Introduction to Cyber-Surveillance

Colin J. Bennett, Andrew Clement & Kate Milberry

2012

Surveillance & Society

Editorial | Introduction to Cyber-Surveillance

Colin J. Bennett

Political Science, University of Victoria, Canada. cjb@uvic.ca

Andrew Clement

Faculty of Information Studies, University of Toronto, Canada. andrew.clement@utoronto.ca

Kate Milberry

Faculty of Extension, University of Alberta, Canada. kate.milberry@gmail.com

The rapid expansion of digital networking and especially the Internet over the past two decades has been a boon for the many informationally intensive activities that facilitate and increasingly constitute contemporary social, economic, political and cultural life. Access to information and the means to produce information have grown dramatically, enabling both individual empowerment and democratic participation. Digital mediation is transforming the design, production, marketing, distribution and consumption of a widening array of goods and services. The Internet provides a platform for active involvement in campaigns, groups, movements and political activism, allows individuals to disseminate the fruits of their creation to the world at virtually no cost, and enables the instantaneous search of volumes of data.

The corollary, of course, is that it is now much easier for individuals and organizations to capture, process, and disseminate information about individuals. A wide variety of entities can now observe, track and record online behaviour, as well as a host of other everyday activities, by monitoring digital networks, by tapping into the vast quantity of data collected about personal transactions, or by installing spyware directly on individual computers. For as long as individuals have been going online to communicate, shop, apply for services, and network, those concerned with information and communication rights have expressed anxieties about the capture and processing of personal information, and how this may be used to affect people's life chances. The Internet is unquestionably a surveillance medium *par excellence*.

The Origins and Properties of Cyber-Surveillance

We can begin to gain a sense of the salient characteristics of cyber-surveillance by attending to some of the general and widely observed features of digital networking. It is no coincidence that surveillance and computerization are so closely associated, because they have common roots in the post-WWII linked developments in cybernetics and digital computation. We can see this most notably in the work of MIT

Bennett, Colin J., Clement, Andrew, and Milberry, Kate. 2012. Editorial: Introduction to Cyber-Surveillance. *Surveillance & Society* 9(4): 339-347.
http://www.surveillance-and-society.org | ISSN: 1477-7487

mathematician Norbert Weiner who originated cybernetics and made fundamental contributions to the theories of feedback and control systems, which now underpin all applications of computing technology including surveillance practices (Weiner 1948). The subsequent revolution of digital media, which both reflected and reinforced surveillance approaches in pursuit of effective control of dynamic socio-technical phenomena, has several related general features that greatly amplify its surveillance potential. The key breakthrough of the (electronic) digital turn comes with the ability to represent all informational artefacts across the full spectrum of recording, transmitting, computing, and displaying activities using a single common universal form, a string of (binary) digits.

In combination with the revolution in electronic circuitry using silicon wafer substrates following, and further propelling, Moore's Law, digitalization has exploded exponentially in terms of processing speed, storage capacity, miniaturization, affordability, availability, portability, spatial reach, and scope of application. This has meant that digital mediation has been worked into many conventional activities of everyday life, and has opened up new spheres of activity only imagined previously. Digital systems, as a by-product of their functioning, produce a continuous stream of fine-grained digital information, readily available for further exploitation in the management of this process – "informating," according to Zuboff (1988). This provides the perfect environment for the expansion of surveillance practices, as long as there are parties willing and able to exploit them.

But potentiality is not actuality. It is easy to over-estimate the ubiquity and detail of digitally mediated surveillance practices based on these overall trends. Because your Internet service provider may have the capability of intercepting, recording, analyzing and reporting all of your Internet traffic does not mean it is actually (yet) doing so. As noted above, there are a host of specific technical factors that may make this infeasible. Furthermore, it depends on organizational and institutional considerations, notably whether it is in the financial interest of the business (see Mueller this issue) and whether it may incur risks from regulators or public opprobrium.

What is commonly referred to as the Internet consists of not one but a myriad of networked systems each managed independently, and largely without external control or oversight. Beyond the various technical standards-setting organizations, the Internet is bound by few rules and answers to no single organization. It is a system of networks that nobody completely understands, and can operate in surprising ways. That is its supposed strength, and its weakness – a radical decentralization fostering near costless and instantaneous dissemination of information.

The greatly expanded surveillance capabilities associated with digital networking are a matter of public controversy and concern, something that is demonstrated almost daily in media reports of the latest privacy scandal. Much of this controversy, of course, focuses on traditional, governmental forms of monitoring as they are extended into "cyberspace." As the Internet has become a mainstream communications medium, so law enforcement and intelligence agencies have tried to develop new surveillance capabilities and acquire new legal powers to monitor Internet communications. At one level, the debate surrounds high-profile and integrated surveillance systems, such as Echelon, Carnivore, and more recently the National Security Agency's (NSA) "warrantless wiretapping" program (Klein 2009; Bamford 2012). These capabilities have obviously been boosted as part of the government's "war on terrorism" since 9/11. What is also increasingly obvious is the extent to which corporations are implicated in these trends. Privacy International has launched a campaign called "Big Brother Incorporated" that "outs" the companies that have been responsible for selling surveillance technology for use by repressive regimes (https://www.privacyinternational.org/projects/big-brother-inc).

The capture, processing, and disclosure of personally related information online is not just about privacy. It is also fundamental to the very business models through which the Yahoos, Googles, and Facebooks of the world actually make money (Becker and Stalder 2009). Advertising is the lifeblood of the Internet

economy. To the extent that companies can discover more detailed and extensive information about personal preferences and behaviours, they will make more money. The very rules that comprise privacy law and policy potentially constrain that ability. Rules about notification, informed consent, access and correction of personal data and so on, are not just an important constraint on the ability of an organization to monitor consumers, they also have profound economic consequences. Privacy has, therefore, risen in importance as an economic issue, and scholars have had to get their minds around the technical complexities of online advertising and the business models upon which they are based.

In this environment, risks to personal privacy and other rights and liberties are more difficult to pin down, and invariably contingent on a number of technical questions relating to the means by which organizations may actually identify individuals and monitor their behaviours and preferences. Those questions require analysis at a complex technical level requiring an understanding of network architecture, software standards and protocols, the strength of encryption, the nature and content of log files, and so on. The ability to monitor is also related to the intended, and unintended, consequences of multiple organizational policies and individual choices. Any one transaction might involve a number of entities, no one of which has complete knowledge or control over the personal information captured and processed. And that is the central challenge to the study of cyber-surveillance—the perplexing number of actors, and the dynamic and multidimensional set of technical, political, and social issues.

Research Agendas

There is, however, a striking paucity of analysis of the actual processes of information capture and processing on the Internet within the very broad tradition of surveillance studies (Murakami Wood 2009). It is interesting to note that many recent books in this literature do not tend to see cyber-surveillance as a separate issue or concern, at least if judged by the crude measure of chapter headings and index references (e.g. Zureik and Salter 2005; Haggerty and Ericson 2006; Monahan 2006; Lyon 2007; Ball, Haggerty & Lyon 2012). One explanation is that most surveillance scholars tend not to possess sufficient levels of technological expertise. Surveillance capabilities are clearly contingent on the complexities of technical standards and protocols, the distinctions between the various forms of spyware, the nature of "cookie" technology, the uses of deep packet inspection by providers, the distinction between symmetric (private-key) and asymmetric (public-key) encryption and secure socket layers (SSL), and so on (Bennett and Parsons forthcoming). These technicalities are central to an understanding of the medium and its potential for surveillance. Any evaluation of the extent of cyber-surveillance as well as the attendant risks to individual and collective rights and interests is always dependent on answers to a number of highly complicated and technical questions.

Research has largely focused, therefore, on the facts of a given situation, rather than on whether the admitted practices are wrong or right. Much of the effort of outsiders is to demystify and render transparent an inherently inscrutable medium. Why are those third-party cookies logged? Do search engines really need to retain individual searches for such a long time? What is the real strength of the SSL encryption keys that protect our credit-card transactions? What does deep-packet inspection actually accomplish?

In this context, an understanding of the perspectives and attitudes of Internet users is crucial, not just out of scholarly interest but more importantly to determine the various levels of trust which are a necessary condition to realize the potential for electronic commerce, online service delivery and peer-to-peer communication. One major tradition of research on cyber-surveillance is, therefore, the public opinion or focus group analysis (e.g. Zureik *et al.* 2010; boyd 2010). People experience and make sense of surveillance practices, whether benign or harmful, effective or haphazard, in varied and contingent ways. How do encounters with surveillance practices, either being observed or being influenced or managed, affect peoples' perceptions and attitudes? What roles do news reports and other media portrayals play in

developing the cultural images around cyber-surveillance? How does the framing of Internet privacy really affect different peoples' willingness to use these technologies to communicate, network, shop, use services, and so on? There are powerful economic and governmental motives for discovering the answers to these questions and allaying individual fears. At the same time, the analysis of everyday experiences and the understanding of how people actually perceive the capture, trafficking and possible use of their personal data is a vital condition for effective activism.

While privacy protection is obviously a primary concern, it is certainly not the only important social issue raised by cyber-surveillance. Even when information is "de-personalized" and hence out of range of conventional privacy legislation, it can still play a potent role in discriminatory social sorting (Gandy 1993, 2009; Lyon 2003). Both by its nature and often by intent, cyber-surveillance is hidden from view and asymmetric in reinforcing pre-existing power differentials, lending advantage to the better-resourced, more secretive parties. This makes Internet or cyberspace governance more challenging, especially if it is to involve the wide array of legitimate stakeholders and reflect the public interest. This suggests that while pursuit of privacy protection should remain an important focus for remediating cyber-surveillance, other approaches that resist its incursions, and more generally bring it under democratic accountability, are equally important.

The answers to these questions are also complicated by the fact that it is not at all obvious what it means to "go online" and therefore when and how personal data is being captured. The integration of digital technologies into a large array of artefacts beyond "computers" has produced ubiquitous computing, and by extension the potential for ubiquitous surveillance. There are a growing number of ways in which everyday activities involve digital technologies with the capacities to capture, store, analyse, decide, disseminate and intervene, seemingly anywhere and at any time. The impending emergence of the "Internet of things" promises (or threatens) to further insinuate digital surveillance capabilities into the fabric of daily life. How and to what extent our cars, mobile phones, household appliances, and even our clothes embody digital surveillance capabilities are pressing questions that tax our analytical capacities as well as our regulatory regimes. There is, therefore, considerable confusion as to how to describe the technologies, understand the various practices and frame the associated issues.

Sustained reflection on the nature, causes and consequences of cyber-surveillance is also hampered by the episodic nature of the political disputes surrounding these issues. There is a "dispute of the month" character to the politics of this issue typically triggered by a corporate announcement of a new feature or service, which then motivates the community of skilled security experts and privacy advocates to analyze, blog, warn and critique. This is then followed by a period of corporate denial or retreat, and perhaps regulatory investigation. There is a cycle to Internet privacy disputes that has been witnessed for many years in relation to Microsoft, Intel, Google, Choicepoint, Facebook and many other smaller companies (Bennett 2008). The frenzied attention to the issue of the month tends to militate against the sustained reflection needed to build more general understandings of systemic trends and impacts.

The development and growth of the Internet are universally acknowledged as both a cause, and an effect, of the various trends that have extended and intensified levels of surveillance. Personal information is routinely captured on the net and therefore exemplifies what Lyon termed "everyday surveillance" (Lyon 1994). The flows are increasingly remote and global, creating multiple disconnections between the structures and agencies of information capture and control (Bennett and Raab 2006). Internet communications and activities have progressively been defined as a matter of risk assessment and securitization (Monahan 2006). Perhaps the Internet symbolizes exactly what Haggerty and Erickson (2000) meant by the "surveillant assemblage," signalling the "disappearance of disappearance" whereby anonymity and evasion of corporate and state monitoring become increasingly difficult to achieve.

Yet, it is by no means clear that the surveillance problems associated with the digital networking are conceptually or empirically separate from the range of questions addressed in other issues of this journal. Every practice and institution is perennially and profoundly affected by the capacity of new digitally mediated communications. Just as it is impossible to study more traditional sites of surveillance without understanding the ways in which the Internet has deepened and extended capacities for surveillance, so perhaps it is impossible to distinguish a discrete set of research questions or policy problems associated with the Internet. Internet surveillance still tends to be framed in terms of traditional institutions and practices: monitoring e-mail in the workplace; controlling Internet activity in schools; integrating online applications with electronic health records; targeted marketing and advertising; capturing online communications for national and international law enforcement. Some would contend that these issues generate distinctive sets of privacy problems, not because of the Internet, but because of the discrete sets of questions raised by different information sensitivities within distinct institutional contexts (Nissenbaum 2009).

Is there, therefore, any useful purpose in carving out a subfield distinction on the assumption that there must be some normative or empirical distinctions to be made? Are there quite separate surveillance practices that occur on the Internet, and nowhere else? Just because a great deal of interesting research is being conducted on cyber-surveillance does not mean that it can, and should be, justified as a distinct area of academic or practical concern.

This Special Issue

At one level, this special issue and the workshop on which it was based, interrogates this very question. The central rationale is provided by the observation that we now have a history of developments and disputes that permits some more considered theoretical and empirical reflection about whether the Internet has produced, or been produced as, a worldwide surveillance infrastructure within which individuals are increasingly "transparent" to a diverse variety of public and private institutions. Certainly there is a widespread fear that the amount of personal data being collected and trafficked is expanding rapidly and that this is contributing to an intensification of surveillance. But to what extent is this actually the case? While moving from analogue to digital formats can greatly facilitate the copying and transmission of data as well as the interoperability of systems, achieving properly joined-up, integrated organizational surveillance systems that are effective in meeting the high ambitions often set for them is a great deal harder. Can surveillance activities keep up with these developments, or are they prone to being bogged down in data overload? Does the desire for greater surveillance capabilities drive the development of digital mediation, or the other way around?

To address these and associated issues we convened an international research workshop on Cyber-Surveillance in Everyday Life at the University of Toronto in May 2011 (see http://digitallymediatedsurveillance.ca). The aim of this special issue, as well as the research agenda of the SSHRCC-funded "New Transparency" project[1], which sponsored the Toronto workshop upon which this issue is based, is to understand and critique digitally mediated surveillance practices in the context of the wider theoretical and empirical literature on surveillance. Media alarmism has fuelled a general popular understanding that one's life is an open book when one goes online, making one increasingly subject to unwelcome intrusions. The reality is obviously more complex and contingent on a variety of technological, institutional, legal and cultural factors. Those contingencies need to be better understood and analyzed.

This issue presents selected highlights of the workshop discussions. While the seven articles included here, drawn from the 25 presented at the workshop and subsequently revised and peer-reviewed, cannot

[1] http://www.sscqueens.org/projects/the-new-transparency

address the full range of issues tackled there, they do touch on some of the central concerns. They all grapple in various ways with the generative and disruptive effects of incorporating surveillance-enabling digital networks into the fabric of everyday life.

We begin by looking at one of the most significant and controversial aspects of digital networking—the rapid growth of unauthorized copying of copyrighted materials— also known as online "piracy." While the Internet has contributed greatly to undermining the business models of large copyright holders, not surprisingly they have turned to online surveillance for combating this phenomenon. This has brought the "content" industries, notably music recording and filmmaking, into tension with a hitherto quite separate sector—the telecommunications industry. In particular, as Milton Mueller, Stephanie Santoso and Andreas Kuehn show, content producers have attempted to force telecom carriers to install special equipment in their networks to identify and report on suspected "pirates."

Their article investigates how deep packet inspection (DPI) and other network surveillance techniques have become important factors in the EU and USA policy debates over online copyright infringement. These new technical capabilities reopened an old debate about the responsibility of Internet service providers for policing the Internet. Using a hybrid of actor-network theory from science, technology and society studies and actor-centred institutionalism in political science, Mueller *et al.* seek to understand the extent to which new technological capabilities have the power to alter regulatory principles. It shows that while the technology disrupted a policy equilibrium, neither the EU nor the USA applied DPI to copyright policing in a way that realized its radical potential. The key factor preventing such an integrated response was the disjunction between the interests of network operators and the interests of copyright holders. Even though the debate is not yet settled, this article offers a helpful reminder that technological potentials for surveillance, even those as flexible and seductive as DPI, are not alone determining. Social actors, in this case entrenched industrial interests and public advocacy campaigns, can play an important role.

Trisha Meyer and Leo Van Audenhove's article continues the theme of online surveillance as a means to reduce copyright infringement, but focuses exclusively on France, the country that has gone furthest in this approach. In 2009, France passed two laws aimed at fighting online piracy through "graduated response"—a warning and sanction system. Graduated response depends on surveillance of Internet use and encourages technological regulation, such as Internet filtering and blocking. As noted in Mueller et al. in this issue, while the attempt to use DPI within the network failed, copyright holders could conduct online surveillance outside the network, and report offenders to a special newly established independent public authority, HADOPI (Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet). The article analyzes the rationales advocated for copyright and the Internet and the argumentation for surveillance and technical protection measures. In the French debate on graduated response, much attention was given to the policy goal—reducing piracy, while the means of reaching the policy goal—surveillance and code, were rarely discussed. Graduated response deals with much more than copyright. It promotes informational control by copyright holders and contributes to the normalization of surveillance and to an increase of centralized control on the Internet.

The most prominent new arena of digital networking over the past decade has been the spectacular rise of social networking. Facebook is perhaps the best exemplar— founded in 2004, it claimed 850 million monthly active users as of May 2012, over 80 percent of which were outside the US and Canada (Facebook, 2012). Other leading examples of digital network platforms enabling people to find others with similar interests, communicate informally with them and share details of their lives include Wikipedia, Twitter, YouTube, World of Warcraft and Second Life. While enormously popular, these have generated considerable controversy, in large part because the aggregation and availability of detailed personal information makes them very attractive to a range of surveillance actors using a variety of techniques. The surveillance dimensions of social networking were by far the most popular topics at the Cyber-Surveillance Workshop, with several sessions devoted to some aspect of it.

Whereas much treatment of surveillance in traditional as well as digitally mediated settings focuses on hierarchical power relations, Alice Marwick explores peer-based surveillance. Her article argues that closely examining content created by others and looking at one's own content through other people's eyes, a common part of social media use, should be framed as "social surveillance." While social surveillance is distinguished from traditional surveillance along three axes (power, hierarchy, and reciprocity), its effects and behaviour modification is common to traditional surveillance. Drawing on ethnographic studies in the US, she looks at social surveillance, how it is practiced, and its impact on people who engage in it. Marwick uses Foucault's concept of capillaries of power to demonstrate that social surveillance assumes the power differentials evident in everyday interactions rather than the hierarchical power relationships assumed in much of the surveillance literature. Social media involves a collapse of social contexts and social roles, complicating boundary work but facilitating social surveillance. Individuals strategically reveal, disclose and conceal personal information to create connections with others and tend social boundaries. These processes are normal parts of day-to-day life in communities that are highly connected through social media.

A central issue of concern with social networking has been the various ways that commercial enterprises attempt to monetize the enormous quantities of fine-grained personal information they generate, putting individual users at a relative disadvantage vis à vis marketers. One recent attempt to turn the tables has been the development of group buying sites, in which social networking techniques are used to aggregate consumer-purchasing demand to negotiate better collective deals. Nora Draper's article explores the resulting tension between consumer power and surveillance through an analysis of group buying websites. These websites celebrate the power of the consumer generated through bulk purchases. Underlying the rhetoric about the autonomous consumer, however, is the systematic practice of buying, selling and reflecting consumer information. Through an examination of available promotional materials, websites and privacy policies, as well as interviews with representatives from group coupon companies, Draper outlines a number of concerns surrounding the ways that digital surveillance techniques are being used, and have the potential to be used, to define consumer interests. The article argues that such practices are particularly problematic when they are couched in the rhetoric of consumer freedom and power. The article concludes by suggesting emerging industry trends, including industry consolidation and geolocation technology, which raise additional questions about how companies shape consumer behaviour.

Another major strand of social networking has been the creation of online, virtual worlds. These have been heralded as offering exploratory spaces, freed from the physical and cultural constraints of the "real world," where people can develop new social identities and practices in relative privacy (Turkle 1995). However, as Jennifer Martin discovers in her study of surveillance in Second Life, there are some familiar patterns— surreptitious tracking of individuals for purposes of social regulation and commercial advantage. Surveillance patterns in Second Life come, perhaps not surprisingly, from other users, and Martin finds that the technological affordances of the virtual world enable both social surveillance and resistance. In an interesting twist, it turns out that the IP (Internet protocol) address assigned by the telecom networks to enable network routing provides a vital and problematic link to ones real life body. Mobilization of concerned users "in world" led to the exposure of covert surveillance technologies and their associated problems.

Indeed, while digital networking greatly facilitates surveillance, it also affords the means for resisting such surveillance. Among these is (for the moment) the possibility for anonymous interaction, at least in appearance. At the same time, critics charge that anonymity on the Internet presents a threat to public civility and safety. Kenneth Farrall explores this debate as it has played out in East Asia, and finds that contrary to Western stereotypical views, there strong popular support for anonymity in this region on various grounds. Drawing data from related academic studies, trade press and mass media, his article

examines recent variations in the salience, use, and comparative value of anonymity, and its relationship with individuality and collectivism, across three specific cultural contexts: China, South Korea, and Japan. While online anonymity in East Asia plays a role in affiliation and in acts of collective cognition, it is also valued as an individual privacy resource. Farrall concludes that we must be especially wary about assuming social systems might be better off, or more secure, without it.

Thwarting the surveillance potential of digital networking is perhaps nowhere more visible than among political activist communities fearing law enforcement agencies. Oliver Leistert's article reports on how activists around the world are developing and adopting specific measures to resist cyber-surveillance. These range from using code words and removing mobile phone batteries during meetings to the use of privacy enhancing technologies. The article draws on his interviews with activists from various countries, as well as documents from German law enforcement agencies in a recent case against activists. These documents reveal that the meta-data produced automatically by mobile telephony are at least as important for law enforcement as the content of the calls. Moreover, law enforcement will resort to generating surreptitiously the meta-data they need to determine the whereabouts of activists. Leistert thus argues that a mutual relationship between resistance and surveillance unfolds as one side reacts to the practices of the other: as soon as activists advance in protecting the content of their telecommunication, the surveilling parties shift to other tactics to track their targets, which in turn calls for new forms of avoidance, including disconnection from the network altogether.

This pattern of action and reaction by the various actors brings us full circle. The field of cyber-surveillance is in a particularly dynamic and formative stage. While it may be difficult to define the essential characteristics of cyber-surveillance, it is also obvious that it is not simply an extension of traditional forms of social control into a new media. We may not yet be able to put our finger on it, but each of these articles is testament to the fact that there is something very different and important going on when personal data is captured, controlled, disseminated, or manipulated in cyberspace.

References

Ball, K., K.D. Haggerty and D. Lyon, eds. 2012. *Routledge Handbook of Surveillance Studies*. London: Routledge.

Bamford, J. 2008. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York: Doubleday.

Bamford, J. 2012. 'The NSA Is Building the Country's Biggest Spy Center (Watch What You Say).' *Wired*. March 15, 2012. http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

Becker, K. and F. Stalder. 2009. *Deep Search: The Politics of Search Beyond Google*. Studienverlag.

Bennett, C.J. and C. D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge: MIT Press.

Bennett, C.J. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press.

Bennett, C.J. and C. D. Parsons (2012 forthcoming) 'Privacy and Surveillance: The Multi-Disciplinary Literature on the Capture, Use, and Disclosure of Personal information in Cyberspace' in *The Oxford Handbook of Internet Studies*, ed. W. Dutton. Oxford: Oxford University Press.

boyd, d. 2010. 'Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications.' In *Networked Self: Identity, Community, and Culture on Social Network Sites*, ed. Zizi Papacharissi, pp. 39-58.

Facebook. 2012. *Fact Sheet*. Retrieved from http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

Gandy, O. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder: Westview.

Gandy, O. 2009. *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Aldershot: Ashgate.

Haggerty, K.D. and R. Ericson. 2000. 'The surveillant assemblage.' *British Journal of Sociology* 54: 605–622.

Haggerty, K. and R. Erickson, eds. 2006. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Klein, M. 2009. *Wiring Up The Big Brother Machine...And Fighting It*. Charleston South Carolina: Booksurge Publishing.

Lyon, D. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D., ed. 2003. *Surveillance and Social Sorting*. London: Routledge.

Lyon, D. 2007. *Surveillance Studies: An Overview*. London: Polity.

Monahan, T., ed. 2006. *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge.

Murakami Wood, D. 2009. Situating Surveillance Studies. *Surveillance and Society* 19: 52-61.

Nissenbaum, H. 2009. *Privacy in Context*. Palo Alto: Stanford University Press.
Turkle, S. 1995. *Life on the Screen : Identity in the Age of the Internet*. New York: Simon & Schuster.
Wiener, N. 1948. *Cybernetics: Or Control and Communication in the Animal and the Machine*. MIT Press.
Zuboff, S. 1988. *In the Age of the Smart Machine*. New York: Basic Books.
Zureik, E. and M. Salter, eds. 2005. *Global Surveillance and Policing: Borders, Security, Identity*. Cullompton: Willan Publishing.
Zureik, E. L. Stalker, E. Smith, D. Lyon and Y. Chan, 2010. *Surveillance, Privacy and the Globalization of Personal Information: International Comparisons*. Montreal: McGill-Queens.