The World Wide Web of surveillance: The Internet and off-world power-flows

David Lyon
Department of Sociology
Queen's University
<lyond@post.queensu.ca>

The rapid growth of the Internet has provided many new opportunities for surveillance, understood as the garnering of personal data for a variety of uses. Modern surveillance systems developed in discrete spheres of the workplace, government administration and the military, generally for specific and limited purposes. The adoption of computer technologies since the 1960s has vastly increased the power of surveillance systems, and has also given rise to greater inter-agency collaboration, using techniques of data-matching or record linkage. This has been accompanied by a growth of what might be called commercial surveillance, that engages in clustering and targeting populations through geo-demographic data-collection. The advent of the Internet in the 1990s contributes to a further expansion of surveillance into a global sphere, even while the surveillance web is spun more finely. From police uses of the Internet (FBI sting in MD 1995) through the tracking of browsers (allegedly done by Netscape) to massive new interactive systems for wooing consumers (such as I-Spy's keystroke monitoring to obtain customer profiles) examples abound of a growing world-wide surveillance web, courtesy of the Internet. While earlier responses to surveillance tended to focus on legal protections of data and of "privacy", within and, increasingly, between nation-states, as an antidote, broader issues of ethics, education and politics in globalised settings are also raised by Internet-based surveillance (IBS). This paper highlights the differences made by IBS and comments on technical, legal and political strategies for counteracting its negative effects.

Introduction

Much is made of the enabling character of the Internet. We are told that this amazing tool liberates us to do things hitherto undreamed of. The idea of a "World WideWeb" suggests a global network of interconnected electronic nodes that make possible a new level of communication, that goes beyond the older broadcasting mode, into a sphere of interchange that promises to better even the democratic structure of the telephone system. The decentralised character of telephones, and

the interchangeable positions of sender and receiver, are augmented and enriched in the Internet, with the potential for new communicative relations within a burgeoning cyberspace (see, e.g. Poster 1995).

Webs can have other purposes, of course. The spider spins the web in order to entangle and entrap the unsuspecting fly. The more the fly struggles, the more it is stuck. Without disputing the inherently democratising possibilities latent in the Internet, it is worth exploring the capacity of the "web" to capture and control, to target and to trap, to manage and to manipulate. Although much has changed since the birth of the Internet's precursor as a Cold War military communications system, power has not simply been discarded as an infantile trait. Rather, power is now bound up with an extensive, increasingly integrated, surveillance technology.

"Personal" data caught in the Web are of many kinds. The Internet makes possible new levels of surveillance-integration, relating to work-situations, government administration, policing and, perhaps supremely, marketing. You may see a surveillance camera in the shopping mall, or even suspect that someone else is listening in to your cellular phone call. But Internet-based surveillance is far more subtle. You are part of a Usegroup? "People-finding" tools such as Alta Vista or Dejanews gather personal data from them. You visit Websites? Many such sites automatically create visitors' registers, collecting data such as the kind of computer you own, your e-mail address and the previous page you visited. The fine threads are almost imperceptible, and although each "fly" movement creates more entanglement, the "fly" remains blissfully unaware of what is happening.

In order to understand the world-wide-web of surveillance, firstly, some background is needed. The precursors to contemporary surveillance are many, but the Internet helps to shift such activity into a different register, a different plane. Where once the monitoring of place was significant, now surveillance data flows in a kind of "off-world" sphere. ("Off-world" real estate is advertised in the movie, *Bladerunner*. As used here the term echoes Manuel Castells' (1989) reference to economic "flows", uncoupled from physical places.) Secondly, the various forms of surveillance activity generated on the Internet are explored, and common traits are noted. Thirdly, the question is asked, how should these surveillance practices be understood? Are they an extension of capitalist control, or further evidence of our identity-less incarceration in an electronically-enhanced "iron cage" of bureaucratic organization? Or are they better understood as a form of panoptic power, where an unseen observer oversees a regime of truth and knowledge?

Surveillance: a modern growth industry

Watching others' activities, as a means of monitoring and supervising them, is hardly a new practice. The most ancient records — say of Egypt or Babylon —

indicate that surveillance has been carried out to keep tabs on populations for taxation or military purposes, or to ensure that work was carried out satisfactorily. In modern times, however, surveillance became much more routine and general, involving whole national populations, across a range of activities and life situations. Births, marriages and deaths were recorded systematically, individual persons were listed as being of an age and status to vote in democratic elections, and workers were assembled under one roof to facilitate supervision.

In the twentieth century, these processes intensified. Government administration undertook surveys of populations, and departments such as health, welfare, immigration, taxation, customs, housing, vehicle and driver licencing kept more and more detailed records. Rational mechanisms for bureaucratic organization, analyzed par excellence by Weber, employed a panoply of methods for creating and maintaining files, and ensuring that a hierarchy of rule-observing officials kept control thereby. The logic of capitalist development also entailed supervision and monitoring in order to maximise productivity and profit. Scientific management represented this trend towards greater surveillance-intensity, with its focus on detailed time-and-movement analyses. By the mid- twentieth century it had become clear that surveillance was constitutive of modern organization. Except that the term "surveillance" was still reserved mainly for intelligence and security services, not the routine business of everyday life.

The term "surveillance" was really only popularized in the mid-1980s, for several interesting reasons. One was that organizations of all kinds started to computerize, from the 1960s onwards. The massive collection of personal data, begun during the Cold War era, when state socialist societies still exerted tight political control over their citizens, generated fears of Orwellian police states and Kafkaesque faceless bureaucratic machines. Investigations of the social implications of electronic technologies suggested to some the advent of "surveillance societies" (Marx 1985, Flaherty 1989).

At the same time as widespread and accelerating computerization occurred, enthusiasm was mounting for Michel Foucault's ground-breaking studies of modern forms of discipline. These appeared in a series of related books, but most famously for present purposes in his *Discipline and Punish* (1979). In that book, the architectural plan for the "Panopticon" prison was elevated to exemplary status for modern disciplinary techniques. What Foucault did not attempt, however, was an extension of his analysis to electronic forms of surveillance.

Two major debates began concerning surveillance. The first focuses on whether electronic technologies contribute to a qualitatively different kind of surveillance from that characterized by paper files and classic bureaucratic organization. Analysts such as James Rule (1973) and Gary T. Marx (1988) argue

that they do, and present sociological explanations of how this happens. The second question, however, is how far Foucault's work can be applied to electronic surveillance (see Lyon 1993). Analysts such as Webster and Robins (1986), Zuboff (1988) and Gordon (1987) were early exponents of the relevance of panopticism, while others were less sure.

The two debates now converge in the area of most rapid expansion, consumer surveillance. The use of the newer technologies raises the question of how far database marketing goes beyond older styles of mass advertising, coupon delivery and club memberships. So-called "mass customization" creates incentives for collection of personal data for use in the production-marketing process. Manufacturers or retailers wish to establish a service-type relationship with customers, collecting, storing and manipulating information about them in order to control their behaviours (Samarajiva 1994, 91).

Database marketing works by clustering consumers by social type and location, and by more and more tightly trying to personalize advertising and consumer advice. This is linked directly with the question of Foucaldian analysis. For Webster and Robins, the attempt more closely to influence consumers is seen as "social management" — an extension of Taylorist practices of scientific management. This is elaborated and refined in Oscar Gandy's work on what he calls the "panoptic sort", where database marketing is seen as a "discriminatory technology" for grading and guiding consumers.

Consumer surveillance uses many of the same techniques as other forms of dataveillance, such as profiling, record linkage, and so on, but in North America operates largely beyond the reach of regulatory limits placed on government use of these practices. This, coupled with the apparent effectiveness of the crude behaviourist sociology involved in channeling choice and directing desire, means that database marketing has mushroomed in a few short years. Until recently, the only other brake on its progress was the relative lack of communicative means for transmitting data, not only within, but also between countries and continents. Enter the Internet.

Cyberspace surveillance

The term "World-Wide-Web of Surveillance" is more a metaphor than a precise indicator. "Internet-based surveillance" comes closer to designating the field, but even this, technically speaking, would not encompass e-mail systems, despite the fact that many refer casually to e-mail as being "on the net" or their e-mail accounts as "Internet addresses." Perhaps "cyberspace surveillance" would serve better, referring to any forms of surveillance that occur in computer-mediated communications. From the viewpoint of the data-subject, all these are part of the

web whose weaving is triggered at the keyboard and which can be seen — if one knows where to look — on the screen.

Three main categories of cyberspace surveillance may be discerned, relating to employment, to security and policing, and to marketing. These categories blur in practice, for at least two reasons. One is that the very existence of electronic networks makes it easier in principle for data to be shared between different agencies, even though in most countries regulatory regimes limit this. The other is that the same network used by large and powerful bodies such as governments or corporations can also be used by individuals or groups with far less power. At the very least this means that cyberspace surveillance is not necessarily centralized. As William Bogard (1996,134) observes, this is not just a global system, "but an orbital and cellular network linking the macro and micro levels of information-gathering . . ."

In employment situations, monitoring and supervisory forms of surveillance are common, so it is hardly surprising that increasing use of the Internet, and above all e-mail, by employees has created new challenges. In December 1996, a Canadian federal scientist at the Department of Defence was arrested for allegedly downloading more than 20,000 pictures and video clips of child pornography, using his office computer (MacLeod 1997). Also in 1996, Compaq Computer in Houston, Texas fired twelve employees for using work-time to visit sex sites. With respect to e-mail, concerns have arisen among employers about the use of company time and resources for private correspondence, within and beyond the organization.

Responses to such practices generally take the form of technical measures to minimize the risk of recurrence. Software is installed to record and report all activities entailing use of the Internet and e-mail. All company information technology services divisions have the capacity to track the use of electronic network use, and to monitor the content of e-mail messages. In most of North America, whether they do so or not is a matter of company or organizational policy. A few years ago, a U.S. survey of managers revealed that 22% had searched employees' computer files, voice-mail, e-mail and other electronic communications (Pillar 1993, 7). The results are sometimes dramatic. A Los Angeles police officer, Laurence Powell, got into deep water after sending an e-mail to a friend, describing his involvement with Rodney King: "I haven't beaten anybody this bad in a long time" (Weisband and Reinig 1995, 41).

These examples, from work-situations, also spill over into the area of policing and security. Part of the policing is private, as when Canadian service-provider I-STAR removed certain risqué groups in the alt.sex hierarchy from public access. But another part is public, when Internet-based surveillance is undertaken by legally-constituted police services. In 1995, for instance, the American FBI

undertook "Operation Innocent", an undercover sting involving the interception of America On-Line (AOL) e-mails of people who had responded to messages purporting to be from pedophiles. Raids were conducted on 125 homes and offices in 57 cites and many arrests were made (*New York Times*, September 16, 1995, cited in Zuijdwijk and Steeves 1995).

The best-known effort to enable widespread "security" surveillance on the Internet is the so-called Clipper Chip. In 1994, the U.S. government proposed to introduce a uniform encryption standard, that would effectively prohibit the proliferation of codes designed to protect the privacy of electronic communications. While individual users could rest assured that their messages would remain private, the one exception was that, in the interests of "national security", government agents would be able to listen in, when appropriate and necessary. Needless to say, the controversy aroused by this proposal has been fierce — on and off-line — and is, as yet, unresolved (see Levy 1994).

While the preceding examples of cyberspace surveillance in employment and policing are interesting and, for many, alarming, they are on a small scale when compared with the massive armory of commercial surveillance used by marketers. Apart from the suspicion of many that Netscape itself tracks the virtual movement of its users — Netscape admits that they know each time a browser of theirs is in use — many other companies are certainly engaged in extensive profiling of Internet users. Some of these use the well-worn ploy of registration — as when one fills a warranty form for an appliance, thus giving extensive personal data to the company — to profile visitors to Websites. In this case, some informed consent is required of netsurfers.

In many other cases, however, no such consent is sought or required. Websites frequently send automatic messages back to their owners, providing data about users' needs, habits and purchases, based on users' visits to the site in question. Some transactional information is passively recorded, such that the Webmaster can determine what files, pictures or images are of interest to the user, how long was spent with each, and where the user was before and after visiting that site. Internet Profiles, known better as I/PRO, indicates just how well and by whom a site is used. I/PRO's clients include Yahoo!, Compuserve, Netscape, and others such as CMP Publications and Playboy (Stagliano 1996).

So-called "Cookies" (Client-Side Persistent Information) give extensive tracking capacities to companies eager to exploit commercially the valuable segmented personal data on discrete individuals. Cookies allow Websites to store information about visited sites on the user's hard drive, then they read the drive each time a site is visited to discover if the user has been there before. The latest marketing techniques applaud these practices, as offering the benefits of

customized advertising to the consumer, tailored to their needs. But the title of one such manual — *Strategic Marketing for a Digital Age* (Bishop 1996) — also leaves little doubt about who else will benefit from this "military" manoeuvre.

However, lest these examples be discounted as paranoid, it should be noted that much data gathered via the Internet is available to any user with a credit card. A "privacy panic" arose in late 1996, over the activities of Lexis-Nexis and their P-TRAK system, designed to help police and lawyers locate litigants, witnesses, shareholders, debtors, heirs and beneficiaries. In response to an outcry regarding the availability of Social Security numbers along with names, addresses and telephone numbers, the U.S. Federal Trade Commission (FTC) called for broader privacy protection, and Lexis-Nexis eliminated access to Social Security numbers. As it happens, other companies offer much fuller services than P-TRAK, also for fixed fees per datum. Information Resources in Fullerton, California, for example, offers items such as criminal and court records, Social Security numbers, driving records and employment background checks. Although one cannot obtain such information directly from the Web, all such companies — Information Resources, CDB Infotech, Information America, and so on — have Websites for marketing purposes (<isworld@listserv.hea.ie>).

Much uncertainty still surrounds the Internet use of such databases. No one seems to object to having national white-pages directories available as a means of locating people and businesses (such as Canada411: <http://canada411.com>). Yet when the city of Victoria put its tax-assessment rolls on the Internet, British Columbia Privacy Commissioner David Flaherty announced an investigation. The fear was that people could be located when they might have legitimate reasons for withholding details of their whereabouts. The site proved extremely popular but the mayor closed it down after the investigation was announced (McInnes 1996).

Theorizing the surveillance web

What John Beniger (1986) calls the "control revolution" extends through all modern organizations. Especially in the police, the military, and in business corporations, a bureaucratic drive is evident, pushing towards tighter predictability as a means to greater control. For Beniger, such control is understood as increasing the probability of a desired outcome. This is the logic behind surveillance of many kinds. All contemporary institutions in the so-called advanced societies are characterised by an internal imperative to obtain, store, produce and distribute data for use in the risk management of their respective populations.

The examples given earlier show how this works in practice. Employers try to reduce risk — of workers using office time or equipment for their own purposes, for instance — in employment situations. The police work towards preventing the

risks of crimes being committed. And marketers do all in their power to avoid risks of lost opportunities, market niches, and, ultimately, profit. All engage in data gathering procedures to try to pinpoint risks (or opportunities) and to predict outcomes. So surveillance spreads, becoming constantly more routine, more intensive (profiles) and extensive (populations), driven by economic, bureaucratic and now technological forces.

The surveillance literature becomes fuzzy at this point. Two main concerns are expressed regarding the outcomes of surveillance situations. One has to do with social participation, the other with personhood. The first sees surveillance outcomes in terms of social division and inequality, and thus social access and exclusion. The second focuses on questions of "invasions of privacy," on identity and, sometimes, on human dignity. Unfortunately, some theorists seem so concerned with the one that they ignore or minimize the significance of the other. Yet the two dimensions overlap, indeed, are two sides of the same coin. Identification and identity, for example, may be the means of inclusion and exclusion. Personhood is realized in participation.

Surveillance is clearly implicated in the maintenance of social inequality and division. The panoptic sort (Gandy) distinguishes between different classes of consumers, reinforcing the lifestyle patterns and expectations of each group, and maintaining a barrier between consumers and non-consumers. The latter form marginal populations — due to their age, ethnicity, income, neighbourhood and so on — that are in part constituted by the workings of surveillance systems that concentrate on the more rich and respectable echelons of society. Such marginal groups have their own surveillance, that tend to be much more punitive, found in health, welfare and penal systems (Lyon 1994; cf. Ericson 1995).

Surveillance also deepens questions of identity, when the capacity to control communication about oneself is wrested from the individual. This is one strand in the debate over privacy, the right to which is often held to entail taking — or being given back — such control by various means. Analyses of surveillance that start from a premise of privacy are really focusing on fairly philosophical questions of personhood, and, in particular, what sorts of expectations one might have for communicative self-determination. Such analyses tend to assume that autonomous, individuated "selves" are threatened by intensified surveillance.

These issues are clearly ones of considerable political and ethical import, and that is why they should be discussed in relation to the burgeoning practices of cyberspace surveillance. However removed from daily life and remote from public control these practices seem to be, the drives behind them are very powerful, and their material consequences are all too real. As Stephen Graham says, many of these systems are directly "geared to the protection and fortressing of affluent consumer

neighbourhoods and corporate districts . . . and to the exclusion, enforcement and control of the groups and areas that are marginalised by labour market and welfare restructuring" (1996, 28). The distribution of life-chances and of communal and personal well-being are increasingly dependent on the increasingly efficient systems of advanced surveillance.

Beyond these questions of participation and personhood, however, lie some further concerns about the nature of contemporary cyberspace surveillance. The kinds of issues just discussed assume that modern discourses of human rights or social justice still hold good in the world of the Internet. Yet the Internet is implicated in certain cultural shifts that call in question just those kinds of categories. Mark Poster, for instance, argues that the way that today's "personal" databases function makes them more like a "superpanopticon" (1995). Surveillance practices are not so much a threat to the "privacy" of an individual subject, but are actually involved in the very constitution of subjects. This puts a new slant on surveillance.

The "new slant" may be observed in more conventional settings. In the case of medical practice, notes Robert Castel, there has been a shift of emphasis away from face-to-face examination of the patient and towards an examination of records "compiled in varying situations by diverse professionals and specialists interconnected solely through the circulation of individuals' dossiers" (Castel 1991, 282). This process has, he believes, crossed a threshold and taken the character of a mutation, a new form of surveillance that has prevention of risk at its core. Individual subjects are now less significant than statistical correlations; autonomized management becomes the order of the day. If one can guide and assign individuals rather than take responsibility for them, then the management strategy has worked. This could even be seen, argues Castel, as a "post-disciplinary" situation, where the quest of efficiency has become paramount. To "forward plan social trajectories from a 'scientific' evaluation of individual abilities" is the new — maybe mythical — goal (Castel, 296).

The idea that there might be a "mythical goal" of surveillance has been taken up more recently by William Bogard (1996). He argues that a "simulation" of surveillance is contributing to "hypercontrol" in societies infused with communication and information technology networks. The "mutation" described by Castel seems to have wider relevance. Bogard brings together the work of Foucault with that of Jean Baudrillard to try to obtain theoretical leverage on the simulated or virtual aspects of surveillance. Where the panopticon dealt with real time and physical space — it is, essentially, an architecture — today's "hyperpanoptics" exist in a realm of electronic environments, where time is asynchronous and speed of flows is crucial, and where distance and proximity are

blurred in "cyberspace." Existing surveillance literature often speaks of data-images or data-shadows, and of blurring boundaries between images and realities, but Bogard's work suggests that this is central rather than epiphenomenal to today's situation.

Bogard stresses that the simulation of surveillance does not mean it is illusory, unreal. Indeed, "the better a simulation, the less awareness there is of the artifice that identifies it as a simulation" (31). This connects with the idea of a "mythical goal" of surveillance, namely, that the problem of perceptual control over a distance is solved through new electronic means. Knowing in advance who is likely to engage in welfare fraud, buy Bennetton or vote Liberal is seen as the means of maintaining order, normalizing populations, maximizing efficiency. Unlimited surveillance is the unspoken goal (and it is attractive to politicians, police, marketers and high-tech companies alike) but it is, as Bogard says, "actual only in simulation" (49). Alongside older forms of monitoring and supervision (such as the use of software for checking on employees or children's use of the Internet) are these newer methods, that more and more involve the subjects of surveillance, now part of the total surveillance scene. And the Internet serves only to make the mythical goal more (seemingly) realizable.

These reflections aid analysis insofar as they help theory to move beyond the confines of physical space and real time — a task already accomplished in the virtual realm of cyberspace. But it would be a mistake to pull Wittgenstein's ladder up behind us as we rise through the clouds into this next level of surveillant simulation. The danger of discourses that inhabit a world of simulations is to forget the realness of the "real world" (see, e.g. Robins 1995). This demands that whatever constructive insights are gleaned from Foucault and Baudrillard, they be articulated with those of access, inclusion/exclusion and participation on the one hand, and identity, dignity and personhood on the other. As Graham reminds, in respect of the city, "webs of simulated surveillance system become woven into supporting and constructing the fabric of "real" urban life, just as the "real" landscapes of cities themselves become transformed into a realm of surveillant simulation" (1996, 28). Much work remains to be done to understand how these systems work.

Bringing cyberspace surveillance down to earth

The World-Wide-Web of surveillance exists as a means of control, enhancing through electronic networks already existing forms of surveillance. Exactly how that control is sought and is achieved remains debatable, although it is clear that on present showing, existing inequalities of power and access are reinforced, and fears of being held in an unseen gaze are unrelieved. The foregoing discussion suggests that modern surveillance, based in the so-called control revolution, has evolved

rapidly in new directions since the inception of computer-power. While such computerization started as a way to enhance and augment already existing systems of surveillance, its technical possibilities have provided opportunities for novel practices, geared to coping with risk by preempting and preventing or by managing and manipulating. The convergence of computing with telecommunications, seen for example in the Internet, has enabled the growth of virtual surveillance, off-world data-flows, detached from their erstwhile moorings in time-and-space.

Surveillance theories have struggled with these changes, and the classic work of Marx and Weber has been augmented by that of Foucault, and now, Baudrillard. However, theory is still in a somewhat rudimentary condition. Yet if the preceding argument is correct, surveillance, including surveillant simulation, has all too real social, material, and spiritual effects. Understanding these, and thus developing some critical discourses to deal with them, is of paramount importance. As use of the Internet expands rapidly among the well-heeled communities of the so-called advanced societies, so the scope of newer surveillance methods will also grow. At present, most "critical" debate is couched in terms of "privacy" concerns, in which rights to be left alone, or to "free speech" (guaranteed by encryption security) are voiced most stridently. Resistance is all too often understood in terms of charging royalties on the use of personal data, or, better, of encouraging at least voluntary compliance with data protection conventions.

Some theories of privacy, recognizing classic liberal conceptions as a cul-de-sac, have attempted to introduce a social dimension to the argument. Priscilla Regan's (1995) work is exemplary in this respect. But until the inequality-reinforcing and personhood-threatening aspects of contemporary surveillance are seen together, and until these dimensions are understood in relation to the virtualizing of surveillance, the real issues of contemporary surveillance will continue to elude us. Whatever the social benefits of the Internet — and, stripped of hype, there are many — their realization will be jeopardized by the existence of the World-Wide-Web of surveillance. This is not something added to or different from the "rest of" the Internet, but an aspect intrinsic to its constitution.

References

Beniger, John. 1986. *The control revolution.* Cambridge MA: Harvard University Press.

Bishop, Bill. 1996. *Strategic marketing for a digital age.* Toronto: Harper Collins.

Bogard, William . 1996. *The simulation of surveillance: Hypercontrol in telematic societies.* Cambridge and New York: Cambridge University Press.

Castel, Robert. 1991. From dangerousness to risk. In *The Foucault effect: Studies in governmentality,* ed. Graham Burchell, Colin Gordon and Peter Miller, 281-298. Brighton UK: Wheatsheaf.

Castells, Manuel. 1989. *The informational city.* Oxford: Blackwell.

Ericson, Richard. 1995. Review of *The costs of privacy,* by Steven Nock. In *American Journal of Sociology* 100: 294-296.

Flaherty, David. 1989. *Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada and the United States.* Chapel Hill: University of North Carolina Press.

Foucault, Michel. 1979. *Discipline and punish.* New York: Pantheon.

Gordon, Diana. 1987. The electronic panopticon: A case-study of the development of the national criminal records system. *Politics and Society* 15: 483-511.

Graham Stephen. 1996. Surveillant simulation and the city. Paper read at the NCGIA conference, Baltimore.

Levy, Stephen. 1994. The battle of the clipper chip. *New York Times Magazine*, June 12: 44,51,60,70.

Lyon, David. 1993. An electronic panopticon? A sociological critique of surveillance theory. *Sociological Review* 41: 653-78.

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

Lyon, David and Elia Zureik (eds.). 1996. *Computers, surveillance and privacy.* Minneapolis: University of Minnesota Press.

MacLeod, Ian. 1997. Cyber-shirking alarms companies. *Kingston Whig-Standard*, January 16.

Marx, Gary T. 1985. The surveillance society: The threat of 1984-style techniques. *The Futurist*, June, 21-26.

Marx, Gary T. 1988. *Undercover: police surveillance in America.* Berkeley: University of California Press.

McInnes, Craig. 1996. Victoria data site pulled off Internet. *Globe and Mail*, September 27.

Pillar, Charles. 1993. Bosses with X-ray eyes. *MacWorld*, July.

Poster, Mark. 1995. *The second media age.* Cambridge: Polity Press.

Regan, Priscilla. 1995. *Legislating privacy.* Chapel Hill: University of North Carolina Press.

Robins, Kevin. 1995 Cyberspace and the world we live in. *Body and Society* 1 (3-4): 135-155.

Rule, James. 1973. *Private lives, public surveillance.* London: Allen Lane.

Samarajiva, Rohan. 1994. Privacy in electronic public space: Emerging Issues. *Canadian Journal of Communication* 19: 87-99.

Stagliano, Riccardo. 1996. Publicité du troisième type. In *L'Internet: l'ecstase et l'effroi.* Paris: Le Monde Diplomatique.

Webster, Frank, and Kevin Robins. 1986. *Information technology: A Luddite analysis.* NJ: Ablex .

Wiesband, Suzanne, and Bruce Reinig. 1995. Managing user perceptions of e-mail privacy. *Communications of the ACM*, 38(12).

Zuboff, Shoshana. 1988. *In the age of the smart machine.* New York: Basic Books.

Zuijdwijk, Ton, and Valerie Steeves. 1995. *The protection of privacy on the Internet.* Ottawa, Immigration and Refugee Board.