Prometheus, Vol. 24, No. 4, December 2006

Social Impacts of Transport Surveillance

MARCUS WIGAN & ROGER CLARKE

ABSTRACT *The transport sector is a natural focal point for surveillance measures to combat the threat of terrorism. It is also a complex environment that offers many examples of the social impacts of contemporary surveillance. Surveillance needs to be assessed against the standards used to justify other forms of security measures. The efficacy of many surveillance schemes, however, is in serious doubt. Justification for these schemes is commonly either lacking entirely or is unpublished and hence has not been subjected to critical evaluation. A small set of mini-cases is presented, in order to identify the social impacts of twenty-first century surveillance schemes that have been implemented as fear-driven responses to terrorist acts. Those impacts are argued to be seriously harmful to society. Trust is crucial to public acceptance of intrusive measures, but the absence of justification for surveillance, and of controls over abuses, is likely to see the rapid dissipation of trust, firstly in the assertions of national security and law enforcement agencies, and secondly in the politicians who have been rubber-stamping their demands.*

Keywords: trust; legitimacy; Intelligent Transport Systems (ITS); chilling effect; security; deterrence; interception; investigation; mass surveillance; object surveillance; area surveillance; location; tracking; anonymity; passport; data linkage; privacy impact assessment (PIA).

1. Introduction

The citizens of a number of countries are under threat from terrorist actions, or at least perceive themselves to be so as a result of statements by their governments. This mixture of real and perceived threat has enabled national security and law enforcement agencies in many of these countries to achieve extensions to their powers, resulting in a major shift in the balance between human rights and social control. Increased surveillance, and substantial spending on surveillance technologies have been conspicuous features during this phase. This paper considers the social impacts of this increase in surveillance by reference to the surveillance of transport systems.

Transport is an attractive area in which to concentrate investment in surveillance. The huge flows of people through public transport systems, airports and

Prometheus ISSN 0810-9028 print/ISSN 1470-1030 online © 2006 Taylor & Francis
http://www.tandf.co.uk/journals
DOI: 10.1080/08109020601029961

public spaces are subject to transport and traffic management systems. People and goods—including both dangerous goods and dangerous people—are dependent on transport to reach their destination—or their target. Moreover, large transport vehicles, in the form of ships (in Yemen), aircraft (in New York and Washington), buses (in Israel), trains (in London and Madrid), and trucks (in Iraq on a daily basis) are the means whereby criminals inflict damage and misery, and disrupt the confidence required by the community to use transport in order to go about their business and social activities.

In addition, there has been considerable investment in information infrastructure within the transport sector, under the rubric of Intelligent Transport Systems (ITS). In most cases, the justifications for the investment were originally economic or social, but the opportunities that they offer for national security purposes are now being grasped. For example, the National Centre for Intelligent Transport Systems focuses on advanced communications as a natural development of both ITS and the external needs for command, control—and surveillance.

Surveillance is, however, intrusive and demeaning. It signals that powerful organisations distrust people, and it encourages distrust by people of one another, and of organisations.[1] It creates a 'chilling effect' on various kinds of behaviour by various kinds of people. Whether the intended behaviours are chilled, or otherwise constrained, is a critical issue: in free and democratic nations, substantial impositions on people need to be justified, and to be seen to be justified. A primary motivation for this analysis is to assess the extent to which the justification exists, is being communicated, and is being subjected to critical assessment. This is particularly important in those countries where the actual risks are extremely low—particularly when compared to deaths and injuries on the road system (in Australia c. 1,600 p.a.), but even to deaths due to drowning (c. 200 p.a.) and assault (c. 200 p.a.), and possibly deaths due to bee and wasp stings (c. two p.a.) and shark attacks (c. one p.a.).

The continuing rare incidence of successful terrorist attacks may of course now be framed as either over-investment in anti-terrorist measures at a level inappropriate for the risks, or as a 'successful investment'. Claims of 'nil-event success' are easily made, but a naturally sceptical public needs to be convinced.

The paper commences by examining the ways in which surveillance represents an element of security strategy. It then surveys the field of transport surveillance, and examines the social impacts of transport surveillance. The aim throughout is to focus on issues that are relevant to surveillance generally. Conclusions are drawn about the extent to which surveillance, as it has been imposed in the context of 'the war on terrorism' rhetoric, has been publicly justified, and can continue to be imposed as it has been since September 2001.

2. The Positive Functions of Surveillance

This section examines the nature of surveillance as a security tool, and the benefits it can deliver. It first describes the notion of security safeguards, then defines surveillance, outlines the special cases of location and tracking, and places surveillance in the context of security safeguards generally.

2.1. The Purposes of Security Measures

The term 'security' is used in at least two senses: as a condition in which harm does not arise, despite the occurrence of threatening events; and as a set of safeguards

designed to achieve that condition. Threats exist, variously natural, accidental and intentional. Threatening events, in which a theoretical threat becomes real, give rise to harm. They do this by impinging on vulnerabilities, which are aspects of a system that render it susceptible to harm arising.

Safeguards or security measures can be devised to address threats, to monitor vulnerabilities, and to ameliorate harm. Security safeguards may be designed to perform one or more of the following functions:

- deterrence of unwanted behaviour (e.g. threats of punishment or retaliation);
- prevention of unwanted behaviour (e.g. controls on access to materials that can be used to prepare explosives);
- pre-emptive interception of acts preparatory to unwanted behaviour (e.g. road-blocks);
- interception of acts that themselves constitute unwanted behaviour (e.g. preclusion of vehicle access to particular zones, to prevent them from getting close enough to an intended target to inflict major damage);
- detection of instances of unwanted behaviour that have occurred (e.g. monitoring of explosions);
- investigation of instances of unwanted behaviour that have occurred (e.g. cordoning off of blast-zones to enable forensic examination);
- retribution for instances of unwanted behaviour that have occurred (e.g. prosecution for a criminal offence, vengeance attack, torture, execution);
- building of public confidence (e.g. announcements of investment in various safeguards such as port and aircraft security measures). These announcements may or may not have a clear nexus with measures that could have prevented past attacks or reduced their impact.

Any proposed security safeguard needs to be assessed, in order to understand what contributions it is capable of making to those functions, what conditions must exist for the objectives to be achieved, what susceptibility they have to countermeasures, and what new vulnerabilities they give rise to. Any security safeguard requires evaluation in terms of both its identifiable costs and other (to date almost invariably uncosted) social disbenefits such as its impacts on social behaviour, freedoms and privacy. These include not only the direct costs, but also the opportunity costs, by which is meant the opportunities that are foregone by committing specific resources to a particular security safeguard rather than to alternative uses.

2.2. Surveillance

The term 'surveillance' derives from the fraught times of the French Revolution at the end of the eighteenth century. It refers to the systematic investigation or monitoring of the actions or communications of one or more persons. It is useful to distinguish several categories:

- Personal Surveillance. This is the investigation or monitoring of an identified person. In general, a specific reason exists for the investigation or monitoring. It may be applied as a means of deterrence against particular actions by the person, or repression of the person's behaviour (e.g. identity cards linked to mass databases accessible by enforcement agencies; and electronic road pricing systems without a true anonymity option[2]);

- Mass Surveillance. This is the surveillance of groups of people, usually large groups. In general, the reason for investigation or monitoring is to identify individuals who belong to some particular class of interest to the surveillance organisation. It may also be used for its deterrent effects (e.g. the claims made about the feasibility of crowd facial recognition systems);
- Object Surveillance. This is the investigation or monitoring of an object of some kind, to detect movement or a change of its state (e.g. anti-theft image processing movement detection systems); and
- Area Surveillance. This is the investigation or monitoring of physical space, which may or may not include objects or people (e.g. CCTV, pedestrian counting systems, and proposed widespread sensor systems utilising grid computing).

The basic form of surveillance is physical, and comprises watching (visual surveillance) and listening (aural surveillance). Monitoring may be undertaken remotely in space, with the aid of image-amplification devices like field glasses, infrared binoculars, light amplifiers, and satellite cameras, and sound-amplification devices like directional microphones; and remotely in time, with the aid of image and sound-recording devices. In addition to physical surveillance, several kinds of communications surveillance are practised, including mail covers and telephone interception. The popular term 'electronic surveillance' refers to both augmentations to physical surveillance (such as directional microphones and audio bugs) and to aspects of communications surveillance, particularly telephone taps.

Since the explosion in the scale and accessibility of collections of data about things and people, data surveillance has developed as a convenient and relatively inexpensive approach to monitoring. Dataveillance is 'the systematic monitoring of people's actions or communications through the application of information technology'.[3] It depends on the acquisition of data, preferably streams of data, and preferably from multiple sources.

2.3. Location and Tracking

Some surveillance technologies support the location of specific objects or individuals in some space. Further, they may support tracking, which is the plotting of the trail, or sequence of locations, that is followed by an entity within that space, over a period of time. The 'space' within which an entity's location is tracked is generally physical or geographical; but it may be virtual, e.g. a person's successive interactions with a particular organisation.[4]

Due to timeliness limitations, data generated by a surveillance measure may only be able to be used for retrospective analysis of a path that was followed at some time in the past. A 'real-time' trace, on the other hand, enables the organisation undertaking the surveillance to know where the entity is at any particular point in time, with a degree of precision that may be as vague as a country, or as precise as a suburb, a building, or a set of co-ordinates accurate to within a few metres.

A person in possession of a real-time trace is in many circumstances able to infer the subject's immediate future path with some degree of confidence. Given an amount of data about a person's past and present locations, the observer is likely to be able to impute aspects of the person's behaviour and intentions. Given data about multiple people, intersections can be computed, interactions can be inferred, and group behaviour, attitudes and intentions imputed.

Location technologies therefore provide, to parties that have access to the data, the power to make decisions about the entity subject to the surveillance, and hence to exercise control over it. Where the entity is a person, it enables those parties to make determinations, and to take action, for or against that person's interests. These determinations and actions may be based on place(s) where the person is, or place(s) where the person has been, but also on place(s) where the person is not, or has not been. Surveillance technologies that support tracking as well as location extend that power to the succession of places the person has been, and also to the place that they appear to be going.

2.4. Surveillance as a Security Measure

Surveillance can be utilised as a security safeguard, but it is a safeguard of a very particular kind, and it requires careful assessment in order to appreciate what it can and cannot contribute, under what circumstances, and at what costs.

Surveillance is essentially an intelligence activity. It may be designed for any of several purposes:

- to anticipate a violation. For example, a package that has been stationary and unattended needs to be checked;
- to detect a violation. For example, unusual patterns of activity in a passageway may lead to the inference that violence is occurring. This may also play a role in anticipating further violation, e.g. because the violence may spread, or because the pattern of activity is sometimes associated with attempts to disguise or obfuscate;
- to assist in the identification of the person responsible for a violation, or in the authentication of an assertion as to the identity of the culprit.

Generally, a surveillance scheme designed for one of these purposes may not contribute a great deal to others. Security strategies based on anticipation of an action generally do not—and often cannot—work on the basis of verified or verifiable evidence, but rather on profiling, and on narrowing down the range of groups and individuals who might be planning an action, enabling pre-emptive measures.

The capacity of surveillance to assist with the performance of the various security functions identified in Section 2.1 above can be analysed as follows, with a very common traffic enforcement system used to provide immediately recognisable everyday examples:

- deterrence. Covert surveillance is unlikely to have much deterrent effect. On the other hand, if surveillance is known, or at least perceived, to be conducted, but the locations are unknown, then there may be a broad chilling effect on behaviour, at least of some categories of individual, or of some categories of behaviour. Overt surveillance may also have deterrent effects, but a considerable set of conditions needs to be satisfied. The relevant individual needs to know, and believe, that surveillance is being undertaken, and needs to consider that it represents a threat to themselves. It is of little value in the cases of crimes of passion, and in circumstances in which the individual is not concerned about being identified and found after the event. It therefore has no value whatsoever in the case of individuals committing suicide attacks. It is also known from various studies that surveillance tends to displace behaviour rather than to prevent it, and hence it is of limited value where vulnerabilities are widespread,

or otherwise exist outside the area that is subject to monitoring. For example, the use of dummy red light and speed cameras enhances the deterrent effects of actual visible and working cameras (although it has been shown that they need to be backed by random undisclosed cameras and speed measurement devices);

- prevention and interception. Surveillance by itself cannot prevent acts. It may be an element within a conglomerate of measures, which combine to prevent an act being performed. This depends upon the existence and maintenance of the relevant resources, effective linkage between the surveillance measures and the active components, and the ability of the active components to mobilise sufficiently quickly to prevent or intercept the act. For example, the use of widespread automatic number plate recognition depends on police on duty in vehicles to undertake interception;
- detection. Surveillance may provide a basis for establishing the fact that an event has occurred. This depends upon effective linkage of the monitoring activities with measures to record the data, and with (probably human) capabilities to appreciate the significance of the data. For example, automatic speed camera photographs may be examined visually after they are collated;
- investigation. Surveillance may provide information of assistance to an investigation into an event that has occurred. This depends upon effective linkage of the monitoring activities with measures to record the data, in a form accessible and useful to the investigator; for example, CCTV records on toll roads;
- retribution. Surveillance may provide a basis for taking action against the perpetrator of an event, or against the person responsible for the existence of the vulnerability that was impinged upon. This depends upon data quality. In a great many cases, for example, video-surveillance provides data whose evidentiary value is inadequate primary evidence in criminal cases;
- building of public confidence. Announcements of the existence of surveillance measures may bolster confidence that something is being done about the likelihood of threats becoming real, and doing harm.

Within this generic framework, the following section considers various forms of surveillance that are applied in the transport context.

3. Transport Surveillance

The term transport is used in this paper to refer to all forms of conveyance, whether intended for freight or for individuals, and irrespective of the mode, hence including road, rail, water and air transport. This section provides a brief survey of surveillance in transport as a whole, supplemented by mini-cases that provide insight into patterns of use, and impacts and implications.

3.1. The Nature of Transport Surveillance

Transport surveillance may be focussed on objects, including installations such as gates, vehicles, and items of cargo. Applications include video-recording, spatial logging of vehicle location and movement, and RFID usage in supply chains. Alternatively, surveillance may be undertaken of an area, such as a container loading-point, or an inter-modal interchange. A further focal point of monitoring activities is individuals, either directly, or by inference, based on their association with one or more areas, one or more objects, or both.

Surveillance designs that are concerned primarily with people include:

- in public transport:
  - transport smart cards that deny an anonymous option;
  - electronic tolling schemes that deny an anonymous option;
  - electronic passports;
  - service-denial blacklists such as 'no fly' lists (to date not apparent in some countries, although there have been some instances of judicially imposed denial of access to places such as sporting venues);

- in self-driven vehicles:
  - spatial logging of vehicles, and inference of the duration of movement and the location and timing of stops;
  - chip-enhanced drivers' licences capable of carrying, and disclosing, additional data;
  - automatic number plate recognition (ANPR) schemes;
  - medical alert systems linked to vehicles;
  - driver monitoring via engine management chips;
  - time use surveys of individuals using GPS technologies;

- as consumers:
  - RFID usage in supply chains extended to product-purchaser monitoring;
  - purchase of regulated goods such as explosives;

- as workers involved with freight movement:
  - positive vetting;
  - location and activity monitoring.

Such elements of transport-related surveillance create the scope for enormously detailed and precise surveillance of individuals' movements, activities, and personal and business linkages. The privacy impacts of these measures are potentially quite extreme, because they create intensive trails which create the scope for location and tracking, and hence they create the scope for many additional applications for many additional purposes.

Surveillance to assist with security has long been a major issue in goods transport, as loads may be very valuable, and loads may be dangerous. The monitoring of freight transport vehicles has long been accepted as appropriate, and the side-effect of driver surveillance has been worked through over quite some time, starting with automatic vehicle logging systems, in order to achieve an acceptable balance.[5]

But surveillance is now being extended to encompass the great many individuals associated with transport of loads into and out of ports and interchange facilities. This draws into the surveillance net people who are far removed from the driving task. Whereas the monitoring of road transport drivers and train drivers was the subject of prior consultative processes and negotiated and balanced features, these extensions have not had the benefit of such interactions.

3.2. Mini-case: Speed Management

Speed management strategies can be developed in several different ways. For example, the use of covert cameras has been shown to be effective in securing

generally lower traffic speeds, and to be more effective than the use of cameras whose locations are publicly declared. Overt cameras, on the other hand, act as a warning-marker for high-risk locations. The use of covert cameras, especially in what are apparently safe areas and locations, has the effect of reducing public trust in the reasonableness of the speed management strategy. This must be balanced against the general effect of reduction of the speed environment as a whole.

This tension has much in common with surveillance and security strategies, where the pin-pointing of the covert surveillance can undermine the deterrent effect of the strategy, whereas if it is not disclosed at all then the general impact will be lower than if it is intensively focussed on specific locations or systems. This tension between community trust and general effectiveness and deterrence needs to be finely balanced, as indeed is evident in the continuing public debates about speed camera strategies, which oscillate between visible deterrence and systems-wide general impact targets. The system-wide effects of covert enforcement are significant in terms of behavioural modification, but one price of this strategy is a greater distance between the police and the community.

Distinctions need to be drawn between different groups involved in transport. Those employed in transport appreciate that some controls need to be imposed, whereas for the general public a quite different set of standards applies. For example, a fleet management system that can launch alerts when a truck-driver is speeding is perceived very differently to the same system applied to private vehicles.

There are similarities between the security strategies of direct after-the-event prosecutions and pre-event actions based on probabilities and the speed strategies. The speed strategies of direct, credible and immediate on-the-spot enforcement strategies and their clear nexus with civil law, evidence and intent and the system-wide covert automated penalty approach which leaves many weeks between event and reinforcement are both still capable of civil demonstration and evidence, while pre-emptive security actions are not, and cannot be.

In short, the medium-term effectiveness of surveillance schemes is dependent upon social acceptance and trust.[6]

3.3. Mini-case: Automatic Number Plate Recognition

One automated enforcement system that is attracting much attention at present is Automatic Number Plate Recognition (ANPR). This involves a camera stationed near a road, capturing images of the number plates of passing vehicles, using pattern-matching recognition—in a manner similar to Optical Character Recognition (OCR) for documents—and making the data available to back-end applications.

ANPR data can be used to automatically generate and despatch notices of speed violations, and to charge vehicle-owners for road-usage. ANPR can also be used to compare passing registration-numbers against a 'blacklist', reflecting, for example, cars that have been reported as being stolen (and whose numbers have not yet been deleted from the database), or cars that are subject to an alert because they are recorded as having been used in the past by a person who is the subject of personal surveillance. This capacity is already in use in the UK, and has been touted as '[future] infrastructure across the country to stop displacement of crime from area to area and to allow a comprehensive picture of vehicle movements to be captured'.[7] It has been mooted by at least two State Governments in Australia.

A 'hit' on the blacklist may be used merely to generate a record for future data-mining, or to trigger action by law enforcement agencies, e.g. to intercept the

vehicle on the basis of the suspicion generated by the entry in the database. These schemes have been introduced with little or no public involvement, little or no discussion in parliaments, and without any apparent controls over use, abuse, data retention and function creep.

3.4. Mini-case: The Chip-based Passport

> A passport was originally a document, provided by a sovereign to an individual, which requested officials at borders and in seaports to permit the bearer to enter. The notion was known to English law at least as early as 1300. At the end of the nineteenth century, passports were issued on request, by the governments of various countries, in order to provide evidence of nationality, and, by implication, of identity. But there were few circumstances in which it was actually necessary to have one, even when crossing national borders. After World War I, in a climate of mass movements of displaced persons, it became increasingly common for governments to demand documents which evidenced a person's nationality. An international conference in 1920 established the present passport system. During the inter-war period, the passport became a near-universal requirement for international travel. It has remained so.[8]

Government agencies have grasped the opportunity presented by the post-September 2001 terrorism 'managed hysteria' to arrange parliamentary approval for a new form of passport that embodies various technologies. In Australia, the Passports Office actively avoided making information available to the public, and indeed to the Parliament. Even after the new scheme was launched in October 2005, the information made available remains scant.[9]

It appears that the document includes a contactless chip, which contains at least the same personal data as the printing on the document and the previous magnetic-strip, but in a form that is machine-readable provided that the reader has access to a cryptographic key. The original proposals were subject to enormous vulnerabilities of a privacy nature, extending to the point of facilitating identity theft. The protections ultimately implemented are claimed to be compliant with a (hastily flung together) specification approved by an international association of governments.[10] If effective, then the worst of the data-leakage problems in the original proposals have been overcome, but it remains unclear what additional data the chip contains now, what it may contain in the future, and who will be permitted the capacity to access the data.

Among the powers that the Department achieved by submitting a replacement statute for brisk and almost entirely unconsidered approval by acquiescent law-makers was the freedom to implement biometrics, in whatever manner the Department may see fit, subject only to convincing their own minister of the day. This was done in such a manner as to avoid even mentioning the word or concept of biometrics in the relevant s.47. This represents an extraordinary delegation of power to public servants.

The mythology used to produce time-pressure for the provision in the Bill was that a chip-based scheme carrying a biometric was necessary to retain Australian status under the US visa-waiver programme for short-term visits. This was simply presumed to be extremely important. It is unclear how significant the claimed justification is, even for the small minority of Australians who do business in the US or travel there as tourists, and it appears never to have been subjected to analysis or public consultation.

The Department of Foreign Affairs[11] state that 'facial recognition technology is being introduced to coincide with the release of the ePassport'. On the other hand, the accompanying press release of 25 October 2005 said circumspectly that the new passport 'will enable the implementation of cutting-edge facial recognition technology'; so it is unclear whether and when the Department has implemented it.

Facial recognition technology has been trialled in the SmartGate scheme run by the Australian Customs Service (ACS). In responding to criticisms of the technology's effectiveness,[12] ACS has acknowledged that it is not a security feature, but rather a 'customer service' feature. The inadequacies of the facial recognition technology appear likely to be used as an excuse to implement successive biometric schemes, progressively creating a government-controlled pool of biometrics of Australians, available for sharing with friendly governments, and other strategic partners.

The passport has been transformed into a general identity document, with apparently enhanced credibility through the inclusion of a biometric element. This creates the risks of wider permeation of biometric identifiers, and of function creep towards use in circumstances other than at national borders. The Australian Parliament has permitted an enormous leap in the power of the State over individuals. The ability of an agency to achieve these wide and uncontrolled powers, without so much as the pretence of public consultation and debate, augurs very ill for the survival of freedom of anonymous movement within the country's borders.

3.5. Data Linkage

The examples outlined above need to be seen in the context of widespread endeavours to pool personal data sourced from different programmes. The tracking of identified individuals generates increasingly intensive data sets. The existence of data about movement paths creates risks in relation to dangerous cargo, valuable cargo, and persons of interest. Further, through correlation of locations and times in entries for one person with the entries for another person, social networks can be inferred, at least with probabilistic confidence.

The many transport surveillance applications produce multiple data-trails. Linkages and correlations across depot, toll-road, ANPR and public transport schemes, for example, are capable of generating yet more detail about a person's movements and habits. Such intrusiveness is a matter of sensitivity to corporate strategists, deal-makers and salesmen as much as it is to individuals in less exalted occupations. Those who have in mind to exercise rights of political speech and action are increasingly likely to be confronted by this data, directly from national security and law enforcement agencies, or more likely via their employers, benefit-paying agencies, and grants administrators.

Collections of tracking data are capable of being linked with data from other sources, variously for personal data surveillance (of a suspect), or for mass data surveillance (in order to generate suspects). Data may be acquired from many sources, such as consumer marketing databases, government registers, and health systems. The operator of each such system is tempted to seek additional sources to link with their own, and barter is an attractively low-cost approach. Data protection laws are already very weak, and are easily subverted and amended. They represent no significant barrier for powerful corporations and government agencies.

The explosion in surveillance opportunities needs to be seen in the light of strenuous efforts to destroy the longstanding norm of anonymity in both travel,

and the conduct of large-volume/low-value transactions. In the space of a decade, public transport tickets and toll-road payments have been changed to preclude cheap and convenient travel in the absence of an authenticated identifier—simply through refusal to accept payment other than by credit card and debit card. Such cards are subject to 100-point checks as a result of function creep applied to measures that were implemented ostensibly to enable the monitoring of money-laundering. Those schemes have been in place for years, with barely any significant results. The solution has, of course, not been to admit that they do not work, but rather to claim that they will, provided that they are extended yet further.

Some uses of anonymity and multiple identities are for criminal or anti-social purposes, but the vast majority are harmless to society and important to individuals. Examples of people for whom multiple identities are a matter of sheer physical safety include undercover national security and law enforcement personnel, protected witnesses, psychologists and counsellors.

Transport-based security systems targeting people, whether directly or only incidentally, are capable of rapidly breaking down longstanding protections. It is remarkable that schemes could have been introduced so blindly, without a debate as to how society handles these important issues.

4. Social Impacts of Transport Surveillance

The examples of transport surveillance outlined in the previous section evidence a wide range of serious social impacts and implications. They have not yet been subjected to a coherent evaluation of their privacy impacts; nor have the broader social effects of such systems yet been thought through.

A study of surveillance in other settings would appear very likely to generate a long list of comparable problems. For example, some access control systems to premises and to computer-based systems are being linked to criminal records (in such areas as registration of teachers and child-care workers), and to health records (e.g. for pilots and train-drivers). Such inter-system data linkages open up high probabilities of misuse, and of automated errors arising from conflicts and ambiguities in identity-matching, and in data definition, accuracy, precision and timeliness. They therefore give rise to many forms of socially expensive stress.

Consideration of these schemes leads to a number of inferences about their design features:

- there is a widespread lack of appreciation of the distinctions between law enforcement and national security activities, despite the fact that they have fundamentally different philosophies, justifications and processes. Law enforcement is aimed at accurate identification of an offender, presentation in court of evidence of that person's guilt, withstanding the person's legal defences, and securing conviction. National security, on the other hand, is largely anticipatory, is based on suspicion at least as much as evidence, and is seldom able to be defended against. These philosophies collide in any integration process, giving rise to social issues and economic costs;
- there is insufficient understanding that the 'chilling' of behaviour that is perceived to be 'deviant' creates the risk that the behaviour of other people will be modified as well, in ways that are harmful to individuals, and to society. Innovation and progress in all walks of life are fundamentally dependent on behaviour that is (initially) perceived to be 'deviant';

- there is an implicit presumption by policy-makers and designers that individuals are to be forced to use just one identity. This is despite the widespread usage and long history of, and common law support for, multiple identities. Existing law recognises only offences that involve the abuse of multiple identities, e.g. to enable fraud. The safety of psychologists, for example, particularly in highly-charged areas such as the family court, is dependent on the avoidance of discoverable links between their professional and private identities and addresses;
- there is a further implicit presumption by policy-makers and designers that individuals are to be denied anonymity, and even denied strong forms of pseudonymity.[13] They thereby become exposed to authority, and to every other organisation that can negotiate or otherwise gain overt or covert access to the relevant data;
- surveillance schemes are being developed without any guiding philosophy that balances human rights against security concerns, and without standards or guidance in relation to social impact assessment, and privacy design features.

In addition, control issues emerge:

- there are very limited constraints on abuses of surveillance systems (in such forms as independent oversight, audit, investigative resources and activities, criminal sanctions and enforcement). There has always been a shortfall in controls of these kinds, but the freedoms granted to national security and even law enforcement agencies in enactments passed during the last several years by parliamentarians 'asleep at the wheel' far exceeds previous levels of laxity;
- there are very limited constraints on the linkage and consolidation of data-holdings and identities, and the associated destruction of protective 'data silos' and 'identity silos';
- there are very limited constraints on 'function creep';
- there are very limited constraints on the data-mining of organisations' own holdings and of consolidated databases. This is despite the enormous risks involved in drawing inferences from highly heterogeneous data drawn in highly varied ways from highly diverse sources, each of which was designed for narrow, specific purposes;
- there is a desperate shortage of credible audits of the performance of surveillance schemes, and of their compliance with such control mechanisms as exist. Privacy Commissioners and other nominal regulators, when starved of funding, commonly treat their audit programmes as the first sacrifice.

There are clear antidotes to these ills. Techniques for the evaluation of proposals for technology applications are well-established, in such forms as cost–benefit analysis and the more appropriate cost–benefit–risk analysis.[14] The stakeholder concept is well-known to encompass not just government agencies, technology providers, and business 'partners', but also affected individuals. The process of privacy impact assessment (PIA) is well-established.[15] Focus-group techniques are available. Representative and advocacy organisations are available to consult with, and the principles that guide effective community information and consultation processes are well-known. Agencies have no excuses for failing to inform and failing to consult, but some, such as the Attorney General's Department, often prefer to ignore public opinion, and exercise their power.

What is lacking is not the ability to specify appropriate processes, but rather courage on the part of parliamentarians to ask hard questions, and to say 'no' to the national security community. It could be argued that courage is also lacking on the part of senior executives, who are failing to oppose excessive demands from national security and law enforcement agencies, but social control is a primary motivation for many senior government executives. Carriage of the original Australia Card proposition was after all with Health, supported by Treasury and to some extent Social Security and Immigration.[16] The mandarin class appears to subscribe to the belief that there will be a 'trickle-down effect' from the recent spate of authoritarian initiatives, which will benefit mainstream agencies.

5. Conclusions

Transport security systems eat into the social space, and they have been doing so in an unaccountable manner. It is far from clear that the ostensible reasons for their introduction are justified, and the well-established practice of function creep is steadily eroding the credibility of Government claims for various forms of new cards. Their extended application would be even more intrusive and threatening.

Proposals for new and enhanced surveillance schemes, in transport as elsewhere, must be measured against the norms of security analysis and design. It is clear that the dependence on rushed presentation of proposals to ministers and the Parliament under the guise of 'measures necessary in order to conduct the war on terrorism' have been a smokescreen for the absence of any such assessments having been undertaken even behind the closed doors of national security agencies.

The agencies that are imbued with the surveillance and intelligence culture are utilising their opportunity to the utmost, and can be expected to extend the window as long as they can. They have little interest in ceding the ground they have won through the fog of misinformation. What community leaders must now do is appreciate the massive harm that surveillance measures are doing to public confidence in its institutions.

It is increasingly obvious to the public that not only are there few wolves to cry out about, but the impediments that have been built are impediments to normal activities of normal people, not to the violent activities of such terrorists and latent terrorists as exist in this country.

The lack of legitimacy will rapidly undermine the preparedness of the public to accept substantial constraints that are available for government control of miscreants, but are of little or no value in combating the claimed terrorist threat. Recourse to the excuse of 'drug barons' and 'organised crime' is on similarly thin ice, because of the failure of data surveillance in particular to bring them to book. The collapse in confidence will accelerate as abuses come to attention, and as the reality of the various schemes' privacy-threatening features and lack of controls hits home.

Community trust in the State cannot be sustained in the absence of transparency. Individuals and communities are being precluded from contesting claims made by the State of the necessity of extremist measures. The lessons of the speed campaigns of the last 20 years makes it all too clear that this is a pivotal point, as community social capital is inevitably undermined by intelligence-based pre-emptive actions.

Cooperation by the public, and by the workers whose job it is to operate and maintain such schemes, can be withdrawn at short notice if trust is not established and maintained. The integrity of surveillance schemes, in transport and elsewhere, is highly fragile.

The last few years have seen a headlong rush to secure national infrastructure, and to protect people's physical safety from major acts of violence. This movement embodies major risks to society. The right of freedom of anonymous movement within the country has been suddenly and substantially compromised. The freedoms to be, to think, and in most circumstances to act differently from other people, and privacy and civil rights more generally, are being destroyed, not by terrorists, but by 'friendly fire'.

It is vital that Australians energetically resist not only religious fundamentalism but also national security fundamentalism. Transport surveillance is a vital field in which public resistance against highly intrusive and inadequately justified measures can be confidently anticipated.

Notes and References

1. R. Clarke, 'Information technology and dataveillance', *Comm. ACM*, 31, 5, May 1988. Republished in C. Dunlop and R. Kling (eds), *Controversies in Computing*, Academic Press, 1991. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html. All URLs were accessed in April 2006.
2. M. R. Wigan, 'Problems of success: privacy, property, and transactions', in L. Branscomb and J. Keller (eds), *Converging Infrastructures: Intelligent Transportation and the NII*, MIT Press, 1996.
3. Clarke, 1988, *op. cit.*; R. Clarke, 'Dataveillance-15 years on', *Proceedings of the Privacy Issues Forum*, New Zealand Privacy Commissioner, Wellington, 28 March 2003a. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html.
4. R. Clarke, 'Person-location and person-tracking: technologies, risks and policy implications', *Information, Technology & People*, 14, 2, Summer 2001, pp. 206–231. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html.
5. Wigan, 1996, *op. cit.*
6. M. Daniel, M. J. Webber and M. R. Wigan, 'Social impacts of new technologies for traffic management', *Australian Road Research Board, Research Report ARR* 184, 1990; M. R. Wigan, 'The realizability of the potential benefits of intelligent vehicle-highway systems: the influence of public acceptance', *Information, Technology & People*, 7, 4, 1995, pp. 48–62.
7. S. Connor, 'Britain will be first country to monitor every car journey', *The Independent*, 22 December 2005. Available at: http://news.independent.co.uk/uk/transport/article334686.ece.
8. R. Clarke, 'Human identification in information systems: management challenges and public policy issues', *Information Technology & People*, 7, 4, December 1994, pp. 6–37. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html.
9. DFAT, *The Australian ePassport*, Department of Foreign Affairs, undated but apparently of October 2005. Available at: http://www.dfat.gov.au/dept/passports/.
10. ICAO, *Biometrics Deployment of Machine Readable Travel Documents: Annex I-Use of Contactless Integrated Circuits*, International Civil Aviation Organisation, May 2004. Available at: http://www.icao.int/mrtd/Home/Index.cfm.
11. DFAT, *op. cit.*
12. See, for example, R. Clarke, *SmartGate: A Face Recognition Trial at Sydney Airport*, Xamax Consultancy Pty Ltd, August 2003b. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/SmartGate.html.
13. R. Clarke, 'Identified, anonymous and pseudonymous transactions: the spectrum of choice', *Proceedings of the User Identification & Privacy Protection Conference*, Stockholm, 14–15 June 1999. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html.
14. R. Clarke & K. Stevens, 'Evaluation or justification? The application of cost/benefit analysis to computer matching schemes', *Proceedings of the European Conference in Information Systems* (ECIS'97), Cork, Ireland, 19–21 June 1997. Available at: http://www.anu.edu.au/people/Roger.Clarke/SOS/ECIS97.html.

15. R. Clarke, *Privacy Impact Assessment Guidelines*, Xamax Consultancy Pty Ltd, February 1998. Available at: http://www.xamax.com.au/DV/PIA.html.
16. R. Clarke, 'Just another piece of plastic for your wallet: the "Australia Card" scheme', *Prometheus*, 5, 1, June 1987. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html.