Technology vs 'Terrorism': Circuits of City Surveillance since September 11th

DAVID LYON

Introduction

I had no more than a slight feeling of apprehension when the pilot of the plane on which I was flying said we were obliged to make an unscheduled landing, under direction from the airline. I had never before heard of such an order but I assumed, like everyone else, that some simple explanation would be forthcoming when we landed. But I did fear that I might miss my connection to Singapore from Vancouver. It was the morning of September 11th 2001 and as yet no symbolic charge was attached to that date.

As soon as we landed, it became clear that a world event was unfolding. Strangers swapped stories of spectacular attacks on the heart of US global commerce and media in New York, and of the military power at the Pentagon. Soon we were in sight of TV screens that told the same unbelievable story. Even for someone aware of the power of some Islamic varieties of fundamentalism (Lyon, 2001b) and of their anti-American animus, sheer incredulity needed some hours to settle down. It also took a while to come to terms with the fact that I was not going to Singapore after all, and that getting home again, several days later, would involve running the gauntlet of armed security guards and waiting in lengthy security lines.

I tell the personal story because this is how we experience such events, and also because I should be perfectly clear that, like most other sane people, I want to have some assurances that I am safe when I fly. Indeed, it goes without saying that governments and airlines have a responsibility to make every effort to ensure public safety. But the personal trouble rapidly turned out to be a public issue, which is where sociology comes in (Mills, 1967). Security measures introduced since September 11th include prominently a number of surveillance devices and systems. They are intended to increase safety and allay fears primarily by predicting and pre-empting danger and by restricting access to a given country or site to eligible persons only.

The focus of what follows is not primarily the threat of 'terrorism' or the meanings of the spectacular attacks on the World Trade Center and the Pentagon, though these cannot be ignored. Nor do I dwell on the 'anti-terrorism' laws passed in the wake of September 11th, except insofar as they authorized the use of expanded surveillance techniques. I am interested in exploring rather the character and the meanings of the surveillance systems being mounted and reinforced in response to September 11th. Which devices are being promoted (and by whom) as the keys to security? What does this mean in terms of the already existing developments in surveillance at the turn of the twenty-first century? And what are the likely consequences of installing these new systems in what appears to be a new global alliance of surveillance states?

In short, I argue firstly that the devices promoted are precisely those that are already on hand, and already utilized in some (usually more limited) contexts. What transpired after September 11th is that companies and government departments that already had an interest in such surveillance systems now had a rationale — and public support — for installing them. Technological fixes are the common currency of crisis in late modern societies.

Secondly, this represents a continuation, albeit at an accelerated pace, of trends that were already strongly present in all advanced industrial (or 'informational') societies.

9600 Garsington Road, Oxford OX4 2DQ, UK and 350 Main St, Malden, MA 02148, USA

'Surveillance society' (see Lyon, 2001a) describes well the personal and population data-processing aspect of the 'network society' (Castells, 1996). One trend is accented, however: an unprecedented convergence between state and commercial surveillance (Lyon, 2001c).

Thirdly, the consequences are mixed. Success with the intended consequences of increased security is hard to discover. Indeed, most systems retain embarrassing limitations and flaws as far as their overt rationale is concerned. The unintended consequences are a widening of the surveillance web (see Cohen, 1985; McCahill, 2002) and an enhanced exposure to monitoring of ordinary people in their everyday lives (Lyon, 2002b). In comparison, non- or low-technological approaches to security receive little discussion.

Fourthly, the larger perspective is that 'technology' is still seen as a savior, as the first resort of 'advanced' societies. This is nothing new, but the quest for technologies, geared to guaranteed security, has been gathering pace especially since the second world war. Technological solutions are invoked before other more labor-intensive and human-oriented surveillance methods (which, ironically, are in fact more likely to succeed) let alone efforts aimed at mutual understanding and the reduction of Western threats to Islamic countries.

Surveillance technologies

Four main means of improving technological surveillance have been proposed since September 11th. They are: biometrics, the use of data extracted from the body, such as an iris scan, digital image, or fingerprint; identification (ID) cards with embedded programmable chips ('smart cards'); Closed Circuit Television (CCTV), often enhanced by facial recognition software; and communicational measures, such as wiretaps and other message interception methods including Web-based surveillance. In some places, several of these measures are now in place, others had to await legal change and are now being implemented.

Biometrics has to do with the verification of identities, on the assumption that truly unique identifiers are found in the body. These may be used in smart cards, and are implicated in CCTV facial recognition systems as well. Smart cards, similarly, are intended to ensure a one-to-one fit between the identity of the card-holder and the unique card and thus to prevent unauthorized use or access. CCTV systems may be used 'live' to monitor persons in transit for risky behaviors (for example at airports) but also may be enhanced using databases of facial images or other biometrics such as retinal scans. Communicational surveillance is intended to check for potentially dangerous messages passing between suspect persons and groups.

Communicational surveillance is concerned primarily with *monitoring* behaviors, as is 'live' CCTV. All the others, including facial recognition, are more concerned with *identifying* individuals. But these two are linked. The Echelon system of international intelligence monitors *in order to* identify messages, and their senders, that seem risky.[1] Surprise was expressed after September 11th that the monitoring technologies did not seem to have provided warnings (although it now appeared that, rather, the warnings given were not heeded in a coordinated fashion — Rich, 2002). As we shall see, the trend is towards the use of more identifying technologies, and this has important consequences.

Biometrics

Recent advances in biometrics have made the use of physical attributes — body parts, if you will — popular candidates for identification systems. Some means are sought of verifying claims to identity and privilege, and unique physical attributes such as

[1] This distinction between monitoring and identifying benefited from discussion with Bart Simon of Concordia University.

fingerprints, irises, retinas, hand geometry, vein patterns, voices and faces are good tokens. Of course, these are never fully permanent tokens, so one can only ever claim a ‘probable’ match. Such systems are most reliable when used in conjunction with others. If someone makes a claim at a bank with a name, and that is supported by a biometric identifier, the probability of error is low. Errors are much more likely when the system has to identify an individual on its own.

The system must acquire an image, using an appropriate scanner, before localizing it for processing. The image must be cleaned by removing extraneous information, and the remaining minutiae turned into a template for eventual comparison with attributes stored in the database. The ‘minutiae’ are the uniquely distinguishing features of the image — the whorl on the fingerprint or the mole on the face scan — for which matches are then sought on the database. Of course, DNA is reliable in this context, too, but because it is invasive and requires special expertise, it is unlikely to be used for more than forensic purposes in the near future. The others have been seeking mass market acceptance for the past few years.

Biometrics, then, is a more general term than the others, and indeed may be implicated in ID cards or CCTV systems. Biometrics relies on having access to some physical characteristic, and then on algorithms that enable the verification process to be automated. An example is iris scanners, installed at Schiphol Airport in Amsterdam in October 2001.[2] The ‘Privium’ system is intended to fast track passengers carrying the iris data-embedded smart card through passport control and customs. This system does not use a database; the scanner simply checks the eyes to see if they match the ones recorded on the card. In 2003 the Dutch government plans to seal the bearer’s iris code into passports (Simons, 2001). In Canada, before September 11th, iris scans were mainly associated with bank machine tests (Pearsall, 1998).

Other systems use, or in the case of Canada plan to use, fingerprint scanners to enhance security. Canadian airports, ship-ports, and border crossings will have equipment linked to FBI and RCMP databases, to identify terrorists whose fingerprints are on file (CBC, 2001). While international airline authorities have applauded the relatively reliable eye-based scanners, Japanese researcher Tsutomu Matsumoto recently tested several fingerprint scanners, fooling them with his gelatin-based fake finger. He also lifted latent prints from glass and used his photoshop to enhance them to make yet more ‘fingers’ (Costello, 2002).

ID cards

Various kinds of biometric identifiers may also be used to authenticate ID cards, the second major surveillance technology proposed to deal with ‘terrorism’. The government of Peru, for example, issues photo ID cards with an embedded face recognition chip for residents (Francis, 2000). DNA patterns have been proposed for ID cards in the USA (Marx, 1998), and ID implants are also likely to be marketed soon (Reuters, 2001). Since September 11th ‘smart’ ID cards have been consistently touted as a key means of enhancing security — a way of being sure that people are who they say they are and that they have a right or a reason to be where they are.

Other ‘crises’ have sparked similar calls for new ID card systems over the past few decades. During the twentieth century, world wars were a major impetus to the widespread and routine use of identification documents. In some countries the cards remained in place after the war was over, in others, such as the UK, the ID card system was dismantled following the ‘warfare state’ — if only to be replaced by the ID documents of the welfare state (Lyon, 1991; Agar, 2001). Calls for ID cards were repeated during the worst IRA attacks in the UK in the mid-1990s, and soon afterwards in Spain, in response to the ETA (Basque separatist) attacks.

[2] At Schiphol, and at Heathrow, London, iris scanning systems were planned well before September 11th (see, e.g., Greenman, 2001).

It is highly likely that several of the schemes proposed after September 11th will be implemented, though not necessarily in the original form proposed. Larry Ellison, CEO of the world's largest database software company, Oracle, was quick to offer the US government free software for a national ID system. There is little doubt that the offer was serious or that Oracle could have backed it up. The idea of using 'smart' cards on a very large scale for ID purposes has been projected in commercial and administrative schemes for several years, not least because it represents a technological 'next step' from less complex and comprehensive systems. Multi-purpose commercial smart cards (such as Mondex, see Stalder, 1999) were tested during the 1990s. And some countries, such as Malaysia, Thailand and Hong Kong, have already started to implement similar cards as national IDs. But others, such as the USA, the UK and Canada, have held back — or at least they did until September 11th 2001.

The apparent threat of terrorism to national security helped to put electronic ID cards back on national agendas and several proposals were made in the aftermath of the September 11th attacks, no doubt to test the waters of public opinion. While Larry Ellison's offer was turned down, the US nevertheless embarked on a process that could well culminate in the use of enhanced drivers' license cards (and their surrogates) acting as national IDs. Although part of the justification for these schemes is the knowledge that several of the 19 highjackers of September 11th were using assumed IDs, it is not clear that the American public will agree to universal identifiers. Opinion polls show a declining acceptance of such schemes, and in particular, doubt about the competence of drivers' license authorities to have charge of them.

Other countries, such as Germany and the UK, have also looked at new national ID systems in order to strengthen security in the wake of September 11th. The British 'entitlement card' is being phased in as a smart card with biometrics identifiers, building on the already introduced 'Applicant Registration Cards' which are designed to help cope with asylum seekers. In the German case, machine readable cards introduced after a political tussle in 1987 will be upgraded using hologram technology following the September 11th attacks. Yet other countries, such as Malaysia and Spain, have claimed that the systems already being implemented in those countries will have the effect of reducing terrorist threats. Countries are also looking to each other to provide models, guidance, or warnings about potential failure, abuse, or other unintended consequences (see for further details Stalder and Lyon, 2002).

In South-East Asia, both Malaysia and Hong Kong are in the process of introducing national smart card IDs, following Thailand's adoption of a Sun Microsystems ID backbone within its National Registration System. Malaysia's 'Mykad' is currently optional, and contains a drivers' license and passport information. In Europe, Spain is introducing a national smart card ID as well, partly in an attempt to demonstrate its leadership in European high technology developments. In each of these cases, change was well under way before September 11th. These initiatives are not unopposed, however. In the early months of 2002, for instance, considerable controversy was evident in Hong Kong over the new capabilities of the smart card, designed primarily to reduce illegal Chinese immigration.

In countries such as France, Japan and Canada, much interest has been shown in the possibility of introducing new ID systems, including the use of smart card technologies. If adopted, they are likely to be built onto existing systems. In Canada, for example, since 2001 public hearings have been held in Quebec regarding the Telehealth smart card project, which, if implemented as planned, will confirm admissibility to services, create statements of services used by patients, produce data on insured services, access to a provincial patient index, and so on. Such a system would offer useful lessons for smart card use and acceptability. And in a federal program, new immigrants are soon (from June 2002) to be issued a card with a photo and, probably some biometrics measures, a move prompted by the attacks of September 2001.

There are several difficulties with the new ID cards, however. For one thing, they are usually only as reliable as the other documents they are based on. This is often, ultimately, the birth certificate, a document that is notoriously easy to falsify if one has a mind to do it. Secondly, if central databases are used, these become very vulnerable to attack. But thirdly, assuming these problems are overcome, there is still the difficulty that, to put it simply, suicide bombers do not strike twice. It is unlikely that the kinds of terrorists to whom the ID cards are an answer will ever find their way onto suspect lists.

On another level, it has to be said that the new generation of smart ID cards has, even more prominently than in earlier systems, the task of classifying and discriminating between different groups of persons. They are intended to check for illegal immigrants or other persons in transit who have inadequate documentation. This is obvious to any observer, but what may be less than obvious is the negatively discriminatory practices that can easily accompany the use of such identifiers. The history of the twentieth century is replete with such, not only in Hitler's Germany, South Africa under apartheid, or contemporary Israel, but also in countries such as the USA and Canada who mistreated persons of Japanese origin (using the census for ID) during the Second World War. Even now, following September 11th, there is evidence that some 'Arab' and 'Muslim' people in the USA have been singled out for very negative treatment, including lengthy detention without charge or trial (Burkeman, 2002).

CCTV and face-recognition

As we have seen, biometrics is also implicated in new generation CCTV systems, where face-recognition is involved. Airports including Pearson International in Toronto had a system limited to a RCMP search of suspects already in place, when Keflavik in Iceland announced in September 2001 that all visitors' faces would be screened. During October 2001 American airports were quick to respond with announcements that face-recognition technology would be installed. Oakland International laid claim to being first in the USA, using the system to check on passengers detained under suspicion (policing authorities determine who they are) (Fernandez, 2001), but a much broader system was announced at Boston Logan Airport, which uses Visionics 'FaceIt' technology at an undisclosed checkpoint to compare facial characteristics of all travelers, airport employees, and flight crews with those of suspected terrorists (PR Newswire, 2001).

In this field, airport security systems are most closely associated with urban CCTV systems. An ordinary crowd of Superbowl fans in Tampa Florida was scanned using Viisage equipment in January 2001 (and of the 100,000 about nineteen petty criminals were recognized) but similar equipment has been used for some time with 300 cameras on public streets in the Newham district of east London, UK. This was mainly in response to the IRA threats of the 1990s, but street camera systems in the UK got their biggest single boost from the James Bulger case — the toddler murdered by teenagers who were caught on camera in 1993 (Norris and Armstrong, 1999). Britain is easily world leader in using CCTV in public places, but the face recognition aspect is only in some very limited sites. It is unclear whether face recognition systems work for cases of street crime in public places (despite the claims of their promoters), let alone whether their limited successes there can be re-applied to cases of international terrorism (C. Wood, 2001: 97).

It is clear that there was mounting pressure — for instance from the US Defense Department, as well as from a number of major companies and think-tanks such as the Rand Organization — before September 11th to develop and to install face-recognition CCTV systems (Greene, 2001; O'Harrow, 2001). The Defense Advanced Research Projects Agency had anti-terrorism in mind, but private corporations sought customers from banks, motor vehicle officials and others as customers. Imagis, a Vancouver-based company, has been vigorously promoting its products before and after September 11th. They sell to casinos, and also to the RCMP (the Pearson airport system) and the FBI. They market their software through Groupe Bull in France, and Fujitsu and NTT in Japan. The Peruvian ID system is based on Imagis technology, too (Francis, 2000).

But while many promises are made for face-recognition CCTV, the reality is that, like the other biometric technologies, it has only limited uses and reliability. Some airports are using it to scan airport employees such as maintenance workers and baggage handlers. When there is a known database for employee identification, the two checks (biometric and ID) can work together satisfactorily. But picking terrorists out of crowds is a quite different issue — the question is, 'does this biometric match anyone in the crowd?' (Schneier, 2001). Terrorists do not pose for photos (and are likely to use evasive techniques and disguises), but even if one had some good images, the so-called base rate fallacy means that the chances of false alarms would be very high indeed (9,999 for one terrorist — which means a full alert each time).

It is also argued that face-recognition systems, while they may not work for their ostensible purposes, would end up being used for finding petty criminals. These people will already have images in the database, and thus will stand more chance of being 'seen' by the camera. But there are further arguments raised against face-recognition. The potential for abuse — such as tracking individuals — is huge, and data is easily combined with that from other systems such as location systems of the E-911 type. There could also be 'premature disclosure' as Philip Agre calls it — similar to that offered by call display telephones, but based on the passing face-image. Informed and meaningful consent is almost impossible to obtain, and the chances are also high that civil liberties will be overridden in places where systems are established — especially if there is a weak tradition of appeal to them (Agre, 2001).

Communications monitoring

As with other forms of surveillance, September 11th did not prompt their introduction. Intercepting communications is one of the oldest methods of surveillance, which has a long history of use for law enforcement and military intelligence in particular. During the twentieth century, these were increasingly rationalized and eventually enhanced by computerization. Indeed, many of the surveillance technologies that are now visible in policing and even in marketing found their origin in military intelligence systems. Policing has in this way as in others become increasingly militarized (Haggerty and Ericson, 2001), and it must be said that the language of 'strategy' and 'targeting' is not absent from marketing either (Lyon, 1994).

Computerization made possible the narrowing of searches for delinquent communications and, combined with satellite tracking stations, and now internet surveillance, created a situation in which massive power is vested in 'intelligence' services — of all kinds. The searchable database is key to this, and the well-known search engine, Google, demonstrates the ease with which, given a few clues, numerous likely 'hits' can be made very quickly. It also shows how effective — at least in principle — the internet and World Wide Web are in facilitating remote searches.

After September 11th many mass media outlets drew attention to the existence of Carnivore, the internet surveillance system already used by the FBI, and to Echelon, the far larger system for international monitoring of all communications — fax, telephone, telex and email. It came as a surprise to many that such sophisticated search engines already existed, powered by huge 'dictionaries' that check messages for key words and contexts in quest of suspicious or risky communications. These are used not only for military or terrorist threats, either. Increasingly, they may be used by police departments trying to prepare for protests such as those by anti-globalization groups, and also as a means of technological and commercial intelligence, to raise the stakes of economic competition (Lyon, 2001a).

One might justifiably ask how the attacks of September 11th were not detected, given the huge intelligence infrastructure that was in place. FBI assistant director Ron Dick noted that the hijackers had used the net well (Campbell, 2001: 3). Internet Service Providers (ISPs) handed over records of hundreds of messages sent from PCs and public sites such as libraries, in the USA and internationally. They were unencrypted, and used simple open codes. The National Security Agency response to growing internet traffic has been to multiply the power of its storage and search facilities, from a petabyte (roughly eight times the information in the Library of Congress) to a petaplex (20 million gigabytes) system. But it is not clear that this will work any better than what was in place before September 11th, because the problem of correlating diverse information rises exponentially as ever more communications are intercepted.

Several other interesting issues are raised by the rise in communications interception, and particularly internet surveillance, following September 11th. It demonstrates, firstly, the ways in which national governments and corporations are working together more closely, such that companies may do ‘police’ work, both on their own account and for the authorities. Law enforcers have increased by five times their demands for information from email providers and ISPs in the USA (CNN, 2002). Concerns about ‘privacy’ in this area, which were growing before September 11th, seem to have been exchanged for a new willingness of companies to cooperate in the ‘war against terror’. Companies start to comply with requests for data even before the warrant has been issued, which suggests that an ongoing state of ‘emergency’ has been accepted (*ibid.*). Under the US Patriot Act customer payment records can be subpoenaed to find the ID behind an email address, clickstreams can be monitored, and messages can be read or listened to in real time. Similar provisions are in force elsewhere (Mathieson, 2001).

Secondly, US government in particular has taken on a stronger policing role in other countries. Because such a large volume of global internet traffic flows through the USA (80% of Asian, African and South American access points, for example — Associated Press, 2001), foreign hackers can be prosecuted by the USA under the Patriot Act when computers in the USA or abroad are attacked. Thus, because internet traffic passes through US borders, it can be criminalized under US law.

Thirdly, the upshot of post-September 11th surveillance is that more and more mundane transactions and conversations of everyday life are under scrutiny than ever before. The new provisions may not catch terrorists but they could complicate life for others, especially as they are monitored, classified and evaluated. In the UK, for example, where the Regulation of Investigatory Powers Act already had sweeping capacities to obtain communications data without a court order, anti-terrorist legislation allows these to be retained for longer (Millar, 2001). When one considers that the meaning of a website or of search words is different from, say, a phone number (which gives little away in itself), it is clear that captured communicational data is also more and more detailed.

Needless to say, these conclusions about the growing range of surveillance technologies are not uncontroversial. The ever-optimistic *Wired Magazine* still believes that ‘Little Brothers’ will answer back, that ordinary people will empower themselves with their own technologies, that the US Constitution still stands as a bulwark of liberty, and that the sheer volume of new gadgets will countervail against government power (Penenberg, 2001). But the larger sociological context must also be borne in mind before such sanguine conclusions can be confirmed.

Theorizing surveillance after September 11th

The surveillance measures introduced after September 11th are not new. They are all devices and systems with a track record. By and large they extend, enhance, or place in an unfamiliar context technologies whose promise has been advertised for some time or whose use has been proven in some other context. For many readers of newspapers and TV news watchers, words like ‘biometrics’, for example, appeared to be novelties in the last part of 2001. But for a number of years biometric devices have been tested in several contexts, from retinal scans at bank machines to digital records of fingerprints in police databases.

Technologically, what these surveillance systems have in common is a reliance on searchable databases (see Lessig, 1999). This does not hold in the case of ordinary, 'live' CCTV monitoring by a human operator, but it is true of the commonly advanced proposal for facial recognition facilities with CCTV. This means that they are 'algorithmic' — mathematically coded for computers to make 'decisions' as to what behavior, signal, word or image fits in which category (D. Wood, 2001). Their key feature is thus that they are automated, dispensing as far as possible with human operatives (Norris *et al.*, 1998).

In order to understand how these systems developed and became central to surveillance in the last part of the twentieth century, one has to examine in brief the history of surveillance in modern times.

It is important to note from the outset that surveillance is practiced with a view to enhancing efficiency, productivity, participation, welfare, health or safety. Sheer social control is seldom a motivation for installing surveillance systems even though that may be an unintended or secondary consequence of their deployment. From the earliest days of state surveillance in sixteenth-century England, for example, the aim was to consolidate state power against others, and to maintain the position of elites, rather than to use raw informational power to keep subjects in line (Higgs, 2001).

Surveillance in capitalist workplace settings developed as an intrinsic element of this mode of production (Webster and Robins, 1986), and is related in particular to what James Beniger calls the control revolution (Beniger, 1986). It is not doomed by this fact to produce only further exploitation — it can make for more fairness in some cases — but by and large employees have had to struggle against the potentially oppressive aspects of workplace surveillance. It should also be noted that surveillance in the capitalist workplace is not paradigmatic for surveillance in other contexts. There is a surveillance spectrum, from hard, centralized, panoptic control to soft, dispersed, persuasion and influence. Workplace surveillance lies somewhere between the categorical suspicion of policing to the categorical seduction of consumption.

The computerization of administrative tasks and systems that took place from the 1960s had the effect of reducing the burdens of cumbersome bureaucracies, but with the frequent side-effect of increasing dramatically the visibility of all citizens, workers and, before long, consumers, through routine surveillance checks. By the 1980s and 1990s, however, this was also tied into the general economic restructuring that dismantled state welfare and radically individualized risks. Rising affluence and mobility also increased opportunities for crime and deviance, which in turn fostered an emerging 'culture of control' (Garland, 2001). It is important to put these matters in their broad social context, rather than viewing them as some kind of conspiracy of the powerful.

Much of the mushrooming growth of surveillance in twentieth-century administration and commerce may be related to 'disappearing bodies'. Rising rates of mobility, coupled with the stretching of social relationships enabled by new technologies of travel and communications, meant that fewer and fewer transactions and interactions are based on face-to-face relationships. This produces a quest for means of compensation with what can be called 'tokens of trust' (Giddens, 1990; Lyon, 2001a). Hence the PINs, bar-codes, signatures, and eventually photo IDs and biometrics that lace the cards we carry. Human beings, embodied persons, are thus abstracted from place and are siphoned as data into flows, to be reconstituted as 'data images' in surveillance systems. Multifarious systems developed from the 1960s to the 1980s, some of which had links but in general (and partly due to legal constraints) few opportunities to trace across databases without specific cause. Is this 'Orwellian'?

Theoretically, what George Orwell feared was a state-organized central surveillance apparatus, a pyramid of power in which ruler and ruled were transparent to each other. As electronic forms of surveillance became more widely distributed, however, many turned to Foucault's treatment of Bentham's Panopticon as a means of considering ubiquitous power based on continuous observation. It is partly a centralized scheme, though there is scope for its localization into the 'capilliary' levels in the minutiae of everyday life. Such centralized surveillance always brings with it the risk of totalitarianism, as Giddens argues (1985), but checks and balances, and vigilance of privacy lobbies, labor unions, civil rights movements, and consumer groups have traditionally proved quite effective in curbing it, especially in the West.

In recent years, interest in the surveillant *apparatus* has been depleted somewhat as the notion of a surveillant *assemblage* has attracted some sociological attention. The latter idea originates in the fertile imagination of Gilles Deleuze (Deleuze and Guatarri, 1987), and has been pursued fruitfully by a number of sociologists (see Haggerty and Ericson, 2000). The assemblage, in this context, is a set of loosely linked systems, to be distinguished from the operation of government, at least as classically understood by political scientists. It is emergent and unstable. It operates across state institutions and others that have nothing (directly) to do with the state. Examples of this might be insurance categories used by police to determine risk. The assemblage is all about linking, cross-referencing, pulling threads together that previously were separate. And this also hints at its mode of growth — like the weed 'Creeping Charlie' that sends out horizontal shoots which in turn become new nodes in a constantly growing network. Deleuze and Guatarri think of this as 'rhizomic' development.

From what we have seen of surveillance after September 11th, however, it is a mistake to imagine that the loosely networked assemblage simply supplants the centralized apparatus. The rising tide of risk management techniques has indeed flooded over old distinctions between different institutional areas, but instability is endemic. Outcomes are impossible to predict. True, 'organized risk management' was somewhat eclipsed by 'disorganized' and 'disorderly' systems in the last part of the twentieth century (Crook, 1995). But statist forms have by no means disappeared, and a world event like September 11th has shown that they have both power and influence when perceived threats are of a sufficient magnitude. The assemblage and the apparatus are overlapping, even superimposed, systems and the assemblage can still be appropriated by the apparatus.

The key effect of September 11th, then, is to bring the apparatus and the assemblage into closer coordination with each other (Lyon, 2001c) within a larger frame of governance. As we have seen, the rhizomic operation of consumer surveillance can be raided by police and intelligence services, when required to do so. The longer term consequences of this are as yet unclear. But one thing that is clear is that 'privacy' and even 'data protection' are inadequate as means of limiting today's newly-augmented surveillance power. While there is an important 'care' motif (see Lyon, 1994: 211–17) in the post- September 11th measures, the balance seems to be tipping in favor of heightened 'control'. This is neither inevitable nor irrevocable, but it is a trend which, if unchecked, could become a serious threat to human rights.

I say 'human rights' because the effect of increased algorithmic surveillance is to deepen the process of social sorting, of categorization for various purposes. It is a means of inclusion and exclusion, of acceptance and rejection, of worthiness and unworthiness. What may be called 'digital discrimination' is the ways in which the flows of personal data — abstracted information — are sifted and channeled in the process of risk assessment, to privilege some and disadvantage others, to accept some as legitimately present and to reject others. The language of privacy is indeed of decreasing salience to the emerging situation of rhizomic, algorithmic, assemblage-type surveillance. But this does not mean either that some notions lying behind privacy concerns are irrelevant, or that a fresh vocabulary for mobilizing dissent is superfluous. To the contrary, without it, some very regressive tendencies appearing since September 11th will simply be reinforced.

Conclusions: consequences and critique

It will be clear by now that I have no quarrel with the idea that serious measures should be taken to prevent repetition of the horrendous events of September 11th 2001. But the problem is that merely 'technological' solutions are in themselves inadequate to the threat, and simultaneously dangerous to democratic polity. They are 'dangerous' because of three key trends, illustrated in the foregoing discussion: (1) the effective re-centralization of state power; (2) the increased capacity to discriminate between different classes of persons, using algorithmic surveillance; and (3) the relative lack of accountability of these systems, paralleled by the willingness of populations to accept them as the 'price of security'.

The problem with the last point about security is, of course, that the intended consequences of the technologies we have considered are unlikely to be realized. The evidence from biometrics, ID cards, facial recognition associated with CCTV, and communications monitoring is that as tools for an anti-terrorist campaign they are flawed. The automated, algorithmic systems are poorly equipped, by and large, for the task of identifying or monitoring the actions or messages of previously unknown potential terrorists. Moreover, to the extent that surveillance depends on information technologies, the easier it will be for persons who wish to evade detection to do so, just because human beings are more flexible and imaginative than technologies. Any technology can be outwitted, given time and ingenuity.

Of course, many unintended consequences follow from the tightening of security by surveillance. There will be closer monitoring of all who are in fact 'clean' (and have a data image to 'prove' it). The culture of control will colonize more areas of life, with our permission or without, because of the understandable desire for security, combined with the pressure to adopt particular kinds of systems. Ordinary inhabitants of urban spaces; citizens, workers, and consumers — that is, people with no terrorist ambitions whatsoever — will find that their life-chances are more circumscribed by the categories into which they fall. For some, those categories are particularly prejudicial, restricting them from consumer choices because of credit ratings, or, more insidiously, relegating them to second-class status because of their color or ethnic background. It's an old story in high-tech guise.

The alternatives to high-tech monitoring and identification methods seem to receive little attention. The labor-intensive intelligence gathering, the physical checking at airports, the use of security personnel to screen travelers — all these seem to have a low premium compared with extending the surveillance system with a new biometric or search device. Actually mounting programs to try to understand the reasons why certain countries, religious adherents, or political groups would have serious enough misgivings about and mistrust of the Western world to sacrifice their lives in order to destroy it seems well beyond the pale. This is not only labor-intensive, it would involve slow learning processes and cultural contacts of apparently very unwelcome kinds (see Downey and Murdock, 2003).

Much better, it appears, to fall back on the technological fix, just as has been done for over thirty years, since the first highjackings prompted technical modifications to aircraft and airport facilities (Lyon, 2002c). There is tremendous commercial pressure to purchase new surveillance equipment; the current situation is seen as an unprecedented business opportunity by some who have seen their share prices rise several-fold since September 11th. American security companies in particular are hawking their wares around the world in hope of taking advantage of the political climate of anti-terrorist activity. CEOs such as Larry Ellison are still arguing that the interests of Oracle and the USA are virtually identical and that they lie in integrated ID systems (Rosen, 2002).

Political (and public) fears continue to produce panic regimes (that seem like earlier moral panics on a larger scale). Safety and security are good things to desire, but the means are highly dubious, and spring from other sources (Stuart, 2001). So why the fixation on technology (which is even shared, sometimes, by groups such as the

American Civil Liberties Union who warn that the technologies are not *yet* good enough to serve the purposes claimed for them)? I suggest that this is articulated with one of the deepest currents of (late) modernity — the deep-seated belief in the power of technology to protect and to guarantee progress. 'In technique we trust' is the slogan about which Jacques Ellul, Ursula Franklin and David Noble have warned us repeatedly. Whatever one makes of their particular perspectives, they are surely right to say — as I do in relation to 'technology vs terrorism' — that technology won't save us.[3]

David Lyon (lyond@post.queensu.ca), Sociology Department, Queen's University, Kingston, Ontario K7L 3N6, Canada.

References

Agar, J. (2001) Modern horrors: British identity and identity cards. In J. Caplan and J. Torpey (eds.), *Documenting individual identity: the development of state practices in the modern world*, Princeton University Press, Princeton, NJ.

Agre, P. (2001) Your face is not a bar code. http://dlis.gseis.ucla.edu/pagre/bar-code.html.

Associated Press (2001) Internet takes on police role world-wide. *South China Morning Post* 23 November (http://technology.scmp.com/cgi-bin/gx-cgi/AppLogic+FTContentServer?pagename=S_23/11/01).

Beniger, J. (1986) *The control revolution: the social and economic origins of the information society*. Harvard University Press, Cambridge, MA.

Burkeman, O. (2002) Visa detainees allege beatings. *The Guardian* 23 May.

Campbell, D. (2001) How the plotters slipped US net. *The Guardian Online* 27 September, 1–2.

Castells, M. (1996) *The rise of the network society*. Blackwell, Oxford and Malden, MA.

CBC (2001) Fingerprint scans part of new airport security. *CBC News* 11 October (http://cbc.ca/cgi-bin/news 2001/10/11/airport_security.011011).

CNN (2002) Net effect: anti-terror eavesdropping. http://www.cnn.com/2002/TECH/internet/05/27/terror.surveillance.ap/index.html.

Cohen, S. (1985) *Visions of social control*. Polity Press, Cambridge.

Costello, S. (2002) Japanese researcher gums up biometrics scanners. *Infoworld* 16 May (http://staging.infoworld.com/articles/hn/xml/02/05/16/020516hngumsxml?T).

Crook, S. (1995) Ordering risks. In D. Lupton (ed.), *Risk and sociocultural theory*, Cambridge University Press, Cambridge.

Deleuze, G. and F. Guatarri (1987) *A thousand plateaus*. University of Minnesota Press, Minneapolis.

Downey, J. and G. Murdock, (2003) The counter-revolution in military affairs: the globalization of guerilla warfare. In D. Thussu and D. Freedman (eds.), *War and the media: reporting conflict*, Sage, London.

Fernandez, L. (2001) Oakland to be first US airport to use face-recognition ID system. www.siliconvalley.com/docs/hottopics/attack/image101801.htm.

Francis, D. (2000) Canadians master matching mug shots. *Financial Post* 19 October, C3.

Garland, D. (2001) *The culture of control: crime and social order in contemporary society*. University of Chicago Press, Chicago.

Giddens, A. (1985) *A contemporary critique of historical materialism*, vol. II, *The nation-state and violence*. Polity Press, Cambridge.

—— (1990) *The consequences of modernity*. Polity Press, Cambridge.

Greene, T.C. (2001) Think-tank urges face-scanning of the masses. *The Register* 20 August (www.theregister.co.uk/content/6/20966.html).

Greenman, C. (2001) In the airport fast lane with your eyes as a passport. *The New York Times* 2 August.

[3] This article was originally presented as a paper at the International Sociological Association meetings in Brisbane, July 2002. Some sections appear in Lyon (2003).

Haggerty, K and R. Ericson (2000) The surveillant assemblage. *British Journal of Sociology* 51.4, 605–22.

—— and R. Ericson (2001) The militarization of policing in the information age. *Journal of Military and Political Sociology* 27, 233–55.

Higgs, E. (2001) The rise of the information state: the development of central state surveillance of the citizen in England 1500–2000. *Journal of Historical Sociology* 14.2, 175–97.

Lessig, L. (1999) *Code and other laws of cyberspace*. Basic Books, New York.

Lyon, D. (1991) British identity cards: the unpalatable logic of European membership? *The Political Quarterly* 62.3, 377–85.

—— (1994) *The electronic eye: the rise of surveillance society*. Polity, Cambridge.

—— (2001a) *Surveillance society: monitoring everyday life*. Open University Press, Buckingham.

—— (2001b) Fundamentalisms: paradoxical products of postmodernity. In C.H. Partridge (ed.), *Fundamentalisms*, Paternoster Press, Carlisle.

—— (2001c) Surveillance after September 11. *Sociological Research Online* 6.3 (www.socresonline.org.uk/6/3/lyon).

—— (2002a) (ed.) *Surveillance as social sorting: privacy, risk, and digital discrimination*. Routledge, London and New York.

—— (2002b) Everyday surveillance: personal data and social classification. *Information, Communication, and Society* 5.1, 1–17.

—— (2002c) Security and surveillance at airports since September 11. Unpublished paper, The Surveillance Project, Queen's University.

—— (2003) *Surveillance after September 11*. Polity Press, Cambridge.

Marx, G.T. (1998) DNA fingerprints may one day be our national ID card. *The Wall Street Journal* 20 April.

Mathieson, S.A. (2001) The net's eyes are watching. *The Guardian* 15 November (www.guardian.co.uk/0,3858,4298,894,00.html).

McCahill, M. (2002) *The surveillance web: the rise of visual surveillance in an English city*. Willan Publishing, Cullompton.

Millar, S. (2001) Police get sweeping access to net data. *The Guardian* 7 November (www.guardian.co.uk/0,3058,4293489,00.html).

Mills, C.W. (1967) *The sociological imagination*. Oxford University Press, New York.

Norris, C. and G. Armstrong (1999) *The maximum security society: the rise of CCTV*. Berg, London.

——, J. Moran and G. Armstrong (1998) Algorithmic surveillance: the future of automated visual surveillance. In C. Norris, J. Moran and G. Armstrong (eds.), *Surveillance, closed circuit television, and social control*, Ashgate, Aldershot.

O'Harrow, R. (2001) Matching faces with mug shots. *The Washington Post* 1 August, A01.

Pearsall, K. (1998) This technology is eye-catching. *Computing Canada* 24.2, 11–12.

Penenberg, A.L. (2001) Surveillance society. *Wired* December, 157–60.

PR Newswire (2001) Boston Logan Airport chooses South Florida Security Company. 31 October (http://ir.shareholder.com/vsnx/ReleaseDetail.cfm?ReleaseID=63478).

Reuters (2001) Microchips under the skin offer ID, raise questions. *The New York Times* 22 December (www.nytimes.com/reuters/technology/tech-bizchips.html).

Rich, F. (2002) Thanks for the heads-up. *The New York Times* 25 May (www.nytimes.com/2002/05/opinion/25RICH.html).

Rosen, J. (2002) Silicon Valley's spy game. *The New York Times*, 14 April (www.nytimes.com/2002/04/14/magazine/14TECHNO.html).

Schneier, B. (2001) Biometrics in airports. www.extremetech.com/0,3428,a%253D15070,00.asp.

Simons, M. (2001) Security on the brain, solutions in the eyes. *The New York Times* 25 October (www.nytimes.com/2001/10/25/international/europe/25AMST.html).

Stalder, F. (1999) Exploring political issues of electronic cash. *Canadian Journal of Communication* 24.2.

—— and D. Lyon (2002) ID cards and social classification. In D. Lyon (ed.), *Surveillance as social sorting: privacy, risk, and digital discrimination*, Routledge, London and New York.

Stuart, D. (2001) The dangers of quick-fix law and order legislation in the criminal law: despite recent government amendments the Anti-Terrorism Bill C-36 should be withdrawn. Paper presented at a Surveillance Project seminar, Queen's

University, 15 November.

Webster, F. and K. Robins (1986) *Information technology: a Luddite analysis*. Ablex, NJ.

Wood, C. (2001) The electronic eye view. *Mclean's* 19 November, 94–7.

Wood, D. (2001) Algorithmic surveillance and social exclusion: an agenda for research. Paper presented at the 'New Technologies and Social Welfare' conference, University of Nottingham, UK, 17 December.