

Part E: Postscript following the Conference of Privacy Commissioners

Kirstie Ball
David Murakami Wood
Charles Raab

1. Introduction

- 1.1. In the preceding pages we have outlined the origins, nature, controversies and questions surrounding the surveillance society. We have portrayed it in its current state, and speculated as to what the surveillance society may look like in the future. We have also outlined how regulation of the surveillance society may develop using current regulatory tools and instruments as a starting point.
- 1.2. This Report was presented as the main theme of the 28th International Conference of Data Protection and Privacy Commissioners in London, 2-3 November 2006. This is the largest and most inclusive conference of Commissioners held anywhere in the world. It is an important annual event in which the previous year's developments, current issues, and special topics are aired in formal and informal sessions, with a participatory audience of several hundred persons drawn from the regulatory world of Commissioners, from government and industry, from civil-society groups with an interest in privacy issues, and from the academic world. The Conference provided a unique occasion to orient discussions around a central theme and focus of attention, embodied in the Surveillance Society Report, which was specially written for this occasion. A Summary Report was circulated to delegates, and the full Report, its Appendices and the Public Discussion Document were available on the UK Information Commissioner's website. This also included translations of the Summary Report and Public Discussion document into French, German and Spanish.
- 1.3. The choice of surveillance as the centrepiece of this authoritative Conference gained the topic and the Report a great deal of attention in the print, radio and television media of a large number of countries and in many languages. News of the Report and its discussion in the Conference rapidly spread globally via the Internet through its news resources and through more specialised sites and discussion groups. The topic of surveillance was put on the map, and has helped to focus attention and debate in a wide variety of circles. The Report itself has been widely read, and continues to be mentioned by speakers from platforms, with the issues it raised and its terminology appearing in news reports of surveillance issues as they arise.
- 1.4. The purpose of this final chapter is to give a short, general account of the Conference proceedings that involved the Report and that added new perspectives

and commentary on its themes and issues. It constitutes a distillation of formal presentations and of their discussion among participants, both from the floor of the Conference and in special panels that looked at various facets of surveillance and its regulation. It is not intended as a review of the speakers' presentations or as an account of the give-and-take of discussion sessions. Its main aim is to focus further attention on a small number of issues, in order to assist in the further deliberations and debate that the Report and the Conference aimed to stimulate.

- 1.5. This chapter has been written five months after the Conference, and some seven months since the Report was completed in September 2006. The authors have not revised the Report for this April 2007 complete publication. Although surveillance technologies, practices and policies change rapidly, we believe that the expertise and analysis contained in the Report and its Appendices are not outdated and remain valid.

2. Emergent Themes

- 2.1. Five major themes arose from the Conference proceedings, intersecting with those raised in the Report. These were among those to be found in the Report and that also featured in the presentations and panel contributions given by Commissioners and by a large number of others who spoke from the platform or from the floor. To some extent, the themes reflect the different constituencies or stakeholders of the surveillance society: national and international government, policy and law, the private sector, technology, society and the individual, and human rights groups. These themes are identified as follows:

- The relative roles of the public and private sectors in conducting surveillance
- Differing views of the person who is subjected to surveillance
- The variable effects of technology
- Trust and privacy
- The protection of human rights through law and regulatory action.

- 2.2. These themes overlap to a large extent, but the main lines can be summarised and commented on sequentially; for convenience, they are presented again in Table 1 later on in this chapter:

2.3. *The relative roles of the public and private sectors in conducting surveillance*

- 2.3.1. This was a major theme in the Report. In the conference, it emerged from debates that reflected the contrasting roles of the private and public sector as they conduct surveillance. It is clear that the purpose of surveillance as it occurs in these different contexts is also different. The discussion covered the following range of scenarios, where:

- There is total or strong government surveillance of all private entities (individuals, groups and organisations) because they are seen as a security risk;
- The public and private sector collaborate in the delivery of services, which involves the surveillance of citizens/consumers in relation to the consumption and use of those services;
- The public sector uses a variety of instruments to regulate the private sector in the surveillance of individuals in their everyday lives (e.g. as consumers, workers or travellers).

2.3.2. Some speakers flagged up the dangers of a totalitarian state, in part by describing and reflecting on surveillance and its aftermath in political systems where massive and detailed amounts of personal data were gathered by state authorities through a variety of techniques. These techniques included the widespread use of informers in order to keep watch on and intimidate civilian populations and groups.

2.3.3. In other, more democratic settings, states are now prone to engage in systematic surveillance for counter-terrorist, law-enforcement and public-order purposes, but also to undertake more pragmatic and sometimes haphazard surveillance practices for reasons of government efficiency, productivity, or the provision of public services. The dilemma is how to reconcile the legitimate need for information collected through surveillance and other data-collection practices with the legal and good-practice requirements of privacy protection. The latter is under strain in today's world, and there is often strong public opinion that supports the invasion of privacy in order to achieve other policy objectives and consumer benefits, as well as public security. There are a host of issues that reflect the tension: these include data retention, governments' demands that the private sector hand over databases, and difficulties in controlling or penalising private-sector violations of privacy.

2.4. *Differing views of the person who is subjected to surveillance*

2.4.1. The Report acknowledges that different kinds of surveillance feature in different areas of everyday life, and it became clear through the course of the Conference that there were different views of who the surveillance subject was in terms of their constitutional status and propensity for action in relation to surveillance. The range of views depicted individuals as:

- Compliant, paranoid and powerless, with few rights and no voice to challenge or question surveillance;
- Rational - economic utilitarians who will trade privacy for short term economic benefit and are unconcerned or have a limited interest in the consequences of surveillance for them;
- Active, concerned citizens who are willing to participate in debate about surveillance and its consequences.

2.4.2. Much of the discussion of this concerned first, the relationship between the individual citizen and a conception of the public interest and, second, how people weigh up the pros and cons of surveillance; indeed, whether they do so at all. Views on this were intertwined with those on the first theme, insofar as the tensions in policy reflect differing priorities given to privacy protection and surveillance requirements as they bear upon persons.

2.4.3. It is considered to be somewhat puzzling that so much of the public themselves are not more interested in surveillance activities that affect them, whilst there is at the same time a very high concern about privacy, as shown in survey research. On the other hand, many people are unaware of surveillance and of the threats it poses to human rights, privacy and other values and interests such as human dignity, and only see the consumption-related opportunities and benefits that they think are on offer. Many are, understandably, driven by fears of crime, terrorism and public disorder to accept encroachments on civil liberties: at certain points in the conference this was

explicitly referred to as surveillance which had a ‘strong’ public-interest element.

2.4.4. Public discourse about surveillance needs improvement and enlightenment, and issues such as the proportionality of surveillance need to be debated. The image of the frog being slowly boiled to death without realising was used by speakers to warn against the effects of stealthy, creeping encroachment on liberties before it becomes too late to react effectively.

2.4.5. It was observed that a lack of democratic participation in deciding on these issues courted the danger of slipping into excessive and unaccountable surveillance practices. Greater transparency, consultation, and a non-paternalistic approach were important for governments. Whilst government, and the private sector too, rely on the fact that many citizens are compliant and unquestioning in the face of demands for personal data and for enhanced surveillance, others actively seek further knowledge about what happens to their data in commercial and governmental transactions, and still others demand fuller participation and better transparency.

2.5. *The variable effects of technology*

2.5.1. From its outset, the Report highlights the pitfalls of treating surveillance as merely a technological issue, and the problems of treating surveillance as a simple matter of technological efficiency and effectiveness. Indeed, a major section of the Report focused on the limitations of technology and the dangers of using this as a rationale for more surveillance.

2.5.2. Appropriately, much of the discussion at the Conference, as highlighted in the previous two sections, concentrated on the importance of context in configuring surveillance practice, and hence contributing to its complexity. Only one of the speakers devoted the entirety of a talk to technology *per se*, although questions arose from the floor that concerned the collection and treatment of personal data during data-mining, drug testing and internet browsing. Discussion concerning technology covered the following areas:

- The transparency of data collection, particularly in relation to personal data-collection features embedded in web-browsing software;
- The extent of the ability of individuals to use technologies to protect themselves from surveillance or invasions of privacy;
- Data retention by search engines for new product development;
- The different configurations of surveillance based on different kinds of technology and their functionality.

2.5.3. The main discussion of this centred on the different ways that surveillance technologies operated. One speaker explained that some have to do with connection (e.g., moving data around; the use of RFID chips), and others concern disconnection (e.g., control of access to data; the use of biometrics and smart cards). A third way is processing (e.g., collection and storage of data).¹

2.5.4. There were different scenarios arising from these. One is ‘big brother’, in which technologies of connection dominate, and people are tracked and

¹ These findings and in the paragraphs following are reflected in: Royal Academy of Engineering (RAE) (2007) *Dilemmas of Privacy and Surveillance*. London: RAE.

monitored, not only when they are considered to be a threat but also as a matter of course. A second scenario, 'little sister', is where disconnection dominates, personal identity is fragmented, and the effects are less invasive. Where collection dominates, as in a third scenario, there is 'big mess' of multiple agencies collecting information on many people in many contexts.

2.5.5. It was argued that advances in technology will create dilemmas and trade-offs between different groups and interests. Some combination of these scenarios will prevail in the future, with implications for surveillance and its regulation. It was felt to be important to design the dangers out of these systems, and there is an important role for regulation and for placing requirements on technology suppliers. There are also regulatory alternatives, as between centralised and decentralised modes, although these, it was said, could be complementary within an overarching framework of controls.

2.5.6. But an important socio-technical problem is the growing division between those who have the means to enable them to mitigate the effects of surveillance practices and technologies on themselves, and those who are unable to and are therefore exposed to its most invasive and discriminatory effects. The latter point reflects a conclusion from the future scenarios in the Report: that there is an emerging political economy of personal information, with an uneven distribution of advantages and disadvantages across society.

2.6. *Trust and privacy*

2.6.1. A key contention in the introduction to this Report is that a society which relies on surveillance for governance may be committing slow social suicide. This is because a reliance on surveillance in any setting sends messages to the people within that setting that they cannot be trusted, which has knock-on effects for the way in which social relations and privacy are constituted. Very little empirical evidence exists which examines this point, although a range of views were expressed, as follows:

- Totalitarian societies are characterised by low public and interpersonal trust, with little privacy for individuals;
- In consumer-oriented societies, privacy is something to be exchanged for economic benefit, with limited trust formed around economic transactions with organizations and government;
- In an ideal-typical democratic state in which citizens participate more fully, data collection, though often necessary and beneficial, is transparent and privacy rights are fundamental; trust relations were assumed to improve.

2.6.2. Several speakers and participants emphasised the importance of trust, and trustworthy relationships, as a currency that sustained society, commerce and government. Trust has long been acknowledged to be a crucial dimension in the relationship between citizens and governments as well as in private-sector transactions, but levels of trust within democratic and market-based societies appear to have declined.

2.6.3. We have the baleful example of totalitarian states to use as a contrast, but also as a warning. Those countries were low on trust between the state and the public, but also among members of the public themselves, largely owing to the excesses and secrecy of surveillance and its apparatuses. But, following the downfall of most totalitarian states, particularly those in eastern Europe and the

former Soviet Union, there remained dilemmas of privacy, trust and social relationships, that now concern how far the contents of secret-police files should be made available to the public or to individual victims of surveillance, and how far former victims, perpetrators and their families need protection. These issues are very current in post-reunification Germany, for example.

2.6.4. In other democratic societies, technologically-based systems like CCTV operate without a network of informers, but contribute to a decline of trust: for example, the state builds up a picture of a citizen's identity and distrusts the citizen's own view of her identity. Yet in these democratic societies, safeguards placed on data-collection and other forms of surveillance were said to be essential for a level of trust sufficient to sustain transactions between citizens and the public services or in commercial dealings. Although research has been conducted on levels of public trust in government, what is needed is greater understanding of the sociology of surveillance in totalitarian societies, in order to avoid its effects in our own type of society.

2.7. *The protection of human rights through law and regulatory action*

2.7.1. The final section of the Report concerned regulatory issues surrounding the surveillance society and how they compared to the regulation of privacy. As information and privacy Commissioners are in the front line of protection against privacy invasions and the harmful effects of surveillance in societies governed by the rule of law, it was to be expected that the response, as well as the proactive work, of regulatory agencies in the face of threats arising from surveillance would loom large in the Conference. A range of viewpoints were presented which concerned:

- When it is appropriate to apply centralised, paternalistic and security-based surveillance, given its impact on rights and difficulties associated with its regulation;
- The difficulties of regulating surveillance and privacy when issues of public interest and the meaning of 'privacy' are nebulous;
- Engaging the public in debate about regulation and rights under surveillance.

2.7.2. Several speakers addressed the question of human rights under the European Convention and in national laws, pointing out that the right to privacy, which is fundamental but not absolute, could be overridden under certain circumstances. There were some court cases that arbitrated these matters, but the decisions went both ways.

2.7.3. Some speakers and panels concentrated on the range of controls that could be applied to protect privacy and mitigate the effects of surveillance. Law is one of the most important of these instruments, but it is not alone, and there are concerns about its effectiveness in the face of technological developments, public policies and commercial interests, and flows of personal data across jurisdictional boundaries.

2.7.4. The role of supervisory authorities such as Commissioners is seen as crucial, but their powers vary, as do their activities and their courageous resolve to safeguard individual and social freedoms. They need to work with those they regulate in order to find better solutions, but this was difficult in the contemporary post-9/11 context and in the face of other pressing policy

imperatives. Well-established data protection principles need to be applied as far as possible to new technologies, and Commissioners need to innovate strategies and approaches, not simply adhering to the traditional, and suspect, doctrine of finding a ‘balance’ between surveillance and human rights.

2.7.5. One possible way forward might be the implementation of privacy impact assessment, extended also to consider the effects of surveillance on other social values beyond privacy itself.

2.8. *Summary of this Section*

2.8.1. In many senses the proceedings of the 28th International Conference of Privacy and Data Protection Commissioners repositioned privacy and data protection in a wider context, and the preceding analysis has suggested. This context highlights the wider effects that information processes involving personal data have on individual and social rights, freedoms and life-chances, and on the consequences for democratic societies. This takes the work of regulators, and of supportive civil-society groups, academia and the media, into the realm of considerations other than privacy itself, and in this sense the Conference may have broken new and unfamiliar ground in a direction to which regulators are increasingly called upon to incorporate into their remit. Understanding the dimensions of surveillance, both in the technological and in other ramifications, is one of the first steps on the road.

2.8.2. The legitimacy as well as the practical feasibility of taking further steps, and of expanding the role of Commissioners and their relationships with society, may be debated in different ways in different jurisdictions, with different outcomes. But the Conference had an atmosphere of serious application to the pros and cons of surveillance and to a consideration of their implications for practitioners, so that any subsequent debate, amongst regulators, between them and others, and among the general public, is likely to have benefited from the Report and the exposure it enjoyed in the media.

2.8.3. It was very valuable to have participants from a very wide variety of countries, and with diverse policy, social and economic interests, come together to devote their attention to some of the most important issues of our time. Whilst it might be tempting to speculate as to whether the views expressed in the Conference form a coherent set of perspectives which reflect the positions of participants in industry, state, or civil society, we prefer to summarise the views expressed under each theme more simply in table 1, below.

The relative roles of the public and private sectors in conducting surveillance
<ul style="list-style-type: none"> • There is total or strong government surveillance of all private entities (individuals, groups and organizations) where they are seen as a security risk
<ul style="list-style-type: none"> • The public and private sector collaborate in the delivery of services, which involves the surveillance of citizens/consumers in relation to the consumption and use of those services. The market is the object of surveillance
<ul style="list-style-type: none"> • The public sector uses a variety of instruments to regulate the private sector in the surveillance of individuals in their everyday lives (e.g. as consumers, workers or travellers)
Differing views of the person who is subjected to surveillance
<ul style="list-style-type: none"> • The person is compliant, paranoid and powerless, with few rights and no voice to challenge or question surveillance
<ul style="list-style-type: none"> • The person is a rational - economic utilitarian who trades privacy for short term economic benefit and has a limited interest in the consequences of surveillance for them.
<ul style="list-style-type: none"> • The person is an active concerned citizen who is willing to participate in debate about surveillance and its consequences
The variable effects of technology
<ul style="list-style-type: none"> • There are issues around the transparency of data collection, particularly in relation to personal data collection features embedded in web browsing software
<ul style="list-style-type: none"> • There are questions around the ability of individuals to use technologies to protect themselves from surveillance or invasions of privacy
<ul style="list-style-type: none"> • There are questions over data retention by search engines for new product development
<ul style="list-style-type: none"> • There are different configurations of surveillance based on different kinds of technology and their functionality which raise contrasting regulatory issues
Trust and privacy
<ul style="list-style-type: none"> • Totalitarian societies are characterised by low public and interpersonal trust, with little privacy for individuals
<ul style="list-style-type: none"> • In consumer-oriented societies privacy is something to be exchanged for economic benefit, with limited trust formed around economic transactions with organizations and government.
<ul style="list-style-type: none"> • In an ideal-typical democratic state in which citizens participate more fully, data collection is transparent and privacy rights are absolute, trust relations were assumed to improve.
The protection of human rights through law and regulatory action
<ul style="list-style-type: none"> • Is it ever appropriate to apply centralised, paternalistic and security based surveillance, given its impact on rights and difficulties associated with its regulation.
<ul style="list-style-type: none"> • There are difficulties of regulating surveillance and privacy when issues of public interest are nebulous
<ul style="list-style-type: none"> • It is a challenge to engage the public in debate about regulation and rights under surveillance

Table 1: Summary of themes and perspectives

3. What was missing from the Conference

3.1. Whilst the range of the presentations and discussion at the Conference were broad and covered diverse viewpoints, there were a number of important areas considered in the Report that were not the subject of much debate and upon which delegates and readers of this Report may like to reflect in more detail. These will be considered under the headings of the original report:

3.2. *Social context (Section 8)*

3.2.1. The important social and political contexts through which the surveillance society has emerged were not the subject of significant debate. This is not surprising, given the pragmatic focus of delegates whose engagement with these issues occurs to a large extent at the interface of the law and society.

3.2.2. Of the four major trends we identified, only the idea of a personal information economy was considered at any length. In contrast, given far less attention were: the effects of a societal and governmental obsession with risk and fear (as opposed to more positive rationales for policy development and regulation); the militarization of aspects of civil society by the employment of certain surveillance systems and tactics; and the growing economic and political power of the security and surveillance industries.

3.2.3. Whilst regulators may legitimately regard many of these as outside their remit, the possibility of more positive and proactive activities by regulators to counter the dominance of 'fear' as a driver of policy, practice and public attitudes might be a worthwhile recommendation.

3.3. *Technology (Section 9)*

3.3.1. Many technologies and technological developments were mentioned during the Conference in most of the areas that the Report identified. However, it is fair to say that the predominant leaning of most speakers and discussants was towards a practical concern with the dangers of abuse of technologies rather than the problematic politics and social effects of the technologies, both in themselves and as embedded in social and economic systems.

3.3.2. The dangers of technological lock-in, particularly in the context of the many governments current drive to privatise or semi-privatise state service-delivery functions was therefore perhaps underappreciated despite being acknowledged. There was also a tendency in some discussions to favour fashionable and economically buoyant areas of concern to the 'technorati', i.e., privacy and liberty on the Internet, ahead of the majority of more basic technologies involved in surveillance for the vast majority of everyday interactions.

3.4. *Surveillance Processes (Section 10)*

3.4.1. Given the orientation of the Conference delegates, it is not surprising that the important issues of information-sharing and the attendant dangers of identity-theft, fraud and crime were much discussed. Whilst attention to these matters is to be welcomed, some of the more subtle and problematic aspects of contemporary surveillance processes were relatively neglected, and could be of interest in subsequent Conferences of this kind.

3.4.2. Social sorting and discriminatory profiling as an idea seemed to have a strong currency even if its full implications for the formation of new hierarchies, social class and racial divisions were undeveloped. We will return to this below. In addition, linked to the relative absence of concern for the problem of technological lock-in, the prospects for unintentional forms of social control to emerge from entirely 'logical' and efficient information flow-management were not considered in great detail, nor were some of the international surveillance processes involving intelligence organisations and the military.

3.5. *Social Consequences (Section 11)*

3.5.1. Again, in a conference of Privacy Commissioners, it is not surprising that privacy remained the key concern along with the consequences for accountability, transparency and rights conceived of in legal terms. However, there was notable agreement with the agenda of the Report to broaden the object of concern to autonomy, dignity and more complex social implications of surveillance.

3.5.2. It is also notable that certain categories of people, and certain domains of surveillance remained absent. In the first category are the main groups of people who constitute the 'experimental subjects' of many new forms of surveillance: immigrants, prisoners, the lower ranks of the armed forces; the ill; the elderly and children. Thus, as indicated above, 'social exclusion', although never far from the debate, remained as a rather abstract notion.

3.5.3. In the second category are all the places that such groups are to be found, but also in particular the world of work and the world of the home. Borders, shops, town centres and the Internet were all covered, but the increasing intensity of workplace surveillance and the reconfiguration of work practice to provide more easily surveillable environments and workers were ignored, as were the worlds of forced migration, sink housing estates and job centres and other grimy realities of daily life for too many people.

3.5.4. In these contexts, further important debate is necessary on how surveillance might serve to reinforce and extend social divisions even as it provides 'convenience' or 'safety' for the more affluent majority, and even as it helps to provide services and benefits to the surveilled themselves. In addition, the privacy and surveillance effects of emergent ubiquitous technologies, affecting the daily lives of everyone, deserve more debate by regulators.

4. Next Steps for Regulators

4.1. It is relevant to recapitulate and amplify the description, given under the fifth Emergent Theme (Section 47.7 above), of what was said about the future of regulation in the face of surveillance.

4.2. The history of privacy and data protection shows a multiplicity of regulatory instruments deployed in jurisdictions and internationally:

- Legal mechanisms are perhaps the key ones, but they are not self-implementing and they are insufficient. Moreover, there are concerns about

their effectiveness in the face of technological developments, certain kinds of public policy, new commercial endeavours, and flows of personal data across jurisdictional boundaries.

- The role of supervisory authorities such as Commissioners is crucial, but their powers vary, as do their activities and their willingness or ability to act vigorously to safeguard individual and social freedoms. Some countries do not have dedicated regulatory agencies at all, making it more difficult for citizens to have their privacy safeguarded. Commissioners need to continue to work with those they regulate, in both the private and the public sector (and in the increasing interpenetration of the two) in order to find better solutions.
- Codes of practice may have an important role to play, but not by themselves, and better ways need to be explored to make them more effective.
- Privacy-enhancing technologies are seen by many as powerful protectors, and even as substitutes for law. But whilst regulators might well promote their development and use, and governments might require their inclusion into procured information systems, their limitations, as well as their applicability to only certain domains of surveillance, need to be recognised.
- Regulatory regimes have an important part to play in maintaining trust between the public and those who use their personal data, often for individual and collective benefit. But protections against the disadvantages of surveillance is more difficult in the contemporary post-9/11 context and in the face of other pressing policy imperatives, and regulatory agencies realise that they must re-think their roles and strategies, for traditional solutions are of decreasing utility.

4.3. Nevertheless, there is much that Commissioners and their organisations, along with others, can do:

- They can redouble their efforts to affect public policy proposals at an early stage, to ensure that the privacy and surveillance dimensions are considered more seriously.
- They can suggest alternative solutions, minimising surveillance, to policy problems where governments might otherwise reach for invasive solutions.
- They can seek more effective legal powers and legal sanctions for the misuse of data.
- They can work more in collaboration with the media and with privacy and consumer pressure groups to raise the level of public awareness, and to warn against present and future dangers to human rights that flow from the excesses of surveillance.
- Well-established data protection or 'fair information' principles need to be applied as far as possible to new technologies, and Commissioners need to innovate decision-making strategies and approaches, not simply adhering to the traditional, and suspect, doctrine of finding a 'balance' between surveillance and human rights.
- They can try to investigate and report on the risks posed by new technologies, policies and practices. For this, one possible way forward might be the implementation of privacy impact assessment, extended – as the Report argues – to consider also the effects of surveillance on other social values beyond privacy itself, such as discrimination, social exclusion, and loss of autonomy and of dignity, mentioned in section 48 above. There are useful examples of privacy impact assessment, but the techniques need improvement as well as more widespread uses within and across countries.

- 4.4. The development of powerful, effective regulation cannot be the affair of single countries alone, or even of groupings such as the European Union, the Asia-Pacific Economic Co-operation countries, the OECD and the Council of Europe, even though these are widely acknowledged to have played often crucial roles in privacy and data protection. Increasingly, privacy protection is seen to require co-ordinated, and sometimes integrated, activity at a range of levels, from the local to the global. This will entail some re-orientation of roles and of ways of working so that threats of surveillance, which themselves operate at various levels, can be contained or prevented by protective regimes of comparable scale. With its experience of nearly thirty years, the grouping of the world's Data Protection and Privacy Commissioners could play an important strategic and co-ordinating role, and perhaps a decision-making role, in shaping the institutionalisation of such a regime at the highest level.
- 4.5. Finally, while data protection concerns the privacy of information, surveillance impacts upon other dimensions of privacy as well, including those associated with space and the body, especially with the advent of 'ambient intelligence' technologies and systems that are destined to loom large. Regulatory agencies and public policy may be called upon more insistently, in the future, to expand their role in those directions, as new technologies for information-gathering and controlling behaviour pose questions about the protection of human rights, of which privacy is one. Reconstructing regulatory roles and strategies for the future may not only be a matter of sharpening old instruments and forging new tools, but also of rethinking what kind of society we want to live in, and how we can bring it about.