David Lyon, Surveillance After September 11 (Cambridge, UK: Polity Press, 2003)

6

Resisting Surveillance

> "I don't want to live in a country where people deceive each other, where people look at each other as if they were potential terrorists . . . I want to live in a country in which one can and does assume helpfulness and cooperation."
>
> Ursula Franklin[1]

The surveillance consequences of 9/11 provide an opportunity to rethink surveillance and also, I believe, to resist it. Thus far, already existing systems have been reinforced, increasing the tendency for cultures of control and of suspicion to be augmented. At least some of the intended outcomes of intensified surveillance are unlikely to be realized, whereas the unintended consequences are already appearing.

In the past few years, surveillance has become algorithmic, technological, pre-emptive, and classificatory, in every way broadening and tightening the net of social control and subtly stretching the categories of suspicion. It thus tends to undermine trust and, through its emphasis on individual behaviors, to undermine social solidarity as well. At the same time, it augments the power of those who institute such systems, without increasing their

accountability. All these features have been amplified since 9/11.

Several years ago, when I first started researching and writing about surveillance, I endeavored to maintain an appropriate stance that was neither paranoid nor complacent. I argued (and still do) that surveillance of some kind is both socially necessary and desirable but that it is always ambiguous. The dangers and risks attending surveillance are as significant as its benefits. In contexts where I felt people were being alarmist and shrill I cautioned restraint and pleaded for more careful analysis. In contexts where complacency seemed to reign I tried to show that surveillance has real effects on people's life-chances and life-choices that can at times be very negative.

Since 9/11, however, the pendulum has swung so wildly from "care" to "control" that I feel compelled to turn more robustly to critique. While I still insist that attitudes to surveillance should be ambivalent, the evidence discussed in this book obliges me to observe that oblique dissent will no longer do. Some instances of early twenty-first-century surveillance are downright unacceptable, as they directly impugn social justice and human personhood. They help to create a world where no one can trust a neighbor, and where decisions affecting people and polity are made behind closed doors or within "smart" systems.

This is not merely a negative critique, however. Major challenges confront the world following 9/11. There is a need for positive suggestions about other ways forward. The challenges, I suggest, are analytical, political, and technological. That is, the challenges affect how the social world after 9/11 is understood; how it is ethically judged and what are taken to be priorities for action; and how people might participate in deciding what technologies are adopted. The world is even more complex, unstable, and

risky after 9/11. But those are reasons for engagement with it, not withdrawal.

Drawing Threads Together

Surveillance as a central social process was already highly developed in most countries of the world before September 11, 2001. Modern societies are surveillance societies, even before they depend on digital technologies, but more fully so after computerization. Surveillance practices and processes were already being augmented by networked communication systems before 9/11, and change was accelerating. More and more surveillance cameras were being installed in urban areas, for example, not only in Britain and other European countries, but in North America and Asia as well. In many ways, however, the effect of 9/11 has been to accelerate the adoption of surveillance practices, such as Neighborhood Watch informers, and technologies, such as internet tracking. The attacks triggered intensified surveillance in many spheres.

Current evidence suggests that already existing trends in contemporary society are being reinforced since 9/11, especially the cultures of fear, control, suspicion, and secrecy. The first, fear, is easily amplified by the mass media, which was clearly seen just after 9/11 itself. The "irrational" attacks, apparently "from outside," mean that "no one is safe." The endless replays of WTC footage themselves helped foster fear and eroded resistance to new surveillance regimes. The second, control, as David Garland has eloquently argued, is not a conspiracy of the powerful.[2] Rather, those in power have capitalized on certain social developments, especially the rise of the consumer-citizen and of privatized mobility, to institute forms of commodified control. These depend on calculating risks and on seeking information through surveillance.

The culture of suspicion follows from the first two. It is a consequence of dependence on a multitude of tokens of trust rather than on direct relations of trust, and of course it has been exacerbated by 9/11. The fear produced by the New York attacks, as Onora O'Neill argues, undermines trust in a peculiarly vicious way.[3] Finally, the culture of secrecy has always been a temptation of bureaucratic departments and governments, and it flies in the face of democratic practices. It too has mushroomed since 9/11.

Irony repeatedly rears its head in this book. The laws passed in the wake of 9/11 often cover ground already covered by existing law, are unlikely to succeed in their stated aims of making terrorist attacks less likely, but are highly likely to have effects not explicitly intended by them. Similarly with new technological measures geared to minimizing risks of repeat attacks. Many are poorly suited to their purposes, while being lamentably conducive to other consequences. Of course, it is understandable that emergency powers, quickly-passed legislation, and hurriedly-installed technologies will have flaws, but the ironies of initiatives following 9/11 go beyond these. They hint at a lack of understanding of actual situations (how devious intelligent terrorist plotters are likely to be, or why networked attacks are not amenable to conventional centralized responses, for example). And they rely on time-honored solutions, technical fixes, and tighter controls, applied across the board.

Surveillance trends have solidified after September 11, especially those of social sorting. The much-publicized debates over "racial profiling" places this in high relief, but the issues are broader than this. Negative discrimination toward those defined as "Muslim/Arabs" is certainly occurring. This is one of the most insidious results of

9/11, not least because it connects suspicions with particular ethnic and religious groups regardless of on-the-ground realities. But social sorting is even more evident than before as a foreground feature of surveillance. All kinds of group may be included in the "terrorist" category, and all kinds of activity, including casual chat, may be construed as suspicious. Such classification frequently takes place using human observers, but it becomes far more powerful when computer-assisted.

Other surveillance trends have also been accented since 9/11. One is the trend towards system integration. This is a goal that has long been shared by both technical system designers and by organization managers. The principle permits data – in this case personal data – to be shared across a range of departments or sections that today are typically networked. Searches and retrieval from remote sites are relatively straightforward. System integration always militates against the principles of fair information handling. This is because such principles create friction in the system, slowing down disparate record linkages and refusing access to certain data. Yet integration performs many functions of centralization, such that power may in fact be more concentrated, even though it appears geographically to be dispersed. The so-called surveillance assemblage, which loosely links numerous data-sets and sources of information, may not itself be hierarchical, but this does not mean that power-pyramids are a thing of the past.

Last but not least, surveillance is being effectively globalized, a process that has been gathering speed since September 11. Personal data of all kinds are flowing more freely across borders, between airport authorities and police and intelligence agencies in the global north in particular. Already flowing data – especially via the internet – are subject to more and more checks and monitors.

But if globalization originates in that very modern process of doing things at a distance, then it is clear that surveillance was set to be globalized from the start. The focused attention on personal details for management and control which comprises surveillance stretches increasingly over time and space, courtesy of new communication technologies. In terms of everyday practices, this touches directly on the "delocalized border." New measures move the information search away from the literal border as surveillance is globalized.

A further irony is this. The globalization processes that enabled the attacks of 9/11 to take place also enable efforts to apprehend potential terrorists. But in addition, they allow others to share information about negative aspects of surveillance and to warn others that not only the twin towers, but the towers of democratic involvement may also now be tumbling.

At the outset, I tried to show how surveillance responses to 9/11 are a lens for seeing two kinds of phenomenon: what is already happening and what is likely to happen in the future. It is important to step back again and recall that much of what has been brought forward as security-through-surveillance was already present in the policing, administrative, and consumer systems of countries around the world, but especially in the global north. 9/11 prompted an acceleration and an intensification of shifts toward surveillance societies that were already very visible in social life. Scholars, film-makers, artists, and political activists were already seeking to show that some trends were more than a minor cause for concern. Even without 9/11, surveillance trends were emerging as a contested site, despite the fact that they had few political champions.

The lens of 9/11 responses also helps us see what sorts of direction are taken when states of emergency are

declared and panic regimes take over. As we start to focus on this aspect of surveillance, some things seem scarcely credible. Certainly they appear contradictory. In the USA especially, the rush toward tight control appears to be reminiscent of highly authoritarian regimes of which the USA has been highly critical in the past. And the relentless hunt for enemies within is uncannily like that which occurred during the McCarthy era, only now "terrorists" with particular ethnic backgrounds rather than "communists" with particular national sympathies are the target. When surveillance turns ordinary citizens into suspects it is time for serious stocktaking.

Such social self-examination seems appropriate in the light of the apocalyptic aspects of 9/11 and the surveillance that is being established in its wake. Responses to 9/11 disclose already existing trends and simultaneously hint at a reckoning, a judgment. Normative approaches, already implicitly present in analysis and theory, need to be highlighted. It is one thing to be made aware of situations where freedoms are being constrained, human rights neglected, and people are suffering needlessly for things they have not done and for deeds they never contemplated; it is another to suggest what to look out for as warning signs as new measures are proposed, what sorts of alternative are appropriate, and why some kinds of response are preferable to others.

Meeting the Challenges

Three major challenges confront those who would resist the surveillance consequences of September 11: grasping their social, political, and technological dimensions. By the first I refer especially to analysis done in the social sciences. Secondly, there are pressing ethical choices in a

world where the politics of information are moving to center stage. And thirdly, understanding the technological dimensions of surveillance, especially after 9/11, is vital to any appraisal of what is going on in the world of identifying, locating, monitoring, tracking, and managing individuals and groups.

The Social Question

September 11, 2001 did not create the need for fresh concepts and new explanatory tools, but it does show how urgently they are needed now. Surveillance has to be understood today as social sorting, which has exclusionary consequences. Watching others has become systematic, embedded in a system that classifies according to certain pre-set criteria, and sorts into categories of risk or opportunity. These categories relate in turn to suspicion or to solicitation – and many others in between – depending on the purposes for which the surveillance is done. Such classification is very important to people's life-chances (as Max Weber would have put it) and choices. Surveillance is becoming a means of placing people in new, flexible, social classes.

How persons are "made up" by surveillance systems, and with what consequences, is a vital question. If the "data double"[4] that circulates through electronic systems does help to determine what sorts of treatment we receive from insurance companies, the police, welfare departments, employers, or marketing firms, then it is far from an innocent series of electronic signals. This is acutely true if ethnic, religious, or other contentious characteristics help comprise that data image. It also means that understanding how the coding systems work is also of utmost importance.

Struggles over classification are not new. What is new today is that classification processes are being automated, and used for a wide variety of tasks within increasingly dominant modes of risk management. Power over classificatory schemes, as Pierre Bourdieu argues, is central to the meaning of the social world. Law contributes to the codifying of classifications, as we saw with regard to definitions of terrorism. But technology buttresses this by removing further the human element, and by digitally facilitating the power of separation. Law and technology may seem remote to many, but their effects are felt locally, relationally, personally. As Bourdieu says: "The fate of groups is bound up with the words that designate them."[5] This could hardly be more true than for those today who are viewed first as "Arabs," "Muslims," or "terrorists." Surveillance practices enable fresh forms of exclusion that not only cut off certain targeted groups from social participation, but do so in subtle ways that are sometimes scarcely visible. Indeed, the automating of surveillance permits a distance to be maintained between those who are privileged and those who are poor, those who are "safe" and those who are "suspect." This may be exclusion as domination, where the categories of outcast reflect deep and long-term tensions. But it may also be exclusion as abandonment in which the way is eased for some simply to "walk by on the other side."[6] So-called social defense technologies work the same way to keep out the proscribed persons as "fast-track" "preferred customer" technologies work to protect privilege.

This is a different kind of argument than is often made about surveillance. Especially in the USA, surveillance is often thought to be a threat to privacy. Editorial writers and activists complain about initiatives such as DARPA's Total Information Awareness as "supersnoop" schemes that imperil personal freedoms.[7] But this is to misconstrue

and underestimate the power of surveillance. To think of surveillance primarily as endangering personal spaces of freedom is highly individualistic. It also misses the point about surveillance contributing to social sorting mechanisms. To process personal data in order to classify groups is to affect profoundly their choices and their chances in life. This is why the *social* analysis of surveillance is so essential to a proper understanding. And it is even more vital after 9/11.

Although 9/11 has brought some questions to the fore, in the twenty-first century surveillance affects everyone all the time. Its intensity varies from country to country and from agency to agency but it is increasingly generalized. In the global north in particular, risk management regimes rely on surveillance for their ongoing data-processing. The addition of "terrorist" categories to those already in operation dramatically deflects attention away from the routine and mundane operation of such systems. For most people, most of the time, insecurity and risk have precious little to do with anything as terrifying as terrorism. In homes and local communities it is items like the vagaries of the job market, the burden of debt, and the fracturing of relationships that constitute risk. Single mothers suspected of welfare fraud also have much to fear. For governments seeking to distract concern over poverty and inequality in their own countries and abroad, anti-terrorist surveillance provides an excellent decoy.

Another important caution: surveillance is not merely about new technologies. Ordinary people play a role within the surveillance process. The power of surveillance varies with circumstances, with the knowledge of the system held by its subjects, and with the responses that people make to the fact of being under surveillance. Sociologically, much power relates to economic factors; the rich tend to rule. Other aspects of power relate to

status, to groups active in their pursuit of political goals, or to personal information held by those who have access to it. Power is always a social relationship, and it is always contested or contestable.

But power is also a resource. The more that power relates to data – retrievable information about groups and individuals that can be cross-checked to filter out particular persons – the more surveillance becomes, in principle, a political matter. If Anthony Giddens is correct, a "dialectic of control" tends to emerge in relation to each of the key axes of power that have developed in the modern world.[8] If surveillance is becoming a central such axis, then what kinds of opposition to its negative features can be anticipated or encouraged? I shall return to this issue in a moment, when we look at the political challenge.

Compliance with surveillance is commonplace. Most of the time, and for many reasons, people go along with surveillance. It is a taken-for-granted fact of the modern world that we have to give our PIN at the bank machine, our driver's license to police, our health card number at the hospital. We assume that our employer, telephone company, and frequent flyer club will have a number for our records, and that when we vote in national or municipal elections our names will be listed. We assume that the benefits – security, efficiency, safety, rewards, convenience – are worth the price of having our personal data recorded, stored, retrieved, cross-checked, traded, and exchanged in surveillance systems. As ordinary subjects go along with surveillance, so the order constructed by the system is reinforced, and persons are "normalized" (as Foucault would say) by the system. Since September 11, compliance has been even more marked, for many, with the additional "fear factor." At the same time, as we shall see, challenges have also appeared, the long-term consequences of which have yet to be seen.

Compliance may not be unwitting, as is seen from the many examples of negotiating surveillance that occur from day to day. Although as yet social scientists know all too little about how people respond to being constant subjects of surveillance, some examples of negotiating it may be mentioned. Subjects may confound the categories when they do not recognize themselves in the descriptions of any number of questionnaires. Teenagers may play up to or evade the cameras in the shopping mall. People required to go through a "routine check" ordeal may refuse – "I ain't going to pee in no jar."[9] Employees may draw the line at public displays of keystrokes or at cameras in canteens or washrooms. Consumers may find technical means of preventing spam arriving in the email inbox. In each case, it may not be that the whole surveillance system is in question, but rather that some aspect of it is challenged.

In some of the above cases, questioning surveillance is just an individual matter, whereas in others, groups may be collectively involved. Individual refusals do count, but when groups and movements emerge that are committed to resisting surveillance or some aspects of it, then counter-surveillance becomes a more serious social phenomenon. Over the past couple of decades, a number of groups have appeared that make it their business to challenge the power of surveillance, most often in the name of privacy or of civil rights. Some issues have become *causes célèbres*, such as the proposal to create a "Clipper Chip" that would give a key to government to unlock encryption codes,[10] or the outcry against Lotus "Household Marketplace" software that would have made personal data by zipcodes available for sale on a massive scale.[11] Note that both these occurred in the USA, and both several years before 9/11. What has happened since builds on those precedents.

There is another, deeper, reason for questioning sur-

veillance, however. The kinds of question just addressed tend to assume that because technological surveillance is growing, it is on these terms that it should be countered. But this is to accept the increasingly dominant terms of reference rather than doubting that discourse itself. This book has shown how in fact new technologies are socially embedded in the practices of institutional and everyday life. From executive decisions made in DARPA to mundane choices about whether to use a credit card or cash, a cellphone call or an email, the socio-technical is always in view. Or should be. We have also seen how the technological "solutions" tend to be self-augmenting and to be presented as the obvious ones. They have a rachet effect in which more systems breed more insecurity which creates a new need for more systems. And all too easily they seem to insinuate themselves into a monopoly position.

This cyclops vision is desperately deficient. So-called social defense technologies and situational crime prevention that have been proliferating over the past 30 years, and which now appear to many as the only viable solution to terrorism, are socially regressive. They tend to reinforce social divisions through social sorting, remove questions of moral responsibility by reducing the real issues to risk and containment, and render true debate a non-starter. This is why I have also stressed the need to consider not just the instrumental, but also the dimension of social life that we might call solidarities. Deeper than law and technology is the level of mutual recognition, of willingness to discuss, of social trust. Questions of surveillance – like those of technology in general or of globalization – can seem very remote even though in fact they affect ordinary lives intimately. An ethics of care for the Other that extends to the practical welcoming of strangers, a nurturing of small-scale communities of many kinds that can mediate between the large scale and the everyday, and

a fostering of trust in appropriate ways – these are the soil within which such solidarities can grow. Whatever might be said about resisting surveillance, it is at this basic level that the practical task takes off.

Engaging a New Politics

The political challenge connects with the social analytical challenge, and indeed flows out of it. It has many aspects, and here I touch on just three. The first is the basic political challenge presented by the surveillance aspects of responses to 9/11. The idea of free democratic participation in an open society is under assault. The second has to do with the "dialectic of control" and raises the question of where leadership will come from in mitigating and reshaping surveillance practices. The third concerns the "politics of the code." This is a key aspect of politics in the twenty-first century, centering on the power of information and communication.

Whether seen in the lack of due process, the closed-door decisions of judges and politicians, the tendentious definitions of "terrorist," or the sheer authoritarianism of administrations engaged in the war on terrorism, democracy is in trouble after 9/11. Treating ordinary citizens as suspects, and simultaneously inciting them to spy on their neighbors, is an unlikely recipe for confidence in the political process. Placing security and military concerns at the top of the political agenda necessarily displaces freedom and democracy. They cannot coexist as equal priorities, at least under the current "surveillance state" regimes that are emerging. The attempt to tighten border security to keep out all manner of aliens may effectively close the door on the real needs of both the world outside and the world within.

Ulrich Beck notes the entrenchment of surveillance states after 9/11 but, like several others, he also advances an alternative: cosmopolitan states. These are characterized by solidarity, with foreigners inside and outside national borders. They would connect self-determination with responsibility for national and non-national Others. Thus: "Cosmopolitan states struggle not only against terror, but against the *causes* of terror."[12] This would lay the groundwork, Beck argues, for international cooperation on the basis of human rights and global justice. He does not discount or underplay the analysis of world risk society, for which he is justly famous. He insists rather that cosmopolitanism would be a way of civilizing it. This is an example of the road not (yet) taken as an alternative to the anti-democratic reinforcement of the surveillance state.

The revitalizing of the state is one challenge presented by the current dangerous drift towards surveillance states. Another is to discover what coalition of groups could tame existing surveillance power. If labor movements arose against the power of capitalist corporations, feminist movements against modern forms of patriarchy, and green movements against industrialism, then what countervailing movements arise against surveillance? It seems fair to argue that the activities of a range of social movements, dedicated to questioning surveillance excesses (which may in some case be surveillance per se) could count as actors in the dialectic of control now forming a firm shadow to surveillance activities in many contexts.

Since September 11, the kinds of agency, group, and movement that already challenged surveillance have redoubled their efforts. Recognizing that 9/11 provides new rationales for surveillance, along with a climate of fear and uncertainty, civil liberties groups and privacy commissions have been active in their critique and opposition to practices and technologies arising as a result of the attacks. Thus the Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU) have been prominent in voicing their unhappiness with new measures,[13] as have similar groups in other countries. Privacy International continues its invaluable work of documenting the growth of surveillance around the world, and of using Greenpeace-type publicity stunts to draw attention to the most blatant abuses. Liberty, in the UK, and Statewatch, in Europe more generally, play a cognate role. Also, government bodies that oversee data-protection and privacy have an important role. For instance, George Radwanski, the federal Privacy Commissioner of Canada, has been outspoken in his criticisms of the anti-terrorism law, as well as of matters like CCTV surveillance in Canadian cities – also growing since 9/11.

It is no accident that the activities of these groups have been strongly augmented since 9/11. In many countries surveillance has been intensified in the quest for security – but also in line with previous policy goals. So while Statewatch has appeared as a voice of dissent in Europe, other groups such as the Japanese Network Against Surveillance Technology (NAST) and the nascent Australian "City-State" activities, have been formed to unite opposition to post-9/11 surveillance developments. It is particularly interesting to note the rising disquiet about surveillance in Japan. Although not directly related to post-9/11 developments, major protests and uncharacteristic civil disobedience followed the introduction of the national computerized registry of citizens in 2002. Yokohama City declared that it would only support a voluntary registry, while Kokubunji simply refused to cooperate. They held a "disconnecting ceremony."[14] Even in the USA, where for a while it appeared that emotional responses would drown dissent, several cities – including

Berkeley, Cambridge, and Ann Arbor – have voted to defy the PATRIOT Act. It is significant how much may be achieved at a local level. Civil society and informal associations are an important alternative to the remoteness of rationalized risk societies.

The same kinds of technology that enable remote networked surveillance are also used to enable communication between those who dissent, above all using the internet. The groups mentioned above, which usually work both online and offline, are all attempting to use whatever means are at their disposal to open up public spaces. This is in sharp contrast with the efforts to close communication channels, and to envelop all significant decisions in a fog of secrecy. Such public spaces, to which democratic use of the internet is making important contributions, are crucial to any return to democratic practice after 9/11.

As the consequences of contemporary surveillance systems and of the specific fallout from 9/11 become clear, so it is likely that more attention will be focused on the code. As more systems are algorithmic, automating the social sorting processes, so awareness of the crucial role of software protocols is likely to rise. Ordinary people are, not unsurprisingly, interested in how facial recognition or racial profiling systems work. As Lawrence Lessig observes, cyberspace is already ruled by the law of the "code;" it never was the realm of unrestricted freedom that some of its idealists imagined.[15] However arcane technical software codes may appear, they are never neutral, never innocent. They refer to the desires and purposes of those designing and implementing the systems, and will express their categories. And, as Lucy Suchman reminds us, categories have politics.[16]

Technological Citizenship

The third major challenge confronting all who are concerned about surveillance, especially after 9/11, is technological. Remember, doing technology is not a foolish error. As I understand it, technology is part of the human calling to use wisely and fairly the earth's resources. Surveillance technologies themselves fall within this rubric as long as a just and appropriate balance is maintained between care and control.

The technology challenge has several aspects to it. At the most immediate level, those involved directly in technological efforts to combat terrorism – and any other perceived evil – have to confront the old conundrum of the likely effects of their work. It is a conundrum because until some system is installed and working at least some of its effects are unknown. But after it is installed, it may be too late to undo any potential damage. What is needed at this level is a keen awareness of the likely consequences, such that limiting measures can be built into the system. Groups such as Computer Professionals for Social Responsibility have been cognizant of these issues for some time. When social sorting is central to surveillance, the dangers of unfair treatment and prejudicial categorization should be highlighted so that potential damage can be minimized.

Beyond this, a time may yet come when the response to new surveillance proposals has, simply, to be negative – don't do it! For many reasons explored in this book, the creation of new surveillance systems may be looked at skeptically. Missing the mark of networked terrorism, the possibilities of abuse, the likelihood of reinforcing social inequalities, the distraction from more appropriate responses – all these and more are good grounds for

caution. But when powerful corporations are working with powerful government departments, and where there is public fear and political resort to fixes, those who speak for technological caution are likely to be voices crying in the wilderness. And yet in times like these it is precisely such voices that are needed.

At an even deeper level, it has to be acknowledged that the technological challenge is no longer merely one for technologists or for politicians to confront. It is not only that these matters are too important to be left to those people alone, but also that the challenge of technology is now one that involves everyone, in the intimate routines of everyday life. The development of technological citizenship[17] is called for, where the responsibilities and the privileges – and perhaps rights – associated with living in a world suffused with technology are a matter for ethical reflection and political practice. Such a process, if it is to succeed, will require some fundamental shifts in thinking.

The countries of the global north, especially the USA, are currently falling over themselves to pass laws and install technologies of mistrust. The cultures of suspicion and control are being legislated and automated. The notion of unreasonable search is blowing in the winds of change as single warrants now permit searches with few limits, online or offline, under the US PATRIOT Act. What would alternatives look like? Langdon Winner suggests that "designing technical systems that are loosely coupled and forgiving, structured in ways that make disruptions easily borne, quickly repaired,"[18] makes a lot of sense. He goes on to list local, renewable energy resources, rather than global ones that are always at risk, technologies operated locally by people who are known personally, and reducing dependence on risk-laden powers wrested from nature as parallel ways forward. Together, they add up to ways of "living lightly on the earth with justice and

compassion," which would also help eliminate grievances that lie behind terrorist attacks.

If such proposals are to have any effect, those of us influenced by western ways will have to turn our backs decisively on the modern instrumental approach to technology. It will have to be exchanged for a more hermeneutical understanding. In the latter view, technologies are "forms of life," embedded in social practices, such that contexts and functions of technology are in constant interplay.[19] Our radical dependence on technology, at least in the global north, means that doing technology has to be seen as part and parcel of all the activities of everyday life. This includes professional, domestic, commercial, legal, and, of course, political life.

To bring this back to earth, the next step is to ask whether technology is serving democratically defined goals or undermining them. Or are technologies simply being removed from public oversight? Who is actually accountable for surveillance systems, and what are the democratic processes that establish this? Who decides on the categories? Such matters may be worked out at very local levels, via what are sometimes called "privacy audits" in universities, firms, or government departments. Beyond this, technological citizenship demands not only a concern with limiting and regulating technologies – especially surveillance technologies in this case – but also in designing new systems. So-called privacy-enhancing technologies have a role to play here.

The question of technology is also a challenge that, at least in the West, confronts some profound cultural claims about the power of technology. David Noble, for example, argues that a deep-seated religious project is expressed – notably in the USA – of transcendence through technology.[20] James Carey calls it the "technological sublime,"[21] the dream of a world perfected through

technology, especially information and communication technologies. To resist technological developments, then, may be, to some, tantamount to sacrilege or blasphemy. When the technicist approach is privileged, questioning it seems quirky if not perverse. It is the voices of prophets that cry in the wilderness, witnessing to the state of the world and to the light of another way. And prophets often get silenced.

Beyond Suspicion and Secrecy

Surveillance after September 11 threatens to widen the net of suspicion and to deepen the darkness of secrecy. In the name of "security" and "risk" all manner of practices and processes are set in train that serve to obscure what is really going on. Questions of power are thus occluded, especially the power of some to classify others and to single them out for special treatment or for exclusion. In the twenty-first century, official classifications were already likely to become a central sociological concern, given their importance for the distribution of resources and benefits.[22] The categories of suspicion were but one means of classification before 9/11, but their range is now rapidly growing.

As for secrecy, it is being explicitly established again as a modus vivendi in the interests of a "war against terrorism." But it is also an effect of using certain technologies which render decisions – especially classificatory decisions – less visible. The first is intended, the second is not, or at least less obviously so. At least some risk of corruption and irrationality is present when power is wielded under cover of secrecy, and, as Sissela Bok argues, such secrecy feeds on itself.[23] It increases power without increasing accountability, but often requires more secrecy as greater

power accumulates. As for the digital aspects of secrecy, what I have in mind is the ways in which automation tends to make systems opaque, especially to those most affected by them.

These cultures of suspicion and of secrecy are anti-ethical and anti-political. Their combined effect is to inhibit trust and to close down discussion. The reduction of key challenges to risk management and security means that risk profiles are applied to relationships, institutions, and places, and, wherever possible, to automate responses.[24] This is why such a heavy emphasis is being placed on border controls and identity documents including smart cards. But this removes any concerns with social and legal contexts, with questions of jurisdiction and power, and the complex reasons individuals and groups might have for crossing borders. It also has implications for specific countries. In the case of the American proposal for "perimeter continental security" US–Canadian relationships would change significantly if common entry and exit policies were established.[25]

Unfortunately, trends towards risk management and related security and surveillance practices were already emerging before 9/11. They have been bolstered all the more unquestioningly since. The subtle but serious processes of social classification carry with them real "risks" that are rendered invisible and irrelevant when the language of risk management is dominant. The supposedly scientific basis of risk management lends it credibility but strips it of meanings that matter to most people – that they are embodied persons who inhabit specific places. Modes of categorizing that pay little or no attention to actual persons and places may seem innocent but in fact have consequences for those people and those places. Yet because the workings of those processes are often beyond the reach of those ordinary people, they

remain in relatively unaccountable spaces of bureaucracy or technology.

Responses to "terrorism" may all too easily give rise to totalitarian tendencies which, as Hannah Arendt astutely pointed out, are ultimately about terror.[26] I am not suggesting that current policies in any countries affected by the anti-terrorist rhetoric are themselves based on terror.[27] Arendt herself was concerned with the seeds and germs of twentieth-century totalitarianism. She held that they had much to do with belief in self-serving myths. Today, there are myths in abundance, such as guaranteed security or risk-proof surveillance, which are used to justify unfair and unaccountable policies. But Arendt's work is relevant in another way too. As Craig Calhoun reminds us, Arendt saw totalitarianism working directly on and within the private lives of families and individuals, which modern form of power Foucault has taught us so much about.[28] Translated into today's surveillance practices, the dangers are palpable.

It is in the mundane routines of everyday life that the effects, the dangers, of surveillance appear. Surveillance after 9/11 raises questions for all of us. Or rather, it prompts questions that ought to be asked. What kind of world do we want to live in? Fortress America? Maximum Security Europe? In early 2003 the burning question was, should the US and her allies attack Iraq to oust Saddam Hussein? But just as the war on terror is fought on more than one front, so too ordinary citizens should ask themselves, do we support the "war" in the "homelands"? If not, why not request or promote alternative approaches to security than those that simply stretch the net of suspicion, further foster the mood of fear, entrench the culture of control, and commodify dubious surveillance technologies as their antidotes?

Opposition to the gratuitous security-and-surveillance

aspects of the "war on terror" is required on many levels. Those who worry about privacy should not be discouraged from querying intensified surveillance. But they would also do well to move beyond the rampant individualism that perceives only "snoops" to consider the serious social consequences of the "sorters" who categorize and profile, to assess and influence people's life-chances. Those who deplore the spread of suspicion in employment, education, and other spheres could do more than merely wring their hands. Opportunities abound to show solidarity, to welcome stigmatized groups – such as Arab Muslims – and generally to trigger trust rather than fomenting fear.

Many people do have opportunities to let contrary opinions be heard about new technologies, just as views on unnecessary or unfair laws can be expressed in messages to papers or politicians. Why are those video cameras needed on the school bus? Why should government databases contain personal information, "just in case"? But such questions, though good, beg others. Those who work where personal data is handled should be bold about demanding accountability, and about the need for those who are classified for whatever purpose to be informed about and involved in the creation of categories.

Surveillance after September 11 places before us some momentous challenges. Above all is the challenge of how to confront a closed-off world of social exclusion and how to resist the rise of classificatory, clandestine power. During the Renaissance the idea took root that peace and prosperity could be engineered through science and technology, and this idea was bolstered by the European Enlightenment. Since then, the attempted engineering of security has become a key priority, spawning the myths mentioned above,[29] and contributing to the very difficulties we now face. The problem is that the Renaissance and Enlightenment encouraged an inversion of priorities. As I

hinted at the start of this book, an appropriate ethic begins by hearing the voice of the Other. And social care starts with acceptance – not suspicion – of the Other. Such an ethic does not exist in a cultural vacuum, however. It grows like green shoots in the soil of shared visions of desired worlds. But such visions seem in short supply today, when history is downplayed by mass media and securing the present preoccupies politicians. Attempts to engineer peace and security have become the default position in a world of amplified fears and truncated hopes. This "fixing" mentality also tends to close off other options, as if they did not exist.

Jacques Ellul once noted, reflecting on the fate of ancient cities such as Babylon and Nineveh, that these cultures were closed, too, "protected against attacks from the outside, in a security built up in walls and machines."[30] Is there anything new under the sun? Yet against that, insists Ellul, is the vision of a city where doing justice and loving one's neighbor is put first. From that commitment to responsibility for the Other proceeds peace and prosperity, freedom and security, sought otherwise through false priorities. This is a city whose gates are never shut. It is a place of inclusion and trust. And its light finally banishes all that is now done in the dark.[31]

Notes

Introduction

1 See David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity Press, 1994); David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy* (Minneapolis: University of Minnesota Press, 1996); David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001); David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (London and New York: Routledge, 2002).

2 Quoted in Michael Richardson, "ASEAN to step up efforts with US in war on terror," *International Herald Tribune/ Asahi Shimbun* (Tokyo edition), July 31, 2002: 2.

3 See e.g. David Garland, *The Culture of Control* (Chicago: University of Chicago Press, 2001).

4 See Ian Roxborough, "Globalization, unreason, and the dilemmas of American military strategy," *International Sociology*, 17 (3), 2002: 339–59.

5 Of course, technology derailed from its role as a servant of proper human purposes is likely to take on the appearance of savior. Cultures influenced by Christianity tread a knife-edge here. Once eyes are averted from a savior worthy of that name, then almost anything or anyone, it seems, will substitute.

6 I use the terms "care" and "control" in part to be consistent with my earlier work on surveillance. There has been a shift

Washington Post, February 1, 2002: A01 <http://www.washingtonpost.com/ac2/wp-dyn/A5185-2002Jan31>

43 See Gary T. Marx, *Undercover: Police Surveillance in America* (Berkeley: University of California Press, 1988) and D. Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity, 1994).

44 Geoffrey Bowker and Susan Leigh Star, *Sorting Things Out: Classification and its Consequences* (Cambridge, MA: MIT Press, 1999).

45 Richard Ericson and Kevin Haggerty, *Policing the Risk Society* (Toronto: University of Toronto Press, 1997).

46 William Bogard, *The Simulation of Surveillance* (New York: Cambridge University Press, 1996).

47 E. Borin, "Private Information Becoming Plane Truth," *Wired*, September 16, 2002, <www.wired.com/news/print/0,1294,55037,00.html>

48 M. Wald, "Boston Airport to Install Scanners," *New York Times*, September 23, 2002, <www.nytimes.com/2002/09/23/technology/23BOST.html>

49 Clive Norris, "From the personal to the digital," in David Lyon, (ed.), *Surveillance as Social Sorting* (London and New York: Routledge, 2002).

50 Stephen Graham and David Wood, "Digitizing surveillance: categorisation, space, inequality," *Critical Social Policy*, 26 (2), 2003.

51 See Gladwell, "Safety in the skies." See note xxii.

52 Michael Ignatieff, "The burden," *New York Times Magazine*, January 5, 2003.

53 Michael Richardson, "ASEAN to step up efforts with US in war on terror," *International Herald Tribune* with *Asahi Shimbun*, July 31, 2002: 2.

54 Document circulated by the "Civil Society Concerned about Globalizing Law Enforcement," obtained from Ogura Toshimaru, Toyama University, Japan.

55 James Norman, "Snoop systems scrutinized," *The Australian*, July 23, 2002: 4.

56 See Colin Bennett, *Regulating Privacy* (Ithaca: Cornell University Press, 1992) and David Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989).

57 See Priscilla Regan, "The globalization of privacy: implications of recent changes in Europe," *The American Journal of Economics and Sociology*, 52 (3), 1993: 257–74.

58 Naomi Klein, *Fences and Windows: Dispatches from the Front Lines of the Globalization Debate* (Toronto: Vintage Canada, 2002).

59 Saskia Sassen, "Towards a sociology of information technology," *Current Sociology*, 50 (3), 2002.

Chapter 6 Resisting Surveillance

1 Ursula Franklin, Science for Peace Forum, December 9, 2001, <http://scienceforpeace.sa.utoronto.ca/Special_Activities/Franklin_Page.html/>

2 David Garland, *The Culture of Control* (University of Chicago Press, 2001).

3 Onora O'Neill, *A Question of Trust* (Cambridge: Cambridge University Press, 2002), ch. 2.

4 Kevin Haggerty and Richard Ericson, "The surveillant assemblage," *British Journal of Sociology*, 54 (1), 2000.

5 Pierre Bourdieu, *Distinction: A Social Critique of the Judgment of Taste* (London and New York: Routledge, 1986), pp. 480–1. Thanks to Craig Calhoun for reminding me of this.

6 This distinction, plus one other, "exclusion as assimilation," comes from Miroslav Volf, *Exclusion and Embrace: A Theological Exploration of Identity, Otherness, and Reconciliation* (Nashville: Abingdon, 1996), p. 75.

7 E.g. William Safire, "You are a suspect," *New York Times*, November 14, 2002 <www.nytimes.com/2002/11/14/opinion/14SAFI.html/> Good points are made but they do not go nearly far enough.

8 Anthony Giddens, *The Nation-State and Violence*; vol 2: *A Contemporary Critique of Historical Materialism* (Cambridge: Polity Press, 1985).

9 John Gilliom, *Overseers of the Poor* (Chicago: University of Chicago Press, 2001).
10 William Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, MA: MIT Press, 1998).
11 Michael J. Weiss, *The Clustering of America* (New York: Harper and Row, 1988).
12 Ulrich Beck, "The terrorist threat: world risk society revisited," *Theory, Culture, and Society*, 19 (4), 2002.
13 See the 2002 report, "Bigger monster, weaker chains," at <www.aclu.org/privacy/privacylist.cfm?c=39>
14 "Japan in uproar as 'Big Brother' computer file kicks in," <www.nytimes.com/2002/08/06/international/asia/06JAPA.html>
15 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).
16 Lucy Suchman, "Do categories have politics?" *Computer Supported Cooperative Work*, 2 (1), 1994: 177–90.
17 Ian Barns, "Technological citizenship," in Alan Petersen, Ian Barns, Janice Dudley, and Patricia Harris, *Post-Structuralism, Citizenship, and Social Policy* (London: Routledge, 1999).
18 Langdon Winner, "Complexity, trust, and terror," *NetFuture*, 137, October 22, 2002, <www.netfuture.org/>
19 See Langdon Winner, "Technologies as forms of life," in his *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago: University of Chicago Press, 1986) and Ian Barns, "The renewal of civic virtue and the difference technology makes," unpublished paper, Sustainable Technology Policy Unit, Murdoch University, Perth, Australia, 2001.
20 David Noble, *The Religion of Technology: The Divinity of Man and the Spirit of Invention* (London: Penguin, 1997).
21 James W. Carey and James J. Quirk, "The mythos of the electronic revolution," *American Scholar*, 39 (1), 1970: 219–41, and 39 (2), 1970: 395–424.
22 See Richard Jenkins, "Categorization: identity, social process, and epistemology," *Current Sociology*, 48 (3), 2000: 7–25. He argues that rather than focusing on the fashionable "reflexive self-identity," sociology ought to be far more concerned with categorization.

23 Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Oxford: Oxford University Press, 1982), p. 106.
24 See Kanishka Jayasuriya, "9/11 and the new 'anti-politics' of 'security'," (2002) <www.ssrc.org/sept11/essays/jayasuriya.htm/>
25 Ibid.
26 Hannah Arendt, *The Origins of Totalitarianism* (New York: Harcourt, Brace, Jovanovich, 1951).
27 One could argue, of course, that the US administration has supplied and supported terrorist states elsewhere, and is thus at least complicit in state terrorism. See, e.g. John Pilger, *The New Rulers of the World* (London: Verso, 2002).
28 Craig Calhoun, "Plurality, promises, and public spaces," in Craig Calhoun and John McGowan (eds.), *Hannah Arendt and the Meaning of Politics* (Minneapolis: University of Minnesota Press, 1997), p. 236.
29 Bob Goudzewaard, *Idols of our Time* (Downers Grove: Inter-Varsity Press, 1984), p. 66.
30 Jacques Ellul, *The Meaning of the City* (Grand Rapids: Eerdmans, 1970), p. 76.
31 Ibid., pp. 192–3.