional relevant research and investigations to confirm the probity and standing of the applicant" (Carratu International).

3.2.3. Internet Surveillance in the Sphere of Consumption

For Internet surveillance in the sphere of consumption, the example of Google and DoubleClick can be outlined: According to the top sites of the web by Alexa Internet, Google has the most visits on the Internet. Google uses a wide range of methods in order to collect data on its users, namely click tracking (to log clicks of users), log files (to store server requests), JavaScript and web bugs (to check users visits), as well as cookies (to record individual actions) (Stalder and Mayer 2009, 102). DoubleClick is one of the main projects of Google (Google 2008).It is a global leader in ad serving and has developed sophisticated methods in order to collect, analyze, and assess huge amounts of users' data on the Internet (Campbell and Carlson 2002, 596-597). Google (2007; 2008) acquired DoubleClick in 2008 for US$ 3.1 billion. DoubleClick is headquartered in New York City. It was found in 1996 and works for leading digital publishers, marketers, and agencies around the world such as About, Durex, Ford, Friendster, Optimedia, Scripps, and MTV (DoubleClick). Ad serving companies such as DoubleClick use methods by placing advertisements on websites and analyzing their efficiency. DoubleClick develops and provides Internet ad serving services that are sold primarily to advertisers and publishers. DoubleClick collects personal data on many websites, sells this data, and supports targeted advertising. DoubleClick's main product is known as DART (Dynamic Advertising, Reporting, and Targeting). DART is an ad serving programme working with a complex algorithm and is primarily developed for publishers and advertisers in order to "ensure you get the right message, to the right person, at the right time, on the right device" (DoubleClick).

In this section, Internet surveillance in the context of the economy was analyzed. Based on the foundations of a critical political economy approach, the distinction of production, circulation, and consumption in the economy was introduced in order to establish a typology of Internet surveillance in the economy. Illustrative examples of economic online surveillance in the spheres of production, circulation, and consumption were presented.

4. Conclusion

The overall aim of Critical Internet Surveillance Studies and Economic Surveillance was to clarify how we can theorize and systemize Internet surveillance in the modern economy. The chapter constructed theoretically founded typologies in order to systemize the existing literature of Internet surveillance studies and to analyze examples of surveillance. Therefore, it mainly was a theoretical approach combined with illustrative examples, advanced from the abstract to the concrete level.

Foundations of Internet surveillance studies were discussed in the second section. In the third section, a critical contribution to Internet surveillance studies was drawn in order to distinguish Internet surveillance into the spheres of production, circulation, and consumption. Based on these findings, we were able to systemize illustrative examples of Internet surveillance in the modern economy such as the Electronic Monitoring and Surveillance Survey, Carratu International, and DoubleClick into the spheres of production, circulation, and consumption.

As shown in this chapter, economical actors such as corporations undertake surveillance and exercise violence in order to control a certain behaviour of people and in most cases people do not know that they are surveilled. Corporations control the economic behaviour of people and coerce individuals in order to produce or buy specific commodities for guaranteeing the production of surplus value and for accumulating profit. Therefore, one can assume that Internet surveillance is a negative phenomenon of modern societies, which should be questioned and struggled against. Based on Gandy (1993, 230-231), Castells (2001, 182-184), Parenti (2003, 207-212), Ogura (2006, 291-293), Lyon (1994, 159-225; 2001, 126-140; 2007a, 159-178; 2007b, 368-377), and Fuchs (2009, 115-117), some political recommendations can be drawn in order to overcome economic online surveillance:

- The first recommendations is that support is needed for critical privacy movements on the Internet in order to develop counter-hegemonic power and advance critical awareness of surveillance.
- "Such public awareness of surveillance issues could further be raised through professional groups and organizations, especially those directly concerned with computing, information management, and so on." (Lyon 1994, 223)
- Furthermore, Lyon (2001, 127) states the importance of political activism by critical citizens: "Films, consumer groups, Internet campaigns and international watchdogs are just some of the ways that ongoing surveillance practices are brought to the surface of our consciousness, and thus overtly into the realm of ethical evaluation and political response."
- According to Fuchs (2009, 116), "critical citizens, critical citizens' initiatives, consumer groups, social movement groups, critical scholars, unions, data protection specialists/groups, consumer protection specialists/groups, critical politicians, critical political parties observe closely the relationship of surveillance and corporations and document instances where corporations and politicians take measures that threaten privacy or increase the surveillance of citizens".

- In addition, it is recommended to support cyberactivism and "counter-surveillance" (Lyon 1994, 159) in order to surveil corporate surveillants or rather to watch the watchers.
- Parenti (2003, 212) suggests civil disobedience, rebellion, and protest: "It will compel regulators to tell corporations, police, schools, hospitals, and other institutions that there are limits. As a society, we want to say: Here you may not go. Here you may not record. Here you may not track and identify people. Here you may not trade and analyze information and build dossiers".
- A further recommendation is to create non-profit, non-commercial social networking platforms on the Internet such as Kaioo. Kaioo is owned by the non-profit organization OpenNetworX, has been available since 2007, and has currently about 30.000 users. Kaioo's privacy terms are created in common and can be edited online by every user. In addition, the data belong to their users (Kaioo). OpenNetworX can do so, because they are not interested in targeting advertising and they do not need to produce surplus value and to accumulate profit.
- "To try to advance critical awareness and to surveil corporate and political surveillers are important political moves for guaranteeing civil rights, but they will ultimately fail if they do not recognize that electronic surveillance is not a technological issue that can be solved by technological means or by different individual behaviours, but only by bringing about changes of society" (Fuchs 2009, 116). Therefore, Internet surveillance has to be put into the larger context of societal problems in public discourse. "We should look at the whole macro picture." (Ogura 2006, 292)
- Finally, Internet surveillance is caused by economical and political issues and is inherent in modern society. It is neither just a technical issue, nor an individual problem, but a societal problem. Internet surveillance is a crucial phenomena, but there are a lot of other features in contemporary society such as information, neoliberalism, globalization, and capital.

References

Albrechtslund, Anders. 2008. Online *social networking as participatory surveillance* [cited 07.09.2010]. Available from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949.

Alexa, Internet. [cited 07.09.2010]. Available from http://www.alexa.com.

American Management Association, and The ePolicy Institute. 2008. *Electronic monitoring and surveillance 2007 survey* [cited 07.09.2010]. Available from http://www.amanet.org/training/seminars/2007-Electronic-Monitoring-and-Surveillance-Survey-41.aspx.

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: Rowman & Littlefield Publishers.

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

———. 2007b. Surveillance in the digital enclosure. *The Communication Review 10 (4)*: 295-317.

Campbell, John Edward, and Matt Carlson. 2002. Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media 46 (4)*: 586-606.

Carratu, International. [cited 07.09.2010]. Available from http://www.carratu.com/.

Castells, Manuel. 2001. *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford: Oxford University Press.

DoubleClick. [cited 07.09.2010]. Available from http://www.doubleclick.com.

Elmer, Greg. 1997. Spaces of surveillance: Indexicality and solicitation on the Internet. *Critical Studies in Mass Communication 14 (2)*: 182-191.

Foucault, Michel. 1995. *Discipline and punish: The birth of the prison*. New York: Vintage Books.

———. 2002. The eye of power: A conversation with Jean-Pierre Barou and Michelle Perrot. In *CTRL [Space] Rhetorics of surveillance from Bentham to Big Brother*, ed. Thomas Y. Levin, Ursula Frohne and Peter Weibel, 94-101. Karlsruhe: ZKM Center for Arts and Media.

———. 2003. *"Society must be defended": Lectures at the Collège De France, 1975-1976*. New York: Picador.

———. 2007. *Security, territory, population: Lectures at the Collège De France, 1977-1978*. New York: Palgrave Macmillan.

Fuchs, Christian. 2009. *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: Research Group Unified Theory of Information.

Gandy, Oscar. 1993. *The panoptic sort: A political economy of personal information*. Boulder: Westview Press.

———. 2003. Data mining and surveillance in the post-9/11 environment. In *The intensification of surveillance: Crime, terrorism and warfare in the information era*, ed. by Kirstie Ball and Frank Webster, 26-41. London: Pluto Press.

Google. 2007. *Press center: Google to acquire Doubleclick: Combination will significantly expand opportunities for advertisers, agencies and publishers and improve users' online experience* [cited 07.09.2010]. Available from http://www.google.com/intl/en/press/pressrel/doubleclick.html.

———. 2008. *Press center: Google closes acquisition of Doubleclick* [cited 07.09.2010]. Available from http://www.google.com/intl/en/press/pressrel/20080311 doubleclick.html.

Gutting, Gary. 1998. Foucault, Michel (1926-84). In *Routledge encyclopedia of philosophy. Volume 4*, ed. Edward Craig and Luciano Floridi, 708-713. London: Routledge.

Kaioo. About Kaioo [cited 07.09.2010]. Available from http://kaioo.com/toro/resource/html?locale=en#wiki.9.

Koskela, Hille. 2004. webcams, TV shows and mobile phones: Empowering exhibitionism. *Surveillance & Society 2 (2/3)*: 199-215.

———. 2006. 'The other side of surveillance': webcams, power and agency. In *Theorizing surveillance: The panopticon and beyond*, ed. Dadvid Lyon, 163-181. Cullompton: Willian Publishing.

Levi, Michael, and David Wall. 2004. Technologies, security, and privacy in the Post-9/11 European information society. *Journal of Law and Society 31 (2)*: 194-220.

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

———. 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: Issues in society*. Maidenhead: Open University Press.

———. 2003a. Cyberspace, surveillance, and social control: The hidden face of the Internet in Asia. In *Asia.Com: Asia encounters the Internet*, ed. K. C. Ho, Randy Kluver and Kenneth C. Yang, 67-82. London: Routledge.

———. 2003b. Surveillance technology and surveillance society. In *Modernity and technology*, ed. Thomas J. Misa, Phlip Brey and Andrew Feenberg, 161-184. Cambridge: MIT Press.

———. 2003c. *Surveillance after September 11.* Cambridge: Polity Press.

———. 2007a. *Surveillance studies: An overview*. Cambridge: Polity Press.

———. 2007b. Resisting surveillance. In *The surveillance studies reader*, ed. Sean Hier and Joshua Greenberg, 368-377. Maidenhead: Open University Press.

Marx, Karl, and Friedrich Engels (MECW 28). 1986. *Collected works: Volume 28*. New York: International Publishers.

Miller, Seumas, and John Weckert. 2000. Privacy, the workplace and the Internet. *Journal of Business Ethics 28 (3)*: 255-265.

Murakami Wood, David. 2009. Situating surveillance studies. Surveillance *& Society 6 (1)*: 52-61.

Norris, Clive, and Gary Armstrong. 1999. *The maximum surveillance society: The rise of CCTV*. Oxford: Berg.

Ogura, Toshimaru. 2006. Electronic government and surveillance-oriented society. In *Theorizing surveillance. The panopticon and behind*, ed. David Lyon, 270-295. Portland: Willan Publishing.

Parenti, Christian. 2003. *The soft cage: Surveillance in America: From slavery to the war on terror*. New York: Basic Books.

Pryor, Benjamin. 2006. Foucault, Michel (1926-1984). In *Encyclopedia of philosophy. Volume 3*, edited by Donald M. Borchert, 698-702. Detroit: Thomson Gale.

Searle, Rosalind. 2006. New technology: The potential impact of surveillance techniques in recruitment practices. *Personal Review 35 (3)*: 336-351.

Soanes, Catherine, and Angus Stevenson. 2005. Surveillance. *The Oxford dictionary of English* [cited 07.09.2010]. Available from http://www.oxfordreference.com/pub/views/home.html.

Stalder, Felix, and Christine Mayer. 2009. The second index: Search engines, personalization and surveillance. In *Deep search: The politics of search beyond Google*, ed. Konrad Becker and Felix Stalder, 98-116. Wien: Studienverlag.

Turow, Joseph. 2005. Audience construction and culture production: Marketing surveillance in the digital age. *The ANNALS of the American Academy of Political and Social Science 597 (1)*: 103-121.

———. 2006. Cracking the consumer code: Advertising, anxiety and surveillance in the digital age. In *The new politics of surveillance and visibility*, ed. Kevin Hagerty and Richard V. Ericson, 279-307. Toronto: University of Toronto Press.

Turow, Joseph, and Michael Hennessy. 2007. Internet privacy and institutional trust: Insights from a national survey. *New Media Society 9 (2)*: 300-318.

Wall, David. 2003. Mapping out cybercrimes in a cyberspatial surveillant assemblage. In *The intensification of surveillance: Crime terrorism and warfare in the information age*, ed. Kirstie Ball and Frank Webster, 112-136. London: Pluto Press.

———. 2006. Surveillant Internet technologies and the growth in information capitalism: Spams and public trust in the information society. In *The new politics of surveillance and visibility*, ed. Kevin Haggerty and Richard V. Ericson, 340-362. Toronto: University of Toronto Press.