Chapter 4

Surveillance, Employment and Location
Regulating the Privacy of Mobile Workers in the Mobile Workplace

Colin Bennett

1. Introduction

The range of complex issues embraced by the term ‘privacy protection’ has assumed a primary place on the political agendas of virtually every advanced industrial state. Few governmental or industry initiatives do not have some implication for the collection and processing of personal information. New practices, such as video-surveillance cameras, biometrics, smart identity cards, drug-testing, telemarketing, genetic databanks, Radio Frequency ID (RFID) and so on, can have intended and unintended consequences for the protection of personal information. Surveillance practices are changing in kind as well as degree. Thirty years ago, citizens were normally aware when personal information was being collected. Now the process of information gathering is more surreptitious. In our everyday roles as citizens, consumers, travellers, patients, students, recipients of social benefits, and employees (the subject of this paper), we continuously and unawares leave fragments of personal data behind us (Cavoukian and Tapscott, 1995).

Privacy protection in the workplace has always featured prominently in the literature on this subject. Although it is impossible to measure individuals have probably always been subjected to higher levels of monitoring and surveillance within the workplace, than without, because employers have generally asserted a greater discretion to observe the actions of “their” workers on “their” property. Of course, the tension between the manager’s desire to know and the employee’s right to privacy has a long history. In the 19th century employee surveillance was even regarded as a progressive method of improving worker productivity, and hence improving workers (Rule, 1996:66).
Yet the methods of workplace surveillance have changed so dramatically that they have led to more dire warnings about the corrosive effects of excessive surveillance upon the workplace environment and the rights of workers (e.g. Garson, 1988; Zuboff, 1988). In keeping with contemporary obsessions with reducing “risk,” public and private organisations have sought corresponding mechanisms to reduce these risks when dealing with the labour market. They share human resource data on prospective employees. They require extensive medical checks, and in some cases, drug and genetic-testing. They oversee work performance through techniques such as key-stroke monitoring, and call-monitoring software. They try to detect slackers and wasters of organisational time, through video-surveillance cameras, and e-mail monitoring software. And they attempt to create a secure environment by monitoring the comings and goings of the workforce through the use of a variety of identification devices, some of which might include biometric identifiers. If a new surveillance technology has been invented, it will, to be sure, become deployed in the workplace.

The central aim of this paper is to review how the rights of the worker in the workplace have been, and can be, regulated in different countries under the principles and instruments of privacy protection. The first section reviews some of the key conceptual issues in order to demonstrate how the policy debates in different countries have tended to be informed by a particular definition of “information privacy” or “data protection.” In the early 1970s when governments were first trying to tackle this question, certain assumptions were made about how one can, and cannot, provide a workable set of information privacy rights for citizens. These assumptions have underpinned most of the policy activity in Western societies throughout the succeeding decades and have led to a general acceptance of a set of “fair information principles” (FIPs) that appear in most international and national legal regimes. Privacy protection policy now comprises a lot more than law, however. An inventory of international, regulatory, self-regulatory and technological “policy instruments” are now at the disposal of government, business and individual citizens (Bennett and Raab, 2003). The paper then applies this framework to the range of instruments currently used to protect workplace privacy, together comprising an inventory of policy instruments designed to place some controls on the collection, processing, and disclosure of personal information by employers about employees.

This paper argues that the privacy protection issue generally, and the workplace privacy issue specifically, are undergoing a further paradigm shift as a result of the introduction of technological practices that permit a precise tracking of an individual’s location and movement. Organisational interests are now no longer confined to understanding individuals and their behaviours in static terms. Rather public and private agencies might have significant interests in knowing not only where we are, but also what we do, and how our behaviours, preferences, needs, and identities change as a result of location (e.g. Tuan, 1982). This shift has significant implications for the definition of the “workplace” and for the protection of “workplace privacy.”

At the heart of these debates is the proliferation of the cellular (mobile) phone, and associated technologies such as Personal Digital Assistants (PDAs) and onboard vehicle telematics systems. The monitoring and tracking of movement, particularly in vehicles, is posing considerable challenges to employee privacy rights and raising a range of new and difficult questions for regulators. Under what circumstances should mobile telecommunications devices be used by employers to pinpoint an employee’s location? What should happen to this data? With whom may it be shared? For what secondary purposes might it legitimately be used? The answers to these questions, however, do not lie in abandoning or revising the theory of information privacy, but to ensure that those principles are properly translated into organisational practices.

2. Information Privacy and the Fair Information Principles (FIPs)

The concept of informational privacy arose in the 1960s and 1970s at about the same time that “data protection” (derived from the German, Datenschutz) entered the vocabulary of European experts. The value was inextricably connected with the information processing capabilities of computers, and to the need to build protective safeguards at a time when large national data integration projects were being contemplated in different European, North American and Australasian states. These projects raised the fears of an omniscient “Big Brother” government with unprecedented surveillance power. Although concerns differed among these countries, a closely-knit group of experts coalesced, shared ideas, and generated a general consensus about the best way to solve the
The Ethics of Workplace Privacy

problem. These efforts led to the world’s first “data protection” or “information privacy” statutes (Bennett, 1992; Bennett and Raab, 2003; Bygrave, 2002; Flaherty, 1989).

The overall policy goal in every country has been to give individuals greater control of the information that is collected, stored, processed and disseminated about them by public, and in most cases, private organisations. This goal was prominent in English-speaking countries, as well as in Germany, where the concept Informationsselbstbestimmung (informational self-determination) was later developed and given constitutional status. This goal also necessitates making a distinction between the subject of the information (the data subject) and the controller of that information (the data controller). Despite some interesting debates about the application of economic, or property-based, models to give individuals greater control over “their” information (Rule and Hunter, 1999; Lessig, 1999), it has been hard to resist the conclusion that only regulatory intervention might redress the power imbalance between the data subject and the data user. Consequently information privacy has been generally defined as a problem for public policy, rather than an issue for private choice.

Once these, and other, assumptions are accepted about how one can and cannot develop public policy on privacy, a logic is set in motion that leads to a basic set of key and basic statutory principles. The historical origins of the “Fair Information Principles” (FIPs) can be briefly traced to policy analysis in Europe and the United States in the late 1960s and early 1970s (Bennett, 1992:95-115). While the codification of the principles may vary, they essentially boil down to the following tenets (Bennett and Grant, 1996:6): An organisation (public or private):

- must be accountable for all the personal information in its possession
- should identify the purposes for which the information is processed at or before the time of collection
- should only collect personal information with the knowledge and consent of the individual (except under specified circumstances)
- should limit the collection of personal information to that which is necessary for pursuing the identified purposes
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the finality principle)
- should retain information only as long as necessary

- should ensure that personal information is kept accurate, complete and up-to-date
- should protect personal information with appropriate security safeguards
- should be open about its policies and practices and maintain no secret information system
- should allow data subjects access to their personal information, with an ability to amend it if inaccurate, incomplete or obsolete.

These principles are, however, relative. However conceptualised, privacy is not an absolute right; it must be balanced against correlative rights and obligations to the community, although the concept of “balance” and the process of “balancing” are highly ambiguous (Raab, 1999).

Despite harmonisation there are, of course, continuing debates about how the FIPs doctrine should be translated into statutory language. There are disputes for example: about how to regulate the secondary uses of personal data – through a standard of relevance, or through specific provisions about legitimate custodians; about the limitation on collection principle and to what extent the organisation should be obliged to justify the relevance of the data for specific purposes; about the circumstances under which “express” rather than “implied” consent should be required; and about the distinction between collection, use and disclosure of information, and whether indeed these distinctions make sense or should not be subsumed under the overarching concept of “processing.” How these and other statutory issues are dealt with will, of course, have profound implications for the implementation of privacy protection standards within any one jurisdiction.

The laws have also differed on the extent of organisational coverage – those in North America and Australia have historically mainly regulated public sector agencies, whereas those elsewhere (especially in Europe) encompass all organisations. This distinction is rapidly changing, however, as countries like Canada, Australia and Japan have moved to regulate private sector practices. Laws have also differed in the extent to which they regulate non-computerised files, but this distinction is also eroding. Most notably they have differed with regard to the policy instruments established for oversight and regulation (Flaherty 1989; Bennett, 1992). Most countries (with the notable exception of the United States) have set up small privacy or data protection agencies with varying oversight, advisory or regulatory powers. Some of these agencies have strong enforcement and regulatory powers; others act as more advisory “ombudsman-like” bodies. Some are headed by a collective
commission (such as in France), others by a single “Privacy Commissioner” or “Data Protection Commissioner.”

It can be finally noted that this deep and extending consensus surrounding the FIPs doctrine has occurred against a backdrop of some profound scepticism as to whether it can actually protect personal privacy and stem the inexorable tide of surveillance. Authors who have examined the issue from a broader sociological perspective have continuously raised the concern that contemporary information privacy legislation is designed to manage the processing of personal data, rather than to limit it. More broadly, David Lyon has contended that “the concept of privacy is inadequate to cover what is at stake in the debate over contemporary surveillance” (Lyon, 1994:196). From the perspective of those interested in understanding and curtailing excessive surveillance, the formulation of the privacy problem in terms of trying to strike the right “balance” between privacy and organisational demands for personal information hardly addresses the deeper issue. Information privacy policies may produce a fairer and more efficient use and management of personal data, but they cannot control the voracious and inherent appetite of modern organisations for more and more increasingly refined personal information (Rule et al., 1980), increasingly extracted through more intrusive technologies that are altering the very boundaries between the self and the outside world.

3. From Privacy Law to Privacy Policy Instruments

Any observer of the privacy issue in the 1970s and 1980s might have concluded that the fundamental requirements of a national privacy policy were: a statutory codification of the fair information principles, an application to every public and private organisation, a coverage of all forms of personal data, regardless of sensitivity and context, and oversight and enforcement by an independent data protection agency. These conditions were generally seen as necessary and sufficient for the implementation of privacy protection policy (Bennett and Grant, 1999:7).

The privacy analysts of the 1990s and beyond, however, have questioned these assumptions and invoked the importance of other supplementary “policy instruments.” A conventional wisdom emerged in the 1990s that data protection required something more than a ‘one-size-fits-all’ solution. According to this view, good privacy protection involves the application of several instruments, considered as a ‘privacy toolkit’, a ‘mosaic of solutions’, or a ‘regulatory mix’, all suggestive, but perhaps misleading, metaphors for combined approaches to data protection (Bennett and Raab: ch. 8).

Four sets of policy instruments have, at one time or another, been considered part of this “toolbox,” “mosaic” or “mix.” On the most general level there are a range of international instruments, designed to regulate the flows of personal data across national borders. The increasing ease with which personal data might be transmitted outside the borders of the country of origin has produced an interesting history of international harmonisation efforts, and a concomitant effort to regulate transborder data flows. In the 1980s, these harmonisation efforts were reflected in two international agreements, the 1981 Guidelines from the Organisation for Economic Cooperation and Development, and the 1981 Convention from the Council of Europe. In the 1990s, these efforts were extended through the 1995 Directive on Data Protection from the European Union which tried to harmonise European data protection law according to a higher standard of protection, and to impose that standard on any country within which personal data on European citizens might be processed. These provisions, above all, have dictated the content of the world’s data protection law (Bennett and Raab, 2003: ch. 4).

A second set of regulatory instruments embraces the comprehensive data protection statutes, within which the fair information principles appear either explicitly or implicitly, including those in the US, Australia, New Zealand and Canada that are called ‘Privacy’ Acts. Data protection law has diffused rapidly around the advanced industrial world in the 1980s and 1990s, and societies more commonly characterised as “developing” are now beginning to pass similar laws. But regulation can also occur on a sectoral level, particular in the United States which has eschewed the European approach in favour of specifically targeted legislation on especially sensitive sectors (such as credit-reporting, health, and telecommunications).

A third set of instruments can be roughly described as “self-regulatory” even though the lines between regulation and self-regulation are not distinct. Within this category, we can distinguish between:

- **privacy commitments** – simple statements of policy, often appearing on websites;
- **privacy codes** – more formal and codified expressions of an organisation’s or association’s policy;
- **privacy standards** – which normally include procedures for independent conformity assessment; and
- **privacy seals** – the “good house-keeping seals of approval” that are awarded once an organisation has committed to, and demonstrated, an appropriate level of privacy awareness and compliance.
This typology expresses a neat cumulative logic. In practice, organisational attempts at self-regulation are more haphazard and incoherent (Bennett and Raab, 2003: ch. 6).

A final set of instruments are technological. Originally considered part of the “problem,” information technologies can now be designed to enhance privacy protection. Technological instruments come in three forms. Systemic instruments are deeply embedded within the architecture of different systems; Reidenberg (1998) refers to such instruments as “lex informatica.” Collective instruments are developed through central policy direction, either by the state or by large corporations. Public-key infrastructures (PKI) for service delivery are the most important examples. Instruments of individual empowerment require explicit choices by end-users. Examples would be the encryption, anonymising and filtering instruments commercially available for Internet users (Bennett and Raab, 2003: ch. 7).

The plurality of instruments is accompanied by a concomitant plurality of actors. Raab (1997) has discussed the co-regulation or “co-production” of data protection, involving broader and multiple relations within and across jurisdictions, organisations and instruments. We now need to acknowledge the relevance of more actors than those who were on the privacy policy stage in the 1970s and 1980s. They include consumer organisations, the media, academics, and privacy advocates. Each of these actors is involved in the “Governess of Privacy” (Bennett and Raab, 2003). But how are these instruments and actors manifested in the context of workplace privacy?

4. Privacy Policy Instruments in the Workplace

In some respects, the fair information principles mean one thing in our role as citizens, and another in our role as workers or employees because it is difficult to assert a claim that employers have no management-related justifications for monitoring employees. They have interests in improving the efficiency and profitability of the organisation, in protecting the health and safety of workers, consumers and the public, in deterring and controlling abuse of the employment relationship, in complying with regulatory requirements, and in promoting certain public-interest considerations (Craig, 1999:26-33). The “balancing” process between an employee’s right to privacy, and the employer’s right to know, is inherently different from that within other organisational/individual relationships.

In the employment context, the inappropriate collection, use and disclosure of personal information can have very adverse consequences for the current and future prospects of an employee. Over and above the information privacy interests of workers, there are other privacy issues concerned with territorial privacy; even within the workplace, workers deserve some private space (in the bathroom, in the changing room, in their personal lockers). They also have certain important privacy interests over their bodies (corporeal privacy). Thus, employer claims about drug-testing, must be qualified by important limitations on the processes by which bodily fluids are extracted (Craig, 1999:18). The extraordinary and expanding scope of employee surveillance means that these “balancing” tests need to be applied with enormous sensitivity to the employment context, and to the ethics of the methods employed (Marx, 1999).

Of course, employees may already find themselves in a dependent relationship over which a long tradition of international and domestic labour law exerts an influence. Therefore, it is not simply the theory of information privacy, as outlined above, that frames the various legal and policy options. Craig (1999:53-54) demonstrates that workplace privacy is inextricably connected with competing schools of management theory. A “collective laissez-faire approach,” for instance, discourages both legislative and judicial interference with freedom of contract, except in cases where collective representation is unlikely to yield industrial stability or justice. A “market individualism approach” asserts that state interference should be opposed, because only freedom of contract can promote the flexible environment necessary for economic growth. A “floor-of-rights approach,” by contrast, supports the enactment of basic rights and standards for the benefit of candidates and employees. Clearly, if one accepts Craig’s “floor-of-rights” approach, then a space is opened up for the imposition of legislative and judicial standards for workplace privacy. The other two approaches would, to differing degrees, assert that, if a worker is dissatisfied with the level of surveillance within a particular job, then she/he can always resign and seek employment elsewhere. Thus, an analysis of the policy instruments for the protection of workplace privacy is also affected by wider considerations about the appropriate role that the state should play in regulating the employee/employer relationship. And those considerations will obviously vary over time and jurisdiction.

Having said that, it is also obvious that workplace privacy rules have emerged less from pressure from unionised labour, and more from international and domestic privacy advocacy. The rules, discussed below, for the collection, processing, and disclosure of personal information in the employment context stem from the same agenda, and from the same policy community, that has produced more general instruments
for privacy protection. The most general international instrument for the protection of worker privacy emerged in 1996, when the International Labour Organisation (ILO) adopted a code of practice on the protection of workers' personal data (ILO, 1997). The ILO code is now regarded as the standard among privacy advocates for protection of workers' privacy rights. The code specifies that workers' data should be collected and used consistently with Fair Information Practices (FIPs). It states that:

- There should be coverage for both public and private sector employees.
- Employees should have notice of data collection processes.
- Data should be collected and used lawfully and fairly.
- Employers should collect the minimum necessary data required for employment.
- Data should only be collected from the employee, absent consent.
- Data should only be used for reasons directly relevant to employment, and only for the purposes for which the data were originally collected.
- Data should be held securely.
- Workers should have access to data.
- Data should not be transferred to third parties absent consent or to comply with a legal requirement.
- Workers cannot be forced to waive their privacy rights.
- Medical data is confidential.
- Sensitive data, such as that on sex life and political and religious beliefs, should not be collected.
- Certain collection techniques, such as polygraph testing, should be prohibited.

The code is not binding in effect. It was intended to be used more as a template in the development of legislation, regulations, collective agreements, and work rules.

Human resources information is increasingly, however, a commodity that is transferred across national boundaries, invoking some of the other international policy instruments. Both the Council of Europe and the European Union have addressed the question of the applicability of the Treaty 108 (Council of Europe, 1981), and the Data Protection Directive (EU, 1995), respectively, to the protection of privacy in the employment context. In September 2001, the Article 29 Working Party (established under the 1995 EU Data Protection Directive) issued an influential opinion on the processing of personal data in the employment context, serving to apply the words of the general Directive to the employment setting and to remind member states and employers of their obligations. The Working Party also noted that much employment-related data are highly sensitive in nature, e.g., union membership, sickness records, records relating to promotion, transfer, performance, etc. and are thus prohibited from processing, unless special exemptions apply.

At the national level, many European countries, such as Austria, Germany, Norway and Sweden have strong labour codes and privacy laws which directly or indirectly restrict workplace surveillance. But most statutory rules have been developed in the context of existing national data protection legislation. Since 2000, for example, the UK Information Commissioner (formerly Data Protection Registrar) has been issuing a series of guidance codes for employer/employee relationships, including recruiting and selection procedures, records management, and monitoring at work. The Employment Practices Data Protection Code states the obligations of employers under the Data Protection Act, taking into account the requirements of the Human Rights Act 1998. Among other things, the code prohibits the making of decisions solely on the basis of automated data, requires employers to notify employees in advance of surveillance policies, requires the explicit consent of employees before sensitive data such as medical information can be collected, and places limitations on drug, alcohol, genetic, aptitude and psychometric testing within the workplace. The Commissioner contends that following such practices will increase trust, encourage good housekeeping, protect organisations from legal action, and assist global businesses conform to international standards.

Most countries with established data protection regimes have, at one time or another, articulated special rules for the processing of personal data in the workplace. For example, the Hong Kong Privacy Commissioner has published a Code of Practice on Human Resources Management, and the Australian Commissioner has published guidelines on Internet use in the workplace. Moreover, most data protection authorities will, at one time or another, have issued guidance on the use of surveillance technologies generally. Thus, statements concerning the use

---


3 Available at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf.


of video-surveillance, the monitoring of e-mail, the use of genetic and
drug-testing or biometric identifiers may have a general applicability,
and make no distinction between the employment and the non-
employment context. The central point is that this guidance presumes a
general set of statutory rules for data protection, which all organisations
are obliged to follow regardless of the context or the type of personal
data being processed. The generality of some legal regimes is attribut-
able to the difficulty of establishing when we cease to become “work-
ers” and start becoming “citizens” or “consumers.”

In Canada, a rather different regulatory framework has been estab-
lished as a result of the peculiar constitutional arrangements for the
federal/provincial division of powers. The 2001 privacy legislation at
the federal level (the Personal Information Protection and Electronic
Documents Act) only regulates the commercial uses of personal infor-
mation; this results from the fact that the federal government could only
legislate in this area under its “trade and commerce” powers within the
Constitution. Employment law has always been regarded by the courts
as a provincial responsibility. The extent to which employment privacy
is protected in Canada is dependent, therefore, on the willingness of
Canada’s provinces to pass legislation, substantially similar to the
federal law. So far, only Quebec, British Columbia and Alberta have
passed a substantially similar provincial statutes protecting privacy in
the private sector.

In the United States, there is no general data protection legislation,
and therefore the rights of workers are dependent on a complex network
of statutory, common law, constitutional and voluntary provisions. For
governmental agencies, employee privacy rights are principally gov-
erned by the long tradition of 4th Amendment jurisprudence regulating
“unreasonable searches and seizures.” In the private sector, however,
there are few relevant statutory provisions. The Electronic Communica-
tions Privacy Act of 1986 (ECPA), which prohibits the intentional
interception of electronic communications, is the only federal statute
that offers workers explicit protections in communications privacy. But
the ECPA contains loopholes, permitting the monitoring of phone calls
and e-mail for business purposes, and allowing employers to intercept
communications where there is actual or implied employee consent.
There have been occasional attempts to increase workers’ privacy
through new legislation. Post September 11th, 2001, however, the

chances of stronger privacy protection legislation passing the Unites
States Congress have been slim. The passage of state legislation has also
had limited success.

With respect to self-regulatory measures (commitments, codes, stand-
ards, seals), these have been developed to protect the organisational-
consumer relationship in the marketplace, rather than the employer-
employee relationship in the workplace. In the consumer context, these
are more often genuine choices about the purchase of goods and ser-
vices, and the provision of personal information. The frenzied way in
which websites posted privacy policies, and subscribed to various seal
programs, as a way to encourage electronic commerce in the late 1990s,
is testament to the important role that consumer privacy now plays in
generating trust in the Internet as a medium through which goods and
services can be purchased. Whether or not there is a “privacy pay-off”
for those businesses that take consumer privacy seriously, as some have
argued (Cavoukian and Hamilton, 2003), is still complex and contro-
versial.

What is more clear is that public and private organisations have been
far more reluctant to grant employees privacy privileges and rights in the
absence of legal obligations and sanctions. A graphic illustration of the
difficulty of translating self-regulatory privacy principles from the
consumer to the employee context has occurred in Canada. The Cana-
dian Bankers Association (CBA) published a code of practice for con-
sumers in the early 1990s, revised in 1997; this code was subsequently
translated into company codes by the major Canadian banks. At the
same time, the CBA declared that it would also develop a code for
employees, one which never emerged before federal legislation was
enacted in 2001. Rhetoric, therefore, about the necessity to build “em-
ployee” trust in a business or a government organisation, is less likely
to convince employers voluntarily to grant rights to employees, if those
rights would impinge on efficiency, profitability and other organisa-
tional values.

The same can be said for the technological policy instruments. There
is no doubt that computer code can have considerable regulatory con-
sequences in the employer-employee context (Lessig, 1999). The simple
logging of cookies on a network server, for example, can be a tech-
nological decision with enormous consequences for the ability of
employers to track Internet usage at work. These “systemic instru-
ments”

---

6 See the advice on workplace privacy rights given by the Privacy Rights Clearing-
house. Available at http://www.privacyrights.org/fs/fs7-work.htm.
7 Available at http://www.epic.org/privacy/workplace.
9 See http://www.cba.ca.
(Bennett and Raab, 2003) or the “lex informatica” (Reidenberg, 1998) clearly need careful analysis in any organisational setting. And employees might voluntarily choose to use encryption of filtering instruments in order to shield their Internet activity from overly intrusive practices at work. Again, however, that choice is exercised within an employer-employee contractual relationship that may have very different consequences when exercised in the “workplace” as opposed to the home environment.

But what constitutes the “workplace”? In the concluding section, I argue that new “mobile” technologies are altering our traditional understandings of the distinction between the workplace and the non-workplace, with serious consequences for the protection of worker privacy and the application of these policy instruments.

5. The Mobile Workforce and the Mobile Worker

As Clarke (2003) notes, during the last few years “technologies have been deployed which made it increasingly feasible for large numbers of devices to be connected without being connected.” Mobile technologies harbour the potential for individual surveillance and there are no doubt powerful organisations that perceive advantages for themselves in being able to locate and monitor what specific individuals are doing at specific times at specific locations. However, there is a plethora of possible relationships between the device-user and remote organisations in a “mobile” environment. As a result, as Clarke (2003) notes, “there is ample scope for people to mean different things when they use the word ‘mobile’.” It is, therefore, critical to any analysis of the surveillance applications and privacy implications of wireless technologies that the sense in which the term ‘mobile’ is being used is made explicit.

Clarke has proposed four different meanings when we talk about mobile technologies. First, devices may be ‘mobile’ in the limited sense of being able to be “in a different location at any given time from that in which they were at one or more previous times.” Second, the term ‘mobile’ could mean that “a device could be anywhere, or, more carefully expressed, a device might be in any location from which transmission to another device is possible.” A third interpretation of ‘mobile’ is in “the more substantial sense of currently moving relative to the earth’s surface, but nonetheless capable of sustaining data transmission, e.g. as a passenger in a plane, a train, a taxi, or a car, or, less safely, as the driver of a car.” A final sense of the term “is to refer to devices that are designed to be easily and conveniently portable, and to rely on wireless transmission, possibly to the extent that they do not support cable-based connections.”

There are a wide variety of “mobile technologies” that are portable, that rely on wireless transmissions and that may be used to communicate from any location to another device. But none of these interrelated definitions implies per se that the location, less still the identity, of the user is necessarily known. This surveillance potential requires a further convergence of technology, standards-setting and organisational interests to produce what has come to be called, “location-based services” (LBS). Of course, that convergence has begun. The combination of cellular technologies, geographic positioning systems (GPS) and mapping products has produced a number of new applications designed to assist consumers, employers, parents and others “locate” individuals and objects in real time: to find the nearest retail outlet, to determine navigational coordinates, to track vulnerable people (e.g. children, teenagers, Alzheimer sufferers) to transmit location when 911 calls are made in times of emergency (Phillips, Regan and Bennett, 2003) and to monitor the behaviour of employees.

With regard to employee surveillance, for illustrative purposes we will focus on Clarke’s third interpretation, on those “mobile” technologies that are integrated into other “mobile” technologies, i.e. vehicles; analysts have coined the term “telematics” to describe the collective group of technologies that enables communication, information and entertainment services delivered to motor vehicles via wireless technology in real-time. The industry is complex, dynamic and impossible to categorise within any degree of precision. To date, the primary values have been confined to issues of safety through automatic accident notification and emergency assistance functions. A second set of concerns relate to security, with features such as stolen vehicle tracking, remote door locking and unlocking, and remote monitoring. A third set of applications relates to information services; most notable are the navigation systems that provide digital maps and dynamic route guidance. A fourth, and more futuristic set of applications lies in entertainment, although the market for onboard devices that allow web browsing, and movie watching, has not been proven (InCode Telecom, 2001:1). Vehicles have ceased to be simply a means of transport. They have become technologies which process information about the outside world for the benefit of the driver, and can relay information about the vehicle and the driver to other agencies – law enforcement, public safety, and/or employers.

Much of the initial analysis has focused again on consumer applications, with particular attention to the feasibility of “m-commerce.” There has generally been less attention paid to the employer-employee relationship. Yet, any employee with a cellular device is susceptible to
having his/her actions and movements monitored whether he/she is at home, on an airplane, and of course in a company's vehicle. A variety of products are now available for the surveillance of the mobile workforce. Here are two illustrations, together with associated marketing pitches from the relevant websites.

A company called 'Fleetboss' markets a range of GPS products of varying sophistication for commercial fleet surveillance. These systems allow a GPS unit in the vehicle to read the satellite signals and record location, speed and other information. These data are transmitted to the base station automatically, which then transmits to the user's computer. The Fleetboss customised software combines mapping and vehicle data and produces customised reports on employee behaviour. It is claimed that these products can lower fuel bills, increase fleet efficiency, raise fleet productivity, control moonlighting, eliminate theft, monitor speeding, reduce accidents, identify unauthorised vehicle use, verify billing time and even be of benefit to employees. I quote:

"The Boss fleet management system "builds character" for fleet drivers who tend to drift from the desired routes and procedures of management. With The Boss system, you'll be able to see who is driving, where and when they are going and for how long. As a result, the "meeting after the meeting" is cancelled, your fuel bills go down, the excuses go away and productivity rises because side trips and non-service stops become a non-issue. With the ability to always "ride" with your drivers using The Boss fleet management system, you can monitor who, what, where and when your vehicles and tools are supposed to be used. Do you think your vehicles and tools might last longer? How much money are you losing from moonlighting? How else would you know?"

A second company, AirIQ, has clients that now include most of the major rental car firms in North America, owners of commercial transport fleets and service companies that operate a "mobile workforce" facilitating the dispatch of routing of calls. The AirIQ system combines five separate technologies: intelligent software systems; global positioning systems; wireless communication networks; digitised mapping software; and the Internet. AirIQ has built an intelligent messaging switch that is capable of communicating with multiple types of wireless networks and devices. Thus, the company prides itself in developing a set of solutions that are device- and wireless-agnostic. Very simply, a location device (AirIQ Onboard), comprising a computer processor, GPS receiver and wireless transceiver, is installed into each vehicle and keeps track of where the vehicle is (generally within 100 yards or 91.4 metres), what direction it is going, what speed it is travelling, and records and reports additional vital information. The GPS transmits data to the onboard receiver, determines a latitude and longitude "fix," and calculates the differences in fixes to determine the speed and direction of the vehicle. By pre-selecting parameters, clients choose the circumstances under which a vehicle will report. This information is then transmitted by wireless networks to the AirIQ Network Operations Center. Clients can view and access their own fleet information on digitised maps at the password protected site (www.AirIQonline.com) by using a standard Internet browser.

The corporate publicity states that "AirIQ develops mobile asset and workforce management solutions to rental vehicle fleets, commercial transport fleets and service companies... AirIQ empowers companies to manage and protect mobile resources (people and vehicles)... For commercial transport fleets, customers can manage driver behaviour more effectively, locate vehicles, predict shipment arrival, inventory vehicles, provide automated maintenance reminders and retrieve lost or stolen vehicles. For service companies, the products are customised to allow fleet managers to increase efficiencies by ensuring that "the right person gets to the right place at the right time."

There are, of course, inherent limitations to onboard telematics technologies. Because these systems utilise wireless technology to communicate to and from the vehicle, the vehicle must be within cellular coverage to communicate; cellular covers approximately 95% of populated North America and some remote rural areas are still outside normal cellular coverage. Additionally, the GPS receiver must have a direct line of sight with the satellites to provide accurate location information; communication in cities with tall skyscrapers therefore poses difficulties. Nevertheless, these and other applications are currently being deployed by many companies that have an interest in managing their "mobile workforce": commercial fleet operators, taxi and limousine companies, courier and postal services, janitorial services, and so on. Potentially millions of "mobile" employees are now susceptible to more intensive and extensive surveillance, about which they may have little knowledge and control.

---

11 Interview AirIQ, August 16, 2002.
6. Conclusions and Implications

The literature on surveillance leaves us with the overwhelming message that the quantity and quality of surveillance have changed — both within the workplace and without. The volume of data collected and stored by both public and private organisations has facilitated a range of new practices that have developed incrementally and without much public attention or opposition. That system has developed through the uncontrolled decisions of thousands of decentralised public and private organisations, all making supposedly rational decisions that one more incremental invasion of privacy is a price worth paying for greater efficiency and/or profit. The examples cited above are supportive of David Lyon’s conclusions about surveillance and the “monitoring of everyday life” (Lyon, 2001). Surveillance is “Janus-faced,” according to Lyon. The same process both empowers and constrains. It gives us a variety of advantages (security, convenience, ease of communication and so on). It also enhances the power of the modern organisation to the detriment of individual privacy and to the disadvantage of marginalised groups. He demonstrates how surveillance systems have grown up to compensate for the weakening of face-to-face social relationships in which mechanisms for social integration are increasingly removed and abstract. Surveillance, then, is the necessary glue that builds trust in a “society of strangers.” The “Invisible Frameworks” of integrated information and communications networks contribute to the “orchestration” of this society of strangers.

It is possible to argue that a further paradigm shift is underway with the development of mobile technologies, and associated location-based services. As these practices assume a greater importance, they become important sources of valuable information in themselves. Surveillance in turn has accommodated these changes by also becoming more mobile (Bennett and Regan, 2004). In the employment context, Lyon argues that the worker is now expected to be geographically mobile, and willing to work variable hours. “Work has become more individualised, and so have surveillance methods” (2001:40). The workplace is defined less in spatial terms (as a place where all workers have one roof over their heads), but in terms of surveillance. You are in the workplace, where and when your activities can be monitored. And due to the availability and relative cheapness of new surveillance methods, those occasions and places are increasingly difficult to define.

Regardless of the roots and extent of modern surveillance practices, from a political standpoint, this increase in surveillance capacity can have a dysfunctional impact on the relationship between individuals and public and private institutions. Many of these new surveillance tools are predicated on an assumption that workers cannot be trusted. Whether one is discussing video cameras, e-mail monitoring or keystroke monitoring, drug-testing, computer matching to detect fraud, or indeed, the use of Fleetboss or AirIQ, these systems serve to increase the level of distrust between individuals and the public and private organisations with which they relate. There is a circular process at work, whereby the increase in surveillance capacity reduces the level of societal trust and alienation, which in turn produces further deviant behaviour, deemed worthy of further surveillance.

But how can the theory and policies of privacy protection address these larger questions? There is a conventional wisdom amongst theorists of surveillance that they cannot. The discourse and policies of “privacy” fall far short of addressing the challenges of contemporary surveillance (Lyon, 2001; Rule et al., 1980; Gandy, 1992; Marx, 1999). There are two central elements to this critique. First, privacy policy echoes rather than disturbs the classification and sorting of individuals as “disembodied abstractions.” It reinforces individuation, rather than community, sociability, trust and so on. It therefore never challenges the larger questions of categorical discrimination. Moreover, privacy protection policies are “cumbersome and unresponsive” to the rapidity and diversity of technological change. At root, privacy claims tend not to see surveillance as a social question, but as a problem that can be addressed by properly implementing the fair information principles doctrine in relation to the personal data on discrete individuals.

There are, of course, larger social, economic and political issues at stake than privacy, when one considers such a complex phenomenon as the monitoring of a mobile workforce. Nonetheless, I believe the critiques of privacy protection are sometimes overstated. The modern claim to privacy does rest on a liberal notion of a boundary between the individual and other individuals, and between the individual and the state. It rests on notions of a distinction between the public and the private. It rests on the pervasive assumption that there is a civil society comprised of relatively autonomous individuals who need a modicum of privacy to make rational self-regarding choices about their lives (Bennett and Raab, 2003: ch. 1). But it also rests on the notion that social values like community, trust, sociability etc. are inextricably connected to the ways in which organisations collect, use, process and disclose personal information. In this sense, as Priscilla Regan has argued, society is better off when we all have greater levels of privacy (Regan, 1995:221). It is overly simple to contend that privacy is about sheltering the “sacrosanct self” behind “legal limits on the promiscuous processing of personal data” (Lyon, 2001:150).
On the question of the effectiveness of much privacy protection policy, this is, of course, dependent on context. Some privacy protection laws are indeed poorly enforced and implemented, replete with vague exemptions, and completely misunderstood by those citizens they are designed to protect. On the other hand, some are not. In some jurisdictions, stronger, unambiguous and comprehensive privacy protection laws that make no distinction between organisational sectors or the means of data processing, are overseen by activist data protection agencies that understand the range of prescriptive measures, besides legal sanction, that they can bring to bear. In some jurisdictions, a more “privacy-aware” citizenry, represented by activist privacy advocates, is far more ready to expose and critique overly intrusive surveillance practices. Although, the success of privacy protection policy is inherently difficult to measure and compare (Bennett and Raab, 2003: ch. 9), it is variable. And there are enough examples of the successful resistance to surveillance, to have a more sanguine view of efficacy of privacy protection policy, and the theory upon which it is based.

We should not downplay the importance of other modes of resistance, nor exaggerate the successes of privacy law and those who implement it. It can be argued, however, that the theory and practice of privacy protection has broadened in response to new surveillance changes in ways that are often downplayed in the sociological literature. On a conceptual level, privacy now embraces values that go beyond the interests of the possessive individual; the contemporary discourse surrounding the promotion of “trust” in new information systems is an example. Moreover, as we have seen above, privacy protection policy has broadened to encompass a plurality of policy instruments besides law, including privacy-enhancing technologies, self-regulatory tools and many mechanisms for individual empowerment.

To translate this conclusion to the practical issues raised by the monitoring of an increasingly mobile workforce, we can conclude that employee rights are far more likely to be protected where comprehensive data protection statutes, overseen by activist data protection commissioners exist. In such countries, basic privacy principles about notice, transparency, consent, relevant usage, non-disclosure, security and so on can go a long way to ensuring that only relevant information is collected on employee behaviour, and that only the appropriate people have access to that data for the right reasons. The effective implementation of privacy protection policy within an amorphous and indeterminate “workplace” will not address wider issues of workplace discrimination. Nor will it effectively interrogate and alter the changing nature of “work” in late capitalist societies. But to the extent that privacy prote-
PART III

ETHICAL ANALYSIS