Routledge
Taylor & Francis Group

EVERYDAY SURVEILLANCE
Personal data and social classifications

David Lyon
Queen's University, Kingston, Ontario, Canada

Abstract

Surveillance is no longer merely a matter of deliberate, individual scrutiny and consequent fears for personal privacy. It is an everyday experience, run by myriad agencies for multiple purposes and exempting no one. Surveillance is also an ambiguous process, the two faces of which must yet be seen in relation to each other. Numerous data – now including biometric, genetic and video data – are abstracted from embodied persons and manipulated to create profiles and risk categories in a networked, rhizomic system. The resulting classifications are intended to influence and to manage populations and persons. The choices and the chances of data-subjects are thus both directly and indirectly affected, but socio-technical surveillance systems are also affected by people complying with, negotiating or resisting surveillance.

Keywords

surveillance, control, privacy, categorization, ethics, bodies, databases

INTRODUCTION

Surveillance by electronic means is an increasingly significant mode of governance in so-called knowledge-based or information societies. As Rose nicely puts it, 'surveillance is "designed in" to the flows of everyday life' (1999: 234). Daily routines are now subject to myriad forms of checking, watching, recording and analysing, so much so that we often take for granted the fact that we leave trails and traces wherever we are and whatever we do (Staples 2000). But those trails and traces, however justified, are not innocent. Taken together, they are located within a network of relationships that service us, situate us and help to organize and order our social lives. Surveillance contributes increasingly to the reproduction and reinforcing of social divisions.

Surveillance in this context means a focused attention to personal details aimed at exerting an influence over or managing the objects of the data, or 'data subjects' as they are sometimes called. Although the word surveillance often has connotations of threat, it involves inherently ambiguous processes that should

Information, Communication & Society
ISSN 1369-118X print/ISSN 1468-4462 online © 2002 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/13691180210130806

not be considered in a merely negative light. Much everyday convenience, efficiency and security depends upon surveillance. Moreover, it occurs in a world where other kinds of 'mediated visibility' (Thompson 1995: chapter 4) – particularly through television, but also using webcams and so on – are available, and have a variety of effects. Surveillance is just one aspect of this mediated world. It also exhibits both hard and soft faces, which need to be distinguished. Nonetheless, surveillance does also raise questions about power, citizenship and technological development, and about information policy, regulation and resistance.

In what follows, I offer a straightforward and simple argument about everyday surveillance but one that is at odds in some significant respects with other treatments of the same themes. I argue, for example, that the rise of routinized, systematic surveillance has rather mundane origins that should not in the first place be construed as socially sinister. Surveillance is seen here as a response to the 'disappearing body' from integrative social relationships, enabled by modern means of communication and information-handling. The outcomes of this process, however, are not inconsequential as far as social order and social control are concerned. The rise of invisible information infrastructures that facilitate the classification and processing of personal data and the increasing porousness of their storage containers generate distinctive questions about everyday surveillance. These questions invite critical responses, ones that go well beyond the conventional discourses of privacy that are so often trotted out as counterpoints to surveillance.

HOW DID SURVEILLANCE BECOME SO CENTRAL?

For most of human history, most social interaction has been face-to-face. I say 'has been' rather than 'was' to emphasize the point that face-to-face interaction continues to be significant. But communication that takes place with the other person or persons present, in certain locales, has been supplemented by many forms of communication that do not involve co-presence and that are stretched over space. It is a key feature of modernity that using new media of communication people can interact and even remain in relationships that are integrated with others despite being divided by distance.

Fresh forms of interaction have developed as a result of this stretching of relations over space and, in some ways, over time. The new technologies are implicated in those new relationships, just because they are the means that enable them. The forms of relationship are not caused by the new technologies (which often have different uses and effects than those intended by their producers and their proponents) but the new technologies mediate them. It is striking, for example, that neither the telephone nor the Internet were conceived as means of helping ordinary people to chat with each other but that is just how they have come to be used (Marvin 1988; Slevin 2000). Some forms of mediated interaction have emerged over the past two centuries that are much less obviously reciprocal than phone calls or e-mail conversations. One thinks of the so-called mass media, where messages may be largely one-way, but where people are nonetheless linked in communication and symbolic exchange. Today, of course, phone-in shows on the radio and e-mail responses to television shows or newspaper articles increase the dialogical possibilities of these media.

I mention this variety of new kinds of mediated relationships to indicate that surveillance is just one among many forms of communication that have emerged as face-to-face relations of co-presence have been supplemented by so many others (Lyon 1997). So, what is special about surveillance? I suggest that as new technologies enabled more and more to be done at a distance, some compensations are sought for the fading face, the disappearing body. In earlier times, suitable compensations included a signature or a seal on a letter to authenticate its personal origin. But in the increasingly complex social settings of modernity, other tokens of trust were sought, to make up for the lack of visual, body clues and cues, such as handshakes, eye contact, and so on. Of course, the tokens of trust were sought by powerful institutions as well as in more informal contexts, which is why a critical analysis is called for.

By the twentieth century, not only the passport (Torpey 2000) or national identification papers, but also other forms of documentary evidence were required for administrative and commercial purposes: for identification at school, the workplace or to police, for admission to certain sites, to obtain cash from a bank or to pay for purchases, tokens of trust, of worthiness, of authentication. Today our wallets and purses are stuffed with credit cards, membership numbers, phonecards, social insurance cards, driver's licences, library cards, health cards and loyalty club cards that can either be used when no other body is present for the transaction – say, at a bank machine – or when the other party is a complete stranger who needs some kind of validation for the exchange to take place.

The body has steadily disappeared from these relations but communication continues, at a distance, mediated overwhelmingly today by electronic means. From the point of view of the organization or agency that issues the magnetic strip, the barcode or the PIN, of course, the process of checking for inclusion or of verifying identity is a means of classifying and categorizing data subjects.

What of the view the other way? Personal data may be released – wittingly or unwittingly – by those to whom they refer and communicated to others (the bank, the welfare department, the airline) who have some interest in them. These data are likely to be the basis of communication with the data-subjects as well but beyond this, the data are frequently combined in new ways and communicated between machines much more than with data subjects. What happens to those data as they are processed is largely unknown by data subjects, although some of it may be guessed when the road-toll invoice, personalized advertising or spam (electronic junk mail) appears in the mailbox or on the screen.

Paradoxes abound. Privacy, which so often is felt to be endangered by these developments, can equally be considered as a key generator of surveillance. As the more anonymous arrangements of the modern 'society of strangers' emerged, and privacy was more valued, so the reciprocal need for tokens of trust grew as a means of maintaining the integrity of relations between those strangers (Nock 1993). As the locally-known, embodied person slid from view in the web of social relations, so the importance of credentials, identification and other documentary evidence was amplified. The other paradox, as I have hinted, is that the same process displays quite different faces. The means of keeping trust between strangers are at the same time the means of keeping track of the details of daily life. Privacy produces surveillance that, it is said, threatens privacy. But not only privacy. As surveillance became a central, constitutive component of modernity, so it became increasingly a social ordering device on a steadily greater scale. This happened as more and more bureaucratic organizations undertook surveillance activities in order to maximize their efficiency and their efficacy. Keeping track is a crucial means of ensuring organizational efficiency, as Max Weber classically demonstrated (Dandeker 1990). But keeping track requires more and more sophisticated means of classification and categorization, that both feeds on surveillance data and stimulates the organizational appetite for them. Mundane means such as form-filling show how this process works, because as Brown and Duguid say, 'Forms are the crucial means by which an organization brings the heterogeneous world into line with its processes' (2000: 108). For all their apparent exactness, many gap-closing improvisations occur to make social realities fit the process especially in residual categories of 'other'. Even in police work, where one might hope for some tight definitions, rather elastic categories such as 'annoying behaviour' may be used in creating formulaic profiles of city 'hot-spots' in cities like Toronto (Verma 1999).

Surveillance depends, then, on information infrastructures, invisible frameworks that order the data according to certain criteria, purposes and interests.

In the later twentieth century, information infrastructures were decisively computerized, which simultaneously made them even less visible and even more powerful, and also produced some specific kinds of coding (Lessig 1999). The kinds of interests behind social classifications expanded to include not only government departments and policing or security services, but also a multitude of commercial organizations as well (Gandy 1993; Lyon 1994). Beyond this, particular kinds of agencies have become prominent – above all insurance companies – and their interests often transcend those of either governmental or commercial domains. They have become, albeit as an unintended consequence of their activities, very powerful social actors on the contemporary landscape (Strange 1996).

To take just one example, there is plenty of evidence that insurance companies contribute strongly to police work in Canada. As Richard V. Ericson and Kevin D. Haggerty show, the 'risk logics' and classification schemes of external institutions such as insurance companies profoundly influence the police, who become in effect knowledge workers for them. Insurance demands lead to a shift from territories to classes of populations with varying risk levels. Biographical data are sought on populations in order to profile them in terms of probabilities and possibilities, which makes surveillance more and more systematic. Computerization simply extends the whole process such that in the end, they claim that:

> Coercive control gives way to contingent categorization. Knowledge of risk is more important than moral culpability and punishment. Innocence declines, and everyone is assumed to be 'guilty' until the risk communication system reveals otherwise.
>
> (Ericson and Haggerty 1997: 449)

But it is not merely that information infrastructures have significant connections with the rise of risk management and insurance classifications. Information infrastructures also enable the expansion of surveillance capacities (Rule 1973) in several important respects. The first is that they allow for plug-ins from other sorts of technological devices, and the second, which I comment on in a moment, is that they permit greater porousness between containers. Two of the plug-ins that I have in mind are video and closed circuit television (CCTV) surveillance on the one hand, and biometrics and genetic surveillance on the other. The one has to do with the visibility of body behaviours, including in some cases the recognition of body identities, and the other, with personal identification using unique body parts and the prediction of behaviours and conditions from reading genetic sequences.

It is important to note that these plug-ins depend upon the information infrastructure for their heightened surveillance capacities. For while in their own right each may contribute in specific ways to the augmenting of surveillance – by adding layers of visibility or by producing more precise identifications or predictions – it is their dependence on computer-based information infrastructures that give them their peculiar power. Without the assistance of complex and sophisticated data processing power, these new technologies would remain relatively weak as means of surveillance. From the point of view of policy, this is a telling development because at present the level of unquestioning acceptance of information and communication technologies is far higher than that of ethical and political critique and assessment.

The second way that information infrastructures tend to bolster surveillance capacities is that they enable networked communication between different databases. Whereas once it was fairly safe to assume that personal records kept for purposes such as health, policing, social insurance, banking and driver licensing would be stored in relatively watertight containers, the computerization of these records means that they are readily amenable to different forms of integration. Given the immense value placed on personal data, both for commercial exploitation and for risk management, huge pressure is placed on these containers to yield their secrets in shareable ways.

Similar methods of data matching or record linkage occur in all sectors, which makes cross-tabulation technically easier. Government departments seek ways of assisting each other in obtaining compliance, but commercial organizations also exchange and trade categorized personal data in an effort to market their wares more effectively. Sometimes similar processes occur in the same place, for very different purposes. At airports, for instance, frequent flyer data, entered as passengers pass through check-in, may be used for other purposes such as car rental advertising. But personal data on airline passengers may also be exchanged for security purposes, particularly after the terrorist attacks of 11 September 2001. US and Canadian border authorities now share such data and the process is likely to escalate in other contexts as well (Lyon 2001; Whittington and Harper 2001).

A related issue of what might be called 'floating data' is that as some dot.com firms have failed, their databases of personal records are among the assets that can be sold off to pay creditors. So, for instance, when in 2000 a defunct company called ToySmart.com tried to sell its personal data they were challenged, and obliged to sell only the entire website, and only to a related company (Stellin 2000). Other cases may not come to light, or may be less clear cut. Again, there are both technical and legal limits to this in most jurisdictions (Flaherty 1989, Bennett, 1992) but this does not mean that the leaky containers will suddenly stop data seeping from one to the other.

One of the key characteristics of what Manuel Castells calls the 'network society' is precisely that it is a 'space of flows' (Castells 1996: 412). Along with the nodes and hubs in the system, dominant groups determine how and in what interests the material infrastructure operates. Among the sequences of exchange and interaction that form the flows are surveillance data, risk communication and personal information, and they, no less than any other flows, circulate according to logics embedded in asymmetries of organizational power. Concrete examples of this are offered by Norris and Armstrong (1999: 8) in discussing closed circuit television (CCTV). Soccer stadia are under the camera's eye to check for (likely signs of) disorder, workplaces are watched to ensure compliance with health and safety regulations, and city centres are monitored to create and maintain ideal conditions for consumption. Differing dominant groups ensure the dispersal of discipline and its undulating, shifting quality as different sectional interests each play their part.

One outcome of this that should not be overlooked is that so-called information societies are thus by their very constitution also surveillance societies. Surveillance societies are not an accidental or malevolent result of perverse developments within information societies. Information societies – or, perhaps better, network societies (Castells 1998) – in which advanced electronics-based information infrastructures are a central means of co-ordination and exchange, operate by means, among other things, of advanced surveillance operations. But they are not necessarily *maximum* surveillance societies, the possibility of which George Orwell worried about, and James Rule analysed sociologically back in the 1970s. While totalitarian potential is always present, particularly in regimes that already exhibit such tendencies, the more subtle development of surveillance power is more likely.

As understood here, surveillance societies are not characterized by a single all-embracing and all-penetrating system, which is what Orwell feared above all. As Norris and Armstrong say of camera surveillance, 'CCTV has been implemented not as one pervasive system but as a series of discrete, localised systems run by a myriad of different organizations rather than a single state monolith' (Norris and Armstrong 1999: 7). The fact that there is no single all-embracing system is no call for complacency, however. The system – or, perhaps better, 'assemblage' (Haggerty and Ericson 2000) – expands and mutates constantly. It is augmented not only within hierarchical organizations of the sort that depict Big Brother overseeing all from the apex or the Panopticon inspector gazing out from the tower, but also, more frequently, within networks that spread horizontally, reaching out here, contracting there, but always finding more ways of seeking and processing personal data with a view to management and influence.

WHY DOES SURVEILLANCE MATTER?

Earlier I proposed that surveillance has become a significant means of governance, and of the reinforcing of social difference, and that is why the issues are important. I do not wish to downplay the fears of those who may feel that their privacy may be impugned or invaded by new kinds of surveillance technologies. They are real fears and deserve to be addressed, but to consider only personal fears about privacy distracts us from the public issues surrounding surveillance (Regan 1995). By suggesting that surveillance has become a means of governance, I mean that it serves to organize social relationships and contributes to patterns of social ordering. It does so largely through what Michel Foucault called biopower, making people up by classifying them according to categories. In the world of surveillance, such categories relate both to risk and to opportunity. Either way, what is statistically or organizationally normal becomes the touchstone of what is right or at least appropriate (Hacking 1990).

Categorizing is an ancient process but became crucial to the rationalized social organization of modernity. Through social convention and custom people accept their place within the hierarchy or learn to see themselves in relation to the status of others. What happens when traditional lines of authority and relationship are dismantled, to be replaced by bureaucratic rules and organizational practices? These too, are eventually accepted, even though they may now be seen as much more mutable. Who says so? Is the query heard in the democratizing situations of the twentieth century, from parliament to labour union to high school? But such queries were arguably much more common in situations where face-to-face interaction still predominated. As the body disappears from integrative social relationships, and is replaced by abstract tokens, so the categories too become more abstract and actuarial, and thus apparently benign. When information scientists design, delegate and choose classification systems they seldom see them as ‘embodying moral and aesthetic choices that in turn craft people’s identities, aspirations, and dignity’ (Bowker and Star 1999: 4). But as Suchman pithily notes, ‘categories have politics’ (1994).

The massive systems of computer-assisted classification that have been developed over the past thirty years are the taken-for-granted infrastructure of informational societies. They represent a concatenation of standards, practices and codes that are more or less interconnected, such that – in the case of the surveillance classifications considered here – personal and population data flows constantly through the nodes and hubs of the network. Though obvious asymmetries of power exist, no one person or body is in charge of surveillance systems; no one person or body can change them. Yet, they help to make us up, to naturalize us to the institutions and agencies that invent and elaborate the categories. And they help to create the sense of who and what is rightly included and excluded; who is this, that, or other (Bourdieu 1984: 470–8) Of course, it is an empirical question as to how far and under what conditions people accept as their own the categories in which they are placed by contemporary surveillance systems (Jenkins 2000). This is a reflexive process. But the history of medical, moral, criminal and consumer categorization suggests that plenty of people accept such labels and live likewise.

Let me make this clear. I am not suggesting that classification and surveillance are socially negative processes. They are necessary aspects of all social situations and serve social purposes, from the vital to the vicious. The point is that as powerful means of governance, of social ordering, they are also increasingly invisible and easily taken-for granted. The risk management (and other) classifications of surveillance societies involve categories that are inherently political, that call for ethical inspection. I am not suggesting either that such classifications are each powerful in the same way. Surveillance as understood here exists on a long continuum along which data is collected and processed for a range of purposes from policing and security to consumption and entertainment. It produces categorical suspicion at one end (such as ethnic profiling at airport security checks) and categorical seduction (such as targeting of potential car rental customers from lists of airline loyalty club members) at the other. Cities are increasingly splintered into socio-economically divided consumption and security enclaves by these practices (Graham and Marvin 2001). But either way, the categories have ethics; the codes have politics.

This, then, is why surveillance matters. It does indeed provoke privacy concerns from time to time. But, as expressed, these personal concerns are frequently temporary and contingent ones, often relating to mistakes and errors in databases or telecommunications systems, or to loss of access to the tokens of trust such as credit cards or driver's licenses. They are not high on any political agenda. And when, for example, surveyed Internet users claim to care about online privacy, it turns out, paradoxically, that the very same persons key-in PINs and credit card numbers online! (*Washington Post* 2000) They want the benefits of e-commerce even if they also want assurances that their personal details are secure and not being used for purposes beyond the immediate transaction. When it comes to legal restrictions on surveillance, whether construed as data protection or as privacy laws, it is usually the data-subject who has to make an appeal. The law only acts as a guarantee of some right to self-protection. This is why legal limits, though not insignificant, scarcely scratch the surface of the social issues raised by rapidly rising surveillance levels in everyday life.

Take the matter of voting in elections, for example. Over recent decades, the influence of television on the electoral process has frequently been noted. The whole public discourse of politics has been shaped by the perceived need for politicians to become sound byte 'personalities' in an attempt to influence the electorate. But the success of systems such as database marketing has spurred new ways of obtaining support, not least through profiling of individuals likely to give donations. The American consulting firm Aristotle International uses public sources such as motor vehicle registrations, the Postal Service and Census Bureau to obtain data on a person's age, sex, telephone number, estimated income, ethnicity, home ownership and party affiliation. It also records makes and models of cars owned, employer and occupation, whether or not they are campaign donors and how often they vote (*The New York Times* 2000). These data are manipulated to extract individual profiles of likely targets.

The above example makes no explicit use of the Internet (though it is not inconceivable that it might wish to), and refers only to personal data that are already publicly available. Moreover, activities such as this in Canada would not be touched by existing legislation (except possibly in Quebec), and it is not clear either that they would be covered by the *Personal Information Protection and Electronic Documents Act* that began to come into force on 1 January 2001. While some persons may wish to object that their voting activities are private – and after all, modern democracies have as a cardinal doctrine the idea of the secret ballot – it is also the case that persons are thus classified and categorized for particular purposes with which they may not agree. Granting or denying consent does not at present enter into data-gathering equations such as this, even though the consequences – for the dissemination of political information and for balanced awareness of alternative policies – may be far reaching. Privacy is one issue; discrimination is another (Gandy 1995).

WHAT CAN BE DONE ABOUT SURVEILLANCE?

It would make sense if some social practices and technological systems that affect everyone were also understood and actively negotiated by everyone. Such is not the case. All too often, convenience and efficiency are all that get noticed in systems that have surveillance aspects, with the result that data subjects are often unaware of the broader discriminatory and classificatory dimensions of such systems. Data protection and privacy policy and legislation have made significant strides in recent decades, even though in some cases they may be minimalist and even cynical. Data protection and privacy remain vital concerns, even if their impact on the negative aspects of social categorization does not yet amount to much. On the other hand, what I refer to as minimalism would be seen in rules that allow only for a right of self-protection, and cynicism may be evident in cases where laws have been enacted in order to facilitate business with a trading partner rather than out of actual concern with the effects on the lives and prospects of data-subjects.

At the same time, surveillance does not simply go on behind people's backs. We participate in and actively – though not always consciously – trigger the data-capture by making telephone calls, using credit cards, passing our hands over entry scanners, claiming benefits, walking down the camera-watched street, surfing the 'net, and so on. Not enough is known about how people in everyday life comply with, negotiate and resist surveillance. But it is clear that workers are cautious if not negative about some electronic devices such as video, audio and computer-use monitoring, not to mention the use of biometric and genetic checks and screens. People using public spaces such as streets and private ones such as shopping malls are aware of and avoid or play up to closed circuit television systems and video surveillance. Users of Web-based e-mail accounts and online shoppers are often wary of divulging personal data, when requested to do so, especially when those data seem to have little to do with the immediate transaction in question. They are aware that some other data image of them circulates in cyberspace and may well accept this as the price paid for some benefit or reward.

But it is not enough to assume that over time people will somehow 'get wise to' mushrooming surveillance systems. Such systems are a largely uninspected and unregulated means of social classification, of social ordering. They affect people's chances and their choices, and as such demand to be recognized. Beyond this, their growth calls for ethical scrutiny and democratic involvement. Of course, there is an ambiguity to all such systems. Of course, surveillance exhibits more than one face. But the face that is publicized is that of the smoothly running organization, the rapid response to consumer demands or to security calls, the flexibility of the management structure, and not the negative and possibly undesirable aspects of personal data processing. The discriminatory power of contemporary surveillance is wielded by large organizations that have strong interests in valuable personal data. The persons from whom such data are abstracted face a built-in disadvantage in this respect.

Various kinds of responses to surveillance have emerged over the past two or three decades. They may be thought of as regulative and mobilizing responses (Lyon 2001b: chapter 8). The first is seen most obviously in the various data protection and privacy laws that now exist in most countries dependent on information infrastructures. But it is also evident in a number of voluntary, market and technical remedies for what is most usually construed as threats to privacy. Voluntary measures include company-based adherence to fair information principles. Most banks and many website operators proactively offer details of their 'privacy policies' today. Market solutions include the growing idea of making personal data earn the equivalent of royalties, such that the data subject has a tangible return for the use of his or her abstracted data. Technical solutions are various, and often relate to security. The most publicized example is that of the electronic signature.

'Fair Information Principles' (that require those collecting data to use them only for the purposes stated and not for others, to obtain only that which is needed for their immediate purposes and to ensure that the data has been obtained with the knowledge and consent of the data subject, and so on) to which most privacy legislation makes reference, do not address directly the issue of the categorization carried out by surveillance systems. They depend, implicitly but importantly, on the idea that data-subjects may have an interest in controlling the flow of personal information about them. This relates to an ethically appropriate desire to disclose oneself to others only in a voluntary and limited way, and within relations of trust. And it must be said that such fair information practices, when installed, may well mitigate some negative effects of discriminatory categorization.

But fair information practices have no brief for ethically inspecting the categories in question, still less for examining how the combined force of multiple categorizations may have the effect of strictly restricting some people's life-chances and choices while at the same time opening doors of opportunity to others. This calls for an approach that goes beyond both liberal pleas for privacy and Marxist arguments about new forms of domination in informational capitalism. Although the first leads, at best, to legal protections, these often reduce to personal property rights over personal data. As for the second, while it rightly highlights asymmetries of informational power, it can easily downplay the role of technological mediations and the role of the subject. An ethical approach, which calls for democratic scrutiny of information systems, raises crucial issues of accountability, and proposes forms of immanent critique – from within informational culture (Lyon 2001c).

Mobilizing responses, on the other hand, have grown in number and volume since the 1980's. Non-government groups and consumer movements have attempted to get to grips with the realities of the rhizomic expansion of surveillance. They may take the form of organized protest or watchdog groups – such as Privacy International or the Electronic Privacy Information Center – or *ad hoc* responses to specific issues. Thus, attempts to create an electronic 'Australia Card' for all citizens in the mid-1980s spawned a social movement that successfully turned down the proposal, as did similar, later attempts in South Korea. Campaigns have also been mounted against specific firms and products such as the Lotus 'Marketplace: Households' software in 1994, or the Intel Pentium III chip with its unique identifier for all computers, in 1999. The use of the Internet to mobilize resistance is an important part of the process.

These mobilizing responses may point the way to new modes of negotiating and resisting negatively construed aspects of surveillance in the twenty-first century. It is the codes, both symbolic and electronically inscribed, that provide the means for surveillance power to flow. As Deleuze (1986) argues, physical barriers and constraint within places matter less today than the codes that enable and disable, admit and exclude, accredit or discredit. Audio-visual and digital protocols permit entry and movement in the city, rather than the old city gates that made the physical container so significant (Virilio 1997: 383). As Melucci (1996) observes, social movements today are increasingly concerned with perceiving risks and identifying them as public issues, with a process of 'challenging codes'. He argues that as everyday concerns about personal identification and life-chances become more obviously set against global flows of data and of power, new kinds of oppositional politics will emerge, appropriate to the 'information age'.

Having said that it remains true that processes associated with communication and information technologies are still regarded in rather a rosy light. Much hype surrounds the development of the Internet, and the networked world in general. But the genuine benefits gleaned from having surveillance systems in place tend to deflect attention away from the inequities associated with many discriminatory dimensions of surveillance. And some technologies simply fare better than others in the public eye do. Whereas biotechology may be construed as 'tampering with the human body', information technologies seldom receive equally negative responses for their capacity either to 'tamper with the mind' or – still less – to produce subtle mechanisms of social ordering (Nelkin 1995). It may turn out, of course, that as more biometric and genetic forms of surveillance become prevalent, that broader questions will be raised about the classificatory power of today's codes.

The question, 'what can be done?' may thus be answered practically rather than abstractly. Many responses to surveillance have emerged and are emerging, as I suggested above, this is entirely appropriate given the increasing monitoring of everyday life. While the lead, in some instances, may be taken by legal initiatives, other responses are also called for, at many levels. The law, at best, can only help to create a culture of carefulness about the processing of personal data, it cannot possibly speak to all issues, let alone keep up with each development in data mining, profiling, database targeting and marketing, locational tracking of vehicles or cellphones, and so on.

Conspiratorial and paranoid responses are counter-productive, not least because negative aspects of surveillance often arise as unintended consequences or by-products of other acceptable or unquestionable processes of risk management or marketing. They are also inappropriate to situations of networked, rhizomic surveillance, where no panoptic inspection tower and no omnipotent Big Brother exists. Rather, constant vigilance on the part of government departments, companies, advocacy and consumer groups, and ordinary users and citizens is called for, especially in light of the panic regimes consequent on the terrorist attacks of 11 September 2001. Focused ethical attention, along with serious proposals for democratic accountability, and educational and awareness-raising initiatives, are needed if everyday surveillance is properly to be understood, and when necessary, confronted and challenged.

David Lyon
Queen's University
Ontario, Canada
lyond@post.queensu.ca

REFERENCES

Bennett, C. (1992) *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca: Cornell University Press.

Bourdieu, P. (1984) *Distinction: A Social Critique of the Judgement of Taste*, London and New York: Routledge.

Bowker, G. and Star, S. L. (1999) *Sorting Things Out: Classification and its Consequences*, Cambridge, MA: MIT Press.

Brown, J. S. and Duguid, P. (2000) *The Social Life of Information*, Boston, MA: Harvard Business School Press.

Castells, M. (1996) *The Rise of the Network Society*, Oxford and Malden, MA: Blackwell.

Castells, M. (1998) 'Materials for an exploratory theory of the network society', *British Journal of Sociology*, 51(1): 5–24.

Dandeker, C. (1990) *Surveillance, Power, and Modernity*, Cambridge: Polity Press.

Deleuze, G. (1986) 'Postscript on the societies of control', *October*, 59: 3–7.

Ericson, R. V. and Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.

Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies*, Chapel Hill: University of North Carolina Press.

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

Gandy, O. H. (1995) 'It's discrimination, stupid!' In J. Brook and I. A. Boal (eds) *Resisting the Virtual Life: The Culture and Politics of Information*, San Francisco: City Lights, pp. 35–47.

Graham, S. and Marvin, S. (2001) *Splintering Urbanism: Networked Infrastructures, Technological Mobilities, and the Urban Condition*, London and New York: Routledge.

Hacking, I. (1990) *The Taming of Chance*, Cambridge, New York and Melbourne: Cambridge University Press.

Haggerty, K. and Ericson, R. V. (2000) 'The surveillant assemblage', *British Journal of Sociology*, 51(4): 605–22.

Jenkins, R. (2000) 'Categorization: Identity, social process, and epistemology', *Current Sociology*, 48(3): 7–25.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*, New York: Basic Books.

Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society*, Cambridge: Polity Press; Malden MA: Blackwell.

Lyon, D. (1997) 'Cyberspace sociality: Controversies over computer-mediated communication', in B. Loader (ed.) *The Governance of Cyberspace*, London and New York: Routledge, pp. 23–37.

Lyon, D. (2001a) 'Surveillance after September 11 2001', *Sociological Research Online*, 6(3). Available online: www.socresonline.org.uk

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

Lyon, D. (2001c) 'Facing the future: Seeking ethics for everyday surveillance', *Information Technology and Ethics*, pp. 171–81.

Marvin, C. (1988) *When Old Technologies were New*, Oxford and New York: Oxford University Press.

Melucci, A. (1996) *Challenging Codes: Collective Action in the Information Age*, Cambridge, New York and Melbourne: Cambridge University Press.

Nelkin, D. (1995) 'Forms of intrusion: comparing resistance to information technology and biotechnology in America', in M. Bauer (ed.) *Resistance to New Technology*, Cambridge, New York and Melbourne: Cambridge University Press.

The New York Times (2000) 'One consulting firm finds voter data is hot property', *The New York Times*, 9 September.

Nock, S. L. (1993) *The Costs of Privacy: Surveillance and Reputation in America*, New York: Walter de Gruyter.

Norris, C, and Armstrong, G. (1999) *The Maximum Surveillance Society: The Rise of CCTV*, London: Berg.

Regan, P. (1995) *Legislating Privacy: Technology, Surveillance, and Public Policy*, Chapel Hill: University of North Carolina Press.

Rose, N. (1999) *Powers of Freedom: Reframing Political Thought*, Cambridge, New York and Melbourne: Cambridge University Press.

Rule, J. (1973) *Private Lives, Public Surveillance*, Harmondsworth: Allen-Lane.

Slevin, J. (2000) *The Internet and Society*, Cambridge: Polity Press.

Staples, W. G. (2000) *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, Lanham MD: Rowman and Littlefield.

Stellin, S. (2000) 'Dot-com liquidations put consumer data in limbo', *The New York Times*, 4 December.

Strange, S. (1996) *The Retreat of the State: The Diffusion of Power in the World Economy*, Cambridge, New York and Melbourne: Cambridge University Press.

Suchman, L. (1994) Do categories have politics? The language/interaction perspective reconsidered, *Computer-Supported Cooperative Work*, 2: 177–90.

Thompson, J. (1995) *The Media and Modernity*, Cambridge: Polity Press.

Torpey, J. (2000) *The Invention of the Passport: Surveillance, Citizenship, and the State*, Cambridge, New York and Melbourne: Cambridge University Press.

Verma, S. (1999) 'Police double crime "hot-spot" targets', *The Toronto Star*, 23 July.

Washington Post (2000) 'Internet users seek assurances over on-line use of personal data', *Washington Post*, 20 August. Available online: http://washingtonpost.com/wp-dyn/articles/A60984-2000Aug20.html>

Virilio, P. (1991) The overexposed city, in *Lost Dimension*, New York: Semiotext (e), pp. 9–27.

Whittington, L. and Harper, T. (2001) 'Ottawa to boost terror laws', *The Toronto Star*, 23 November.