



Surveillance in the Workplace – an overview of issues of privacy, monitoring, and ethics

**Briefing Paper for GMB
September 2005**

Surveillance in the Workplace – an overview of issues of privacy, monitoring, and ethics

Briefing Paper for GMB,
September 2005

Professor Michael Blakemore
IDRA Ltd, blakemoremjb@hotmail.com

THEMES

- Surveillance in the Workplace – an overview of issues of privacy, monitoring, and ethics 0
- 1. Surveillance is nothing new, but the nature of surveillance is changing 2
- 2. Surveillance pre-Internet did not require consent, but it was selective, costly, and not pervasive 2
- 3. Over-reliance on technological surveillance can be problematical 2
- 4. Function-creep has always been a characteristic of surveillant technologies 3
- 5. Surveillance in many circumstances is a positive process, but not without problems 3
- 6. Surveillance of employees focused in the past mainly on physical removal of property 4
- 7. Those using surveillance technologies often rely in simple linear arguments of good and bad 5
- 8. Propagate a powerful myth and embed it into the ‘need’ for pervasive surveillance 6
- 9. Surveillance in the retail sector..... 8
 - 9.1. Routine surveillance in a retail situation is also promoted as a form of employee protection – whether it realistically protects employees, or at least helps in the detection of criminals 9
 - 9.2. How do I know whether I am being surveilled? 9
 - 9.3. Am I justified in being worried by surveillance? 10
 - 9.4. Areas of surveillance..... 11
- 10. Pervasive computing does not necessarily lead to positive benefits 13
- 11. Call Centres.....14
- 12. Legislative reactions 14
- 13. Health and Safety, Risk Assessment..... 15
- 14. Consumer choice can be influenced by ‘social sorting’ 16
- 15. The problem is not just the technologies, but may be more one of consent 16
- 16. The demise of the implied social contract?..... 17
- 17. Sources of Imagery 19
- 18. Sources..... 20

1. Surveillance is nothing new, but the nature of surveillance is changing

Checking up on employees is nothing new. The history of the labour market has been full of people whose primary responsibility is to check that people are working correctly – overseers, foremen, for example – but the rapidly evolving and interconnected digital technologies present significant challenges.

Back in 1998, Michael Ford's publication for the Institute of Employment Rights highlighted challenges, arguing that digital surveillance results in monitoring of workers that is "more widespread, more continuous, more intense and more secretive" (Ford 1998). The computing environment can now collect information that is more 'context aware' (knowing not what we do, but when and where (Bristow *et al.* 2004)), and this creates new tensions in the balance between "the individual's need for privacy and corporate, government, and society's need for information" (York and Pendharkar 2004). Mobile and ambient technologies will introduce new dilemmas, for example "new business models will increase profits, possibly at the expense of safety margins; the balance of political and economic power could shift; economic developments will accelerate and initiate long-term changes in our social values and motives" (Bohn *et al.* 2005, p.21), and some argue that the embedding of technologies into our persona (worn computers, RFID chips in clothing for example), take us into a 'posthuman' environment where "we are physically grounded but conceptually extended" by the information systems that tell us what to do (Pepperell 2005).

That said, consent and the embedding of technology does not in itself render us posthuman, and the Baja Beach Club in the UK now offers the possibility for VIPs to be microchipped (90 have had a chip embedded in their arm), so allowing them to "run a tab on a central computer, which they can check up on with a wave of the arm" (Purcell 2005).

2. Surveillance pre-Internet did not require consent, but it was selective, costly, and not pervasive

The routine checking of employees also is nothing particularly new. Random bag searches by security staff at factory gates is one example, where any worker could be stopped and searched. That act did not require the 'implied consent' of a worker, although it was a long way from the routine searching of every worker every time they walked out of the factory gates. The concern here was to stop physical property leaving the workplace in an unauthorised fashion. Before email and the Internet even intellectual property and confidential information would need to leave on some physical storage device, whether it was paper, disks, or film.

Yet, to search everyone would have required significant numbers of security staff, and the cost of mass monitoring would generally have been prohibitive. Even if everyone was checked at the gates, and even if management were looking at working practices, the surveillant practices pre-Internet and digital technologies was by no means ubiquitous. Surveillance was practiced at certain strategic places in the workplace, and more extensive surveillance was practiced where there was reasonable cause to suspect someone of mal-practice. The costs of surveillance were balanced out against the gains.

3. Over-reliance on technological surveillance can be problematical

In the early 1990s researchers such as Roger Clarke had studied the increasing tendency to join up information from a variety of sources into that was termed 'Dataveillance'. This process involves the routine checking of data against certain norms. It is as if the Police Service decided to move away from 'intelligence-led' policing, to relying on the complete surveillance and screening of all citizens against certain defined norms.

Access to comprehensive information that is joined up is vital for the detection of terrorism (Kablenet 2005b), or overcoming the significant problems that occurred with the Soham murders where information was not shared between police forces (BBC 2003a). The Bichard enquiry that followed in 2004 proposed that police establish an integrated national intelligence system, yet in 2005 the system was still to be scoped, let alone used (Kablenet 2005a).

Even if all the information is available, however, there is no guarantee that it will lead to the effective surveillance of miscreants. This was vividly highlighted in the US 9-11 report (Congress 2004) which demonstrated that the extensive information gathering activities of US security agencies did not work. The volume of information meant that the IT systems found it difficult to process the data quickly (a 'wood for the trees' syndrome), that the agencies did not work together effectively (the 'failure of human agency' syndrome) (BBC 2005b), and that the agencies in general relied too much on the IT working effectively.

4. Function-creep has always been a characteristic of surveillant technologies

Mass dataveillance is one of the underpinning processes for the UK Government plans to move to road-charging by use (Zetter 2005a). Every car would be fitted with a GPS tracking system, and all 'transactions' would be logged so that charging can be calculated. It would be almost unimaginable that government would not be tempted to 'mine' this information to check other events in the same way that Dataveillance has been used by governments and businesses as a means of increasing efficiency and effectiveness (terms strongly linked to the rhetoric of productivity and profitability) by businesses and government.

However, Roger Clarke noted that the underlying data in the separate sources were often not robust, and that the process of Dataveillance was "a highly error-prone and privacy-invasive activity" (R Clarke 1994, p.80-81). In a comprehensive analysis of the use of technology by governments and business Robins and Webster cautioned that the routine electronic surveillance means that the relationship between surveiller and surveilled, between worker and management, between citizen and government, inevitably changes: "the individual becomes the object of surveillance, no longer the subject of communication" (Robins and Webster 1999, p.121). Without communication (and that involved dialogue, dissent, compromise etc.) there is a vacuum replaced by contest and opposition. The electronic surveillance practice involves the risk that we are, at all times, being seen without being able to see who is looking at us, and this complex relationship is even the subject of art (BAL TIC 2003).

5. Surveillance in many circumstances is a positive process, but not without problems

Surveillance has been beneficial in providing evidence of criminal activity, in joining up disparate information within the processes of globalisation, in developing a retail environment

more focused on individual customer needs, in protecting vulnerable people, and in reducing human error.

- We look after each other, for example by checking to see whether relatives are ill.
- Audit trails, such as the IT evidence trail that helped convict Harold Shipman.
- The use of RFID chips in food packaging, so that if there are problems there is a rapid link to information providing food traceability in a global food chain.
- Linking material in a global supply chain – rapid re-ordering (Torex 2005), and linking sales data to customer data (Torex 2005)
- The tracking of babies in hospitals to detect kidnapping, the tracking of old people in homes (Baard 2004; Biever 2004).
- Making schoolchildren wear RFID badges so that they can be tracked around school (Zetter 2005b). This proves, of course, only that the piece of clothing containing the RFID chip was at a location, and not the human being who was assumed to be wearing it. Add to this RFID chips in uniforms and the technology has considerable potential for surveillance, and just as many opportunities for counter-action.
- Implant RFID and other identity microchips into the human body. This has been proposed to minimise medical errors: “by providing an individual's identity and medical history (Anon 2005c). This does, however, fundamentally assume that the underlying information system is robust and free from errors.
- There is a risk of behaviour change where the ‘system’ is assumed to be infallible, and human cross-checks diminish. A more macabre behaviour change could occur: Mexican government officials were microchipped under the skin of an arm, so that they could be ‘traced’ if abducted (Reuters 2004a). Amputating an arm is not beyond the capability of abductors.
- Citizen surveillers are now increasing, particularly where individuals take photos of events using the cameras in their mobile phones. Such images are useful both to security agencies and to security authorities, but there are associated issues, such as whether citizens should be paid, whether this encourages them to become stalkers rather than observers, and “the real issue here is an ethical issue if a bomb goes off and someone stops and takes a picture instead of helping” (BBC 2005a).

6. Surveillance of employees focused in the past mainly on physical removal of property

The process of surveillance of workers could be viewed as a contest over the unauthorised flow of employer property across the borders of the company. There was little that could be done (as it is the case at present) to stop an employee memorising strategic information and selling it to a competitor. A crucial reason for Internet monitoring in the past five years has been the illegal use of Internet at work to access pornography, and early interventions clearly discriminated between illegal use, unethical use, and unacceptable levels of use (Whittle 2000). The problems at present are that the borders of a company are far removed from the physical border of a factory gate or organisation front-door, and the opportunities for property to flow beyond company borders are significant. Furthermore, the ease of communication on the Internet means that one disaffected employee can disseminate information that is prejudicial to a company. The problems seen in the Internet environment involve:

- defamation of an employer using workplace blogs (Zeller 2005);
- Sabotage and data theft (BBC 2005c)
- the development of hacking technologies that can disrupt the technologies of surveillance, such as Blocker tags (Dearne 2004; Zetter 2004).

There then is a set of counter play activities that, in addition to unexpected behaviour changes noted earlier, are emerging as a response to surveillance in the workplace:

- Those carrying out surveillance can themselves be counter-surveilled. Steve Mann is one of the privacy specialists who uses the term “equivallance through sousveillance” (Zetter 2005c). Sousveillance, meaning watching from below, involves the use of commonly available devices such as mobile phones (that can record speech, and can take pictures and short videos), or the use of blogging Web sites (where anyone can post views and invite comments, or even post information about management activities – both workplace and private) (Zeller 2005).
- More extreme is the development of corporate hate sites (Wolrich 2005)
- Those who are required to be surveilled can demand intrusive surveillance from those who are carrying out surveillance. Steve Mann, for example “has designed a wallet that requires someone to show ID in order to see his ID. The device consists of a wallet with a card reader on it” (Zetter 2005c).
- Here we move to “the potential for more pedestrian forms of surveillance,” as stated by Bruce Schneier, with lots of little brothers watching the big brothers (Economist 2004). This process is strongly linked to the public surveillance of government through the Internet (Meijer 2005), where the increasing surveillance activities of government result in more intrusive media surveillance of the activities of politicians through processes such as ‘hactivism’ that is “grass-roots resistance enabled by technology -- is a viable way to battle repression” (Delio 2004).
- Overloading executives who are seen as central to information technologies, or who impose surveillance and surveillance technologies with communication overloads. Bill Gates is the most spammed person in the world, and Microsoft invest considerable efforts to overcome this (Reuters 2004b). George Bush was the subject of citizen surveillance during the 2003 election (BBC 2003b), when individuals could send reports about his movements to enable protestors to gather quickly.
- Contesting the accuracy of the technologies. All technologies are fallible, and “Location-aware devices will never provide perfect information about employee location. Most systems such as GPS have inherent accuracy limitations, may suffer from signal loss interrupting operation, may be subject to incorrect configuration by operators, and may of course simply malfunction” (Kaupins and Minch 2005).

The overall message here is that surveillance does not directly lead to productivity benefits that are stable.

7. Those using surveillance technologies often rely in simple linear arguments of good and bad

Gary Marx, one of the leading researchers on privacy and surveillance, summarised the situation in what he termed ‘info-age techno-fallacies’, and some of these are elaborated below (Marx 2003). These fallacies are not assertions, but are underpinned by extensive research undertaken by privacy researchers.

- (8) “Greater expenditures and more powerful technology will continually yield benefits in a linear fashion”. (9) “Some information is good, so more must be better”. (10) “Applying a war mentality to domestic issues”. These fallacies were central to the post 9-11 US Government proposals for the TIPS (Terrorism Information Protection System) and Citizencorps initiative. Citizencorps would have involved every citizen spying on all other

citizens to “use their common sense and knowledge of their work environment to identify suspicious or unusual activity”. They failed, both through the huge task involved in setting up the information gathering technologies, but also because the fundamental nature of citizen-government relations would change. Yet, the US Government still prevails with huge IT surveillance projects for tracking aliens residing in the USA, and for the screening of all airline passengers entering, or even flying over, the USA. In all honesty they have little option other than to gather mass information – the political damage by inaction would be huge – but businesses do have a reasoned choice to make about mass surveillance of employees.

- (18) “The fallacy of implied consent and free choice”. The most prevailing argument by supporters of mass-surveillance is that it is unpleasant medicine, but it is ‘good for you’. This fallacy is more difficult to unpack, since we surround ourselves with the concepts of privacy, and regard privacy as a democratic right. However, going back to the original Greek terms presents some problems. David Blunkett, when Home Secretary, based his views in the Greek ‘polis’, stating “we only become fully free when we share, as active citizens, in the government of the affairs of the community” (Blunkett 2002). For example, the Greek term for someone who wants to retain privacy is *Idiotis* (idiot-is). The term for someone who is a public person (who contributes to community and society) is *Demosios* (demos-ios). The Greek *demos*/privacy definitions would seem to argue that so long as there is a contest, rather than a partnership between employer and employee, the inevitable outcome is a contested relationship where surveillance is countered by counter-actions (see later). Here, then, is a critical challenge for workers – to be ‘*demos*’ may require you to tell employers about other employees who are stealing.
- (20) “If you have done nothing wrong, you have nothing to hide”. Easy to state, but only if you are confident that total surveillance will not deliver negative outcomes. Research indicates that total surveillance in the workplace leads to lost productivity. “The Future Role of Trust in Work,” was published the London School of Economics and Political Science (LSE) in December 2004. “It reveals that managers are using technologies such as e-mail, mobile phones, and SMS (Short Messaging Service) to keep tabs on employees when in actuality they are reducing workers' productivity and the amount of time that they spend serving customers.” (Pruitt 2004). The key argument is that over-surveillance leads to behaviour changes that are self-defeating in terms of productivity. If management is watching email and other activity, then people will send more routine email to show that they are ‘working hard’, and employees react to surveillance, or to perceived surveillance, to the detriment of effective working, “therefore ultimately damaging UK productivity” (Pruitt 2004).

8. Propagate a powerful myth and embed it into the ‘need’ for pervasive surveillance

The simpler the message the better, especially if it is a myth that is somehow grounded in research. As Vincent Mosco says in his influential critiques of the global information society, “Almost every wave of new technology, including information and communication media, has brought with it declarations of the end” (Mosco 2002, p.3), and “myths are not true or false, but are dead or alive” (Mosco 2004, p.29).

Thus, we see global generalisations that make easy to remember and repeatable myths:

- Check-out operators are regarded as the weakest link: “80% of retail fraud is at point of sale - till fraud” (RetailFraud 2005)

- Employers' organisations argue that the majority of employees are suspect: "Research shows that 25% of employees are totally honest, 25% are totally dishonest, and the remaining 50% are swayed by opportunity" (RetailFraud 2005). The source of the 'Research' was not cited.
- "Research shows that 25% of employees are totally honest, 25% are totally dishonest, and the remaining 50% are swayed by opportunity. Many staff do not regard consuming goods or taking goods for personal use as theft, but as perks of the job" (Anon 2005e). The source of the 'Research' was not cited.
- "Studies have shown that approximately 25% of employees are not honest and will attempt to steal from an employer no matter what controls are in place, 25% of employees are honest and will not steal from an employer, and 50% of employees are somewhat honest and will steal only if it is so easy to steal that they would feel foolish if they did not steal" (Williams and Williams 2002). The source of the 'Studies' was not cited.
- "Recently, a leader in loss prevention security for business and industry stated that 25% of employees were honest, 25% were thieves and the other 50% were only as honest as management required them to be" (AndyFisher 2005). The 'Leader' as not named.
- "Research shows that 25% of employees are totally honest, 25% are totally dishonest, and the remaining 50% are swayed by opportunity" (Firstepos 2005). The source of the 'Research' was not cited.
- "Britain a nation of malingerers", widely cited in the press and by politicians. Yet, when unpacked and critiqued by the TUC the generalisation becomes difficult to sustain. In particular the conclusion "Bad jobs and in equality have a lot more to do with sickness absence than swinging the lead" resonates with the extensive Swiss investigation cited below (TUC 2005).
- "Studies have found that employees are abusing their computer privileges for personal emails, shopping, stock trading, and much more while on the clock at their workplace. The result of this abuse is low employee productivity which creates profit loss for the parent company in the long run. The estimated abuse of computer privileges is 75 minutes every day" (CM 2005). The source of the 'Studies' was not cited.
- "Some retailers estimate that on average, 10% to 25% of their inventory is "lost" in the supply chain at any given time" (TEXAS 2005). The retailers were not named.
- "There is no such thing as too much security", quoted in the context of monitoring call centre employees in Delhi (Baden 2005). The person stating this was the Chief Security Officer, and the growth of CSOs as an employment sector in itself creates a community of people whose interests are best served by promoting the fear of security breaches.

Yet, those promoting the myths of ubiquitous evil in employees (and 25%, 25% and 50% seems both so statistically rounded, and so easy to remember), seem not to critique the myths against more extensive research.

- The Federation of Small Businesses reports that of the 58% of small businesses that have suffered a crime during a year, the crimes comprised "employee theft (8%) and employee fraud (6%)" (Robson and Teague 2005, p.7).
- The 'European Retail Theft Barometer', researched by the Centre for Retail Research in Nottingham, notes "Retailers perceived customer thieves to be responsible for 48% of shrinkage, employees for 29% (up 1% compared to last year) and suppliers for 7%. Internal error, process failures and pricing mistakes were thought to cause 16% of shrinkage, leaving 84% of shrinkage as crime-related" (Bamfield 2004). The level of 29% is "based on results from 423 major European retailers from 24 countries", and therefore measures perceptions rather than actual crimes. A further study by the Centre interviewed security managers about their perceptions of retail crime, reporting that "Staff-related

crime was responsible for 50.8% of total store theft” (CRR 2004). While the methodology of measuring perceptions is controversial, it could be acknowledged that the study findings of a decline in UK retail shrinkage rates may be influenced by more surveillance and security, and this study in no way decries security that is commensurate with the real extent of retail crime.

- The Home Office ‘Crime and Victimization Survey 2002’ reports that 10% of businesses suffered theft by employees, and 4% fraud by employees (Shury *et al.* 2005).
- Jerald Greenberg researched the nature of employee theft, and concluded that intrusive surveillance is not necessarily the answer: “Although people are unlikely to steal from individual co-workers, they are indeed likely to steal from their companies. Among employees who have opportunities to do so, a corporate ethics program has been shown to be an effective deterrent for those individuals who have reached the most common level of moral development” (Greenberg 2002).

There exists, therefore, a statistical contest over whose figures are more believable, rather than those whose figures are more statistically reliable. The propagation of surveys that lead to broad generalisations will, inevitably, fuel the need for more surveillance, such as that a survey by the law company Peninsula, who “polled 1,542 employees across a wide spectrum of industries” (the methodology was not cited by Millar) and found that on average men spend 4 hours a day checking the Internet, and women spend two hours a day (Millar 2005). This would seem to imply that 50% of male productivity is lost in many organisations!

9. Surveillance in the retail sector

CCTVs are by far the most familiar methods of electronic surveillance. Being watched and checked by supervisors is the human version of that process. However, such methods are both labour intensive, and are seldom pervasive. What this briefing covers is what we could term ‘pervasive’ surveillance, where everything, or almost everything, that an employee does can be monitored, analysed, and checked against such things as norms of performance. This briefing looks at critical areas of check-outs, of the use of computers, the retail supply chain, and links back also to previous work on distribution depots.

Electronic surveillance can be ‘ubiquitous’ or ‘pervasive’, in that it can constantly store information about what you do. It has no loss of memory – the ‘evidence’ is often stored, and can be, and it can be used for subsequent analysis and investigation. As Martin Dodge discusses, we may forget what we did, but the information databases do not (Dodge and Kitchin 2005).

Most monitoring requires that the employee be identified to the system of surveillance. For a check-out operator that will be their employee identity that they enter when they sign-on to the till. For the user of a computer terminal it will be their identifier and password, linked to their employee identity. The intensive monitoring tends to be undertaken when the employee is on-task, for example at a computer or a point-of-sales till. More pervasive methods of monitoring involve the employee ‘wearing’ a computer. Such computers communicate via wireless networks to a central control, and they can be fitted with hardware and software that use the GPS satellite constellation to know the location of the employee. Routine screening against norms that are focused on productivity, rather than customer service, means an ever moving target for employees

9.1. Routine surveillance in a retail situation is also promoted as a form of employee protection – whether it realistically protects employees, or at least helps in the detection of criminals

- “essential surveillance needs to prevent shrinkage, improve staff security and store management ... ensure that every transaction is monitored and no irregularities occur” (Axis 2005)
- “By capturing details of cash register transactions and associating them with the relevant CCTV footage, the RS range lets you track activity at every one of your cash registers virtually eliminating sweet-hearting, no-sales, under-rings, and other forms of register theft that are notoriously difficult to catch” (DMicros 2005)
- “IP {Internet Protocol} Video Surveillance can deter employee misconduct such as special benefits for friends; it also enables you to offer reliable protection to your staff, especially during the night shifts”. (Xpert 2005)
- Implement remote monitoring software (Acespy 2005; ELTIMA 2005) that logs almost every type of action and transaction that can be undertaken by an employee, including keystrokes, email, chats, websites, documents, capture screenshots of their terminals, programs that have been used, and also have the ability to “Lock and unlock the remote desktop” or freeze the action of the mouse remotely (CM 2005).
- Use covert GPS vehicle tracking technology for “Monitoring unauthorized use of company owned or commercial vehicles; Monitoring suspected criminal activity; Providing admissible prosecuting or mitigating evidence for use in court; Assisting in preventing Fraudulent activity” (Symmetry3 2005).
- The Tesco paperless picking system not only produces efficiency gains, but “is also very easy to use from a management perspective as the trackability and traceability of what each person does is fantastic” (INTERMEC 2005).
- Maintain workplace standards, even in areas of personal hygiene: “One US company has installed what's known as a hygiene guard¹, which uses sensors on soap dispensers to make sure workers adhere to proper hygiene. If employees fail to wash their hands, a black mark goes directly into their file on the main computer” (BBC 2004b).

There has been considerable anxiety about this technology, particularly in the context of new forms of micro-surveillance. On one level it is not substantially different from the introduction of features such as bar-coding, and while some news feeds have discussed the decision by Wall-Mart to mandate that suppliers use RFID, it is not that different to the decision years ago by WH Smith that all suppliers use barcodes (Lacy 2005). The over-riding focus in the retail sector started out as inventory control and the drive to increase efficiency through automation of processes, and increasing staff productivity (METRO 2004). This links to the home with the ‘smart fridge’ (Batista 2003), where if you decide to cook a recipe in the evening, the fridge contents can be checked, and then an order sent automatically to the supermarket for the ingredients that are still needed to be dispatched for delivery when you arrive home. This all plays on the just-in-time society, and this is nowhere more evident than in the relationships between retail supermarkets, employees, and customers.

9.2. How do I know whether I am being surveilled?

¹ <http://captology.stanford.edu/Examples/hygieneguard.html>

Unless your employer has a code of conduct that tells you what is, and what is not, being done you really do not know. That, according to the research literature, is one of the reasons that employees feel anxiety and stress.

Furthermore, many of the technologies that can be used for employee surveillance are implemented for other reasons, or indeed can be implemented for reasons of employee protection. CCTV cameras can be placed both to deter and record crimes against staff, and also to deter and record theft by staff. The computer software that links the check-out tills will use the bar-code that identifies a customer having just purchased a product, with the storeroom at the back of the store, so that shelf replenishment can be planned efficiently in what is called a 'cradle to grave' tracking process for all products (NRFID 2004). The storeroom is linked to the computers in the distribution warehouses, so that the store can be re-stocked, and the warehouses are linked to the suppliers, who will then receive orders for deliveries to the warehouses (INTERMEC 2005; Torex 2005). The integrated supply chain, and just-in-time delivery methods, are all used to ensure that the right products are in the right places, that errors are minimised, that profitability is increased, and that the customer experience improves (RETEK 2005). After all, we are all customers and many of we customers are employees.

Technologies also are needed to surveil the behaviour of customers. Theft from stores is a significant concern, as is fraud, and RFID technologies are promoted as providing "brand-protection solutions to protect against counterfeiting and return fraud with label materials with overt and covert security features including tamper-evident adhesives, magnetic threads and invisible taggants for authentication, secure laminates and more" (ZEBRA 2005).

GPS-enabled computers can protect staff who are on delivery runs, especially if they are carrying very high-value goods. There is some comfort knowing that your company can track your journey, and that the police can be alerted instantly if a threat occurs. If a medical emergency occurs your location is then used by the emergency services to alert the vehicles and staff that are nearest to you. The same tracking facilities can be used, however, in routine delivery vehicles, and mileage, driving time, stops, deviations from approved or intended route, can be logged. In effect, the technologies can be used to monitor deviations from the expected behaviour patterns of employees. The temptation to use business-oriented technologies for staff surveillance is often called 'function creep'.

9.3. Am I justified in being worried by surveillance?

The fact that the technologies can be used in pervasive staff monitoring, and the fact that the manufacturers of the technologies promote surveillance facilities, that creates a state of potential confrontation in the workplace. Unless the extent of surveillance is stated by employers, then employees have little information on which to estimate the proportionality of surveillance, and are unable to determine the ethicality of the employer. However, the contest is not that simple, since in a surveillance environment where the prevailing assumption is 'you only are afraid of being surveilled if you have done something wrong', employers may fear a counter 'function creep' in employee behaviour. If employees know that the employer is not monitoring a particular area of the workplace, will the employer fear that they will exploit it?

The research literature on surveillance links the constantly monitored workplace to constantly monitored public spaces (shopping malls, airports, train stations, buses etc.), and articulates this form of surveillance as a 'panopticon':

The panoptic society traces back to the well-known Panopticon of Jeremy Bentham who modelled a prison in which the prisoners could be observed from a central point, but were themselves not able to see their observers. Foucault pointed out that the specific meaning of this model lies in the creation of a permanent awareness of being observed that ensures power to take effect automatically. (Peissln 2003, p.22)

There is a further trend evident in the use of surveillant technologies, and this was covered previously by GMB in the material on regional distribution centres. Some of the retail companies report 'reductions in staff training' times. In this context we could see the employee as being regarded as an inefficient intermediary step between linking products and customers. Customer self-service check-outs are one mechanism to reduce employee levels. If employees do not have to learn the lay-out of a warehouse, but are told where to go by instructions sent to computers that they 'wear', then their training overheads are reduced, and the skill-set needed is reduced. A logical end-point will be the full automation of warehouses and distribution centres, with robotic² machines doing the work. This process is clearly similar to the automation of car manufacturing. Such fears are being confronted by some employers, with reports of employee/employer engagement over the technologies at a US distribution company (Lacefield 2004), but the general levels of unease over the potential for surveillance indicates that there is not a systematic process of engagement.

As an intermediary step along the way to automation, the use of headsets, voice-recognition, arm-mounted wearable computers in effect make the humans become an extension of the information systems that drive the supply-chain. The human is no longer given a list of products to find, and then be expected to use initiative and knowledge to find the products. Instead, the information system plans the best route for the human to take, and in effect pre-optimises the human being's itinerary. Since the specific location of all products are known the system can be programmed to estimate the amount of time the human takes to obtain the products, and can build the item-by-item information into an asset-tracking process (the human is another machine asset in this type of business) that provides continuous and comprehensive performance information for managers (in much the same way that check-out operators can be profiled by the minute in supermarkets).

9.4. Areas of surveillance

The companies selling retail systems are quite clear in specifying the types of employee surveillance:

Check-out staff

CCTV systems are the most familiar, but they are fallible both in detecting customer and employee theft and some researchers recommend that "retailers would be better spending their security budget on training workers at the tills to spot suspicious behaviour than on expensive surveillance equipment" (Johnston 2003). However, passive CCTV is being replaced by IP (Internet Protocol) CCTV systems that can be controlled and monitored remotely via the Internet: "Low cost cameras can be integrated with network access around points of sale, allowing video to be taken of transactions to reduce the potential of fraud or theft. ... Monitoring through IP Video Surveillance can also help to improve store

² See, for example <http://www.packexpo.com/ve/36618/main.html> ,
<http://www.aftermarketbusiness.com/aftermarketbusiness/article/articleDetail.jsp?id=169731> ,
<http://www.roboticonline.com/public/articles/archivedetails.cfm?id=880>

management as consumer activity can be observed, recorded and measured leading to better staff planning and store layout” (Axis 2005; Xpert 2005).

Checkout tills provide more comprehensive information about staff activities, with a particular focus on preventing certain categories of ‘till fraud’. These include ‘Sweethearting’, where a product is not scanned at all, or is registered at a lower price, ‘Substitute Scanning’, where two items are passed by a scanner, the higher value one being hidden behind the one being registered, ‘Returns and Refunds’ and ‘No-sales or voids’ (Firstepos 2005; RetailFraud 2005). Hence, RFID chips can be used to prevent shrinkage reduction, and “item level tagging may well replace current EAS tags³. Integration with EPOS systems will inhibit internal shrinkage by the removal of ‘sweet hearting’” (Microlise 2005).

The tills play a critical role in collecting customer information (loyalty schemes), inventory control etc. However, the information they provide also can be used to detect fraud, and “cash-drawer position reports, as well as remote supervisor overrides, system alerts and cashier monitoring” (NCR 2005). Once an employee is logged on to the till, their performance can be logged by time until they log off: the rate at which they scan items, their non-active time, and this can be used to compare their overall performance against that of others, or against norms. The information overall can be used to identify who sells best, or who sells worst. Poorly performing staff may not have their contracts renewed (hence the preference for employing short-term, part-time staff with limited employment protection).

Staff using computers

The misuse of computers by employees has become a major area of concern for employers with the growth of access to email and the Internet. Unethical or illegal use of computer facilities can result in major liability issues for employers.

The range of information that can be gathered about individual use of computers includes: Web sites visited; Documents accessed; Passwords used; Screen saves can be taken at any time to show what is active; Live monitoring of computer ‘desk-tops’ can be undertaken; Keystrokes can be logged, to show the rate of typing, and spelling errors can be logged to check accuracy; Emails and chats, games played, and applications run can all be monitored (Acespy 2005).

Warehouses

Voice-picking and wearable computers are the more recent trends, the motivators here are increased productivity, reduced staff training overheads (Voicepicking 2005), staff flexibility, and greater profits. The promise of the technology is a powerful motivator for businesses, with claims for voice picking of “Increased accuracy – 99.9% plus, Increased productivity – 15% plus ... The biggest benefits are obtained in low margin, high volume, labour intensive case picking operations, and because of this, the Foodservice Industry and Grocery Retailers and Wholesalers are leading the way in adopting the technology” (Beales 2005).

³ EAS is the existing Electronic Article Surveillance where a tag is fitted to a product, and will trigger an alarm at the exit of the shop unless de-activated ADT. (2005). *Retail Security - Electronic article surveillance (EAS) ADT plc*, [cited August 18 2005]. http://www.adt.co.uk/retail_overview.html. However, shoplifters use devices such as foil-lined shopping bags to make the tags invisible, and so the technology must innovate to overcome the innovations of the criminals Anon. (2005a). *Checkpoint Systems Introduces Security Technology System to "Foil" Shoplifters as They Enter the Store; MetalPoint Detects Presence of Foil-Lined Bags and Clothing Favored by Professional Shoplifters* (June 27) Tmcnet.com, [cited July 12 2005]. <http://www.tmcnet.com/submit/2005/Jun/1158446.htm>.

Productivity increases are widely reported, for example Spar stores “in the first 12 weeks picking errors fell by 90% to 0.01%.” (Gomm 2004). Micro-performance increases generate profits for big employers, and for Argos the “pick accuracy has improved to 99.8 per cent, compared with 98.5 per cent on non-voice sites. A one per cent rise in pick accuracy may not sound like much ... but when you are shifting millions of items a year, that results in a huge improvement in our operations” (Anon 2005b).

The implications for employee surveillance are often implicit in the descriptions of the technologies, for example “voice direction ‘pushes’ pickers harder – workers respond well to verbal instructions” (Beales 2005). The other examples above indicate that the producers of the technology sell a hope of total security through ubiquitous surveillance. The issue of whether the technologies are accurate and reliable, is something that further can be contested, some of those at the leading edge of these technologies confront the issues openly⁴.

10. Pervasive computing does not necessarily lead to positive benefits

If the statistics on retail crime apply widely to the retail environment, then the use of surveillance to counteract criminal activity is a plausible response to such events. Check-out surveillance, however, goes beyond this into ‘dataveillance’ of individual staff over time.

- Point-of –sale transactions can be analysed over time to provide a detailed performance profile of each member of staff, with information relating to the speed at which products are scanned, the income per minute/hour for a member of staff, idle time waiting for customers etc. Each of these can be compared minutely against the performance of other staff working at the same time.
- What this implies is that work norms are less and less set by negotiation between employees/unions and employers, and are more and more able to be set by dataveillance.
- For example, the lower performing employees can be sacked (easy with part-time short-duration contracts), or could better be offered training and incentives to perform better. By removing low performance staff the other staff creates a new ‘cohort’ of workers, and that therefore generates a new ‘low performing’ group of staff.
- Micro-surveillance of performance therefore creates the opportunity for performance targets to move ever upwards in a process that almost propagates itself: remove the low performers, create a new set of low performers, remove them, and so on. At its worst it is a sort of Flanders and Swan ‘gas-man cometh’ process.

11. Call Centres

Call centres present some of the most pervasive surveillance situations. Their very technological infrastructure, comprising sophisticated communications technologies and advanced software systems (Anon 2005d; MiTech 2005; Opera 2005), provide an ideal environment for the micro-monitoring of employees. In recent weeks the New York Times (Dhillon 2005) has highlighted some of the surveillance concerns in Indian call centres – India being a very lucrative location for the offshoring of call centres from North America and Europe. Amrit Dhillon notes the very real tensions that exists in the fears of employers that quality control may not be maintained, or that sensitive data may be released – critical given that many of the call centre operators have access to highly confidential personal health and financial information about the callers.

⁴ See, for example, the White Papers of Ubisense at <http://www.ubisense.net/Product/whitepapers&downloads.html>

Nevertheless, Dhillon clearly differentiates between quality control issues, and the types of surveillance that creates oppressive working regimes. Everything an employee does can be recorded, filmed by CCTV or logged in databases: all conversations, the duration of conversations, timings and durations of meal and toilet breaks, personal searches when entering the premises. The people that Dhillon cites both express resignation and acceptance, realising that there may be no option other than to use surveillance, while others find it intrusive, threatening, and oppressive (Dhillon 2005). The differences in views represent the difference contexts for pervasive surveillance. If it is there as a deterrent, and to provide evidence of activity, then the security context is clear. If the information is then linked to the setting and monitoring of workplace norms the panopticon model appears dominant.

Yet again, however, there is no definitive linear cost benefit arising from pervasive surveillance. First, employees can focus on the activities that they know are being monitored, and influence the statistics. Second, the relationship between subordinates and managers is fundamentally changed: "Management had more personal or 'direct' control before and could isolate individuals' movements, now control has shifted towards more statistical or indirect means ... Thus management can pinpoint their staff's productivity in terms of idle, wrap or live time; however, statistics can be, and are being, manipulated by staff" (McPhail 2001, p.46). As Robins and Webster note in their extensive review of 'technoculture', "the individual becomes the object of surveillance, no longer the subject of communication" (Robins and Webster 1999, p.121).

Keeping calls short to meet performance targets injects a tension into the caller/employee relationship, where the caller wants a reasoned and meaningful response, yet the employee wants the caller off the line as soon as possible (McPhail 2001, p.49). McPhail's extensive study of the call centre literature builds on this argument, noting that the manager/subordinate relationship is further decayed because the majority of interventions telling the employee what to do are driven by the software systems. The manager thus reverts to a form on Dickensian overseer. McPhail also notes that "There is almost universal consensus that call centre work is stressful. Even in studies that report the observation that some staff actually enjoy their work, mention of stress is still the norm, and a significant portion of the call centre literature is devoted to detailing the sources of stress in call centre work" (McPhail 2001, p.51), and the most prevalent creator of stress is reported as being performance targets⁵.

12. Legislative reactions

Does the process of ubiquitous surveillance threaten human rights, or rights to privacy? Will there be likely legal implications if the new technologies cause new types of workplace injury – are effective risk assessments being undertaken for example? In Australia the Government of New South Wales has recently intervened, and will "outlaw unauthorised surveillance of employees using technologies including video cameras, e-mail and tracking devices, when the Workplace Surveillance Bill 2005 comes into effect at the beginning of October" (Baden 2005). Surveillance can only now be undertaken if there is reasonable suspicion of wrongdoing, and employers are now claiming that the balance is tipped too far the other way, and that they may even have to stop logging employees in and out of work using smartcards.

⁵ Further discussions of call centres and surveillance can be found at:

<http://www.econ.usyd.edu.au/wos/worksite/surveillance.html>

<http://www.telework-mirti.org/bagnara.htm>

<http://www.hse.gov.uk/lau/lacs/94-1.htm>

<http://www.janus-eu.org/Documents/EBEW/Call%20Centre%20Employment.pdf>

Legislation, while offering powerful protections, does necessarily reflect events at a particular point in time, and in a rapidly moving labour market and technological environment, legislation quickly dates and becomes contested. The Australian situation seems to make no part happy. Unions do not think it has gone far enough, employers find it too limiting by criminalising surveillance, and privacy organisations such as the Australian Privacy Foundation (APF) argue that “the laws don't force managers to be held accountable for surveillance of staff or force them to justify their voyeurism” (Baden 2005). These contests are developed in more detail in the general briefing on labour market surveillance, but if there is one lesson emerging from these case studies, it is that mediation and negotiation are the better options when surveillance is being introduced.

13. Health and Safety, Risk Assessment

There are very real fears related to the impacts of pervasive computing on employees, yet – as with past technologies and the development of RSI– there is limited acknowledgment of health implications by the suppliers of the technologies. The possible health implications of wearable computers were raised by GMB in June, and were noted early in 2005 by the TUC, and these have been cited by Norwich Union's Risk Services section (NORWICH 2005a, 2005b). While the citations do not in themselves give credibility to the sources (in one case this author and GMB), the act of citation does indicate that those selling risk assessment services see a business opportunity in the area of IT and health impacts.

The literature on IT Ergonomics does acknowledge the possibility of new health problems, particularly since “due to many advances in technology, wearable computers are under development in many companies, but unfortunately design is not stressed in the development process” (Lin and Kreifeldt 2001). This is not surprising, since few technology developers can perceive all the eventual uses for their devices⁶, and therefore even ergonomics cannot predict, and test, the outcomes of all uses (Baber and Baumann 2002).

In an extensive study of the impact of IT on people, the Swiss National Technology Assessment Centre advised that the ‘precautionary principle’ be applied to new technologies in the same way that it is in wider areas of healthcare. Key conclusions were that consideration should be given to:

Stress: Pervasive Computing can generate stress for various reasons, such as poor usability, disturbance and distraction, the feeling of being under surveillance (privacy issues), possible misuse of the technology for criminal purposes as well as increased demands on individuals' productivity. Stress has a considerable impact on health.

Restrictions on individual freedom: The trend toward Pervasive Computing may drive some consumers and patients into a situation in which they are compelled to use such technology (if, for instance, alternatives are no longer available) or to co-finance it against their will (as for example with rising mandatory contributions to health insurance). (Hilty *et al.* 2003, p.17)

⁶ It is often useful to differentiate between ‘devices’ such as a CCTV camera, that become ‘technologies’ when they are embedded into a particular context such as monitoring staff. The devices are neutral, and it is the use to which the devices are put that introduces the contests.

14. Consumer choice can be influenced by ‘social sorting’

Researchers at Stanford University write about pervasive technology also being persuasive technology⁷. A term used to describe this process in the retail and social environment is ‘social sorting’, and it was used recently in a Joseph Rowntree Institute study of the impacts of informational surveillance/classification of local areas in the UK, warning of cities shaped by software: ‘The net may increase segregation and hinder social cohesion’ (JRF 2005). Social sorting is undertaken also for customers when contacting retailers and other organisations via call centres. Call Centre operators need to minimise the amount of time that people are queued for a response, and to make sure that they route the caller to the best suited member of staff (MiTech 2005; Opera 2005). Newer functions in call centre management involve call routing and call prioritisation, where it is possible to prioritise incoming calls by geographical area using Caller-ID facilities, or by customer records according to the recognised mobile or other phone number that was used – hence e-Commerce sites increasingly want you to register on them so that they can store phone numbers registered in your profile. Callers can then be routed according to their commercial importance, or even sorted by software into a queue, for example by linking their address geography to credit referencing classifications. It is in the commercial interest for profits to be maximised by satisfying the highest paying customers first.

The increasing ubiquity of surveillance technologies embedded in products can, it is argued “limit consumer choice if RFID is used ubiquitously so consumers have little option but to accept the technology” (Lace 2004), and Lace further argues that “if RFID is used to gain greater knowledge of consumers, such information could be used in potentially exclusionary ways”. Furthermore like any new technology there may be function creep, as new applications are identified, and the wider use of technologies will place significant ethical burdens on employers. Jones writes of the temptation that may be too great for an employer to resist: “What’s to prevent a company from discovering, for example, that an employee has cancer, and then finding an excuse to fire them before having to honor their insurance commitment to pay for treatment? Sure, that may be illegal, but it’s nearly impossible to prove” (Jones 2005). Privacy International observes that not only can communications be logged, but also that employers increasingly surveil employees for health issues before employing them:

“Psychological tests, general intelligence tests, performance tests, personality tests, honesty and background checks, drug tests, and medical tests are routinely used in workplace recruitment and evaluation methods. Since the discovery of DNA, there has also been an increased use of genetic testing, allowing employers to access the most intimate details of a person’s body in order to predict susceptibility to diseases, medical, or even behavioral conditions”. (Privacy 2005)

Linked to inventory control and supply-chain integration, is the understanding of customer behaviour, and in making the customer the increasingly unpaid worker in the retail process. For example the ‘intelligent shopping trolley’ (Boggan 2005) used RFID recognition, but also can allow the customer to be their own check-out agent. These technologies are strongly linked to the de-layering of staff, and in the de-skilling of staff.

15. The problem is not just the technologies, but may be more one of consent

⁷ <http://captology.stanford.edu/>

Technologies are not in themselves bad, and in general there is little social resistance to using them. It is more an issue of informed consent. Those wearing heart pace-makers have computers inside them that can wirelessly transmit information to machines in a hospital. We frequently see people in the street 'wearing' devices, such as Bluetooth earpieces for their phones, and for most people a mobile phone is never far away physically from their body. People willingly answer to the demand/control aspects of their digital devices, breaking off for example from a physical conversation with a real person who is with them, to answer a telephone call. People will answer often trivial emails rapidly, but be less diligent about responding to a physical letter. Nothing in these actions implies a technological control, since there for each of these actions the person can decide whether to respond to the demands of the technology, or to ignore them.

The International Labour Organisation (ILO) has developed the issue of consent and surveillance technologies, noting that:

- Their use is a violation of basic human rights and dignity, and is often carried out without adequate consideration for such interests;
 - Computer data banks and telephone and video monitoring make prying into the private lives of workers easier to perform and more difficult to detect than ever before;
 - Monitoring and surveillance give employees the feeling that they are not to be trusted, fostering a divisive mentality which is destructive to both workers and employers;
 - Such practices can be used to discriminate or retaliate against workers, which may be difficult for workers to discover;
 - Monitoring and surveillance involve both issues of exercising control over workers and control over data relating to specific workers.
- (O'Neil 2005)

More recently, consent and audit have been embedded in the Wiltshire Constabulary online service for those motorists who have been caught by speed cameras. They can now log onto a Web site, enter the unique reference number on the speeding document, and view the video evidence of their transgression (O'Neil 2005).

16. The demise of the implied social contract?

In a globalised environment of Enron and Worldcom executive failure, yet massive personal financial gain, mass worker surveillance threatens to diminish the fragile social contract that exists between employees and employers, particularly in service industries. I do not resent the five minutes extra time I worked, and you do not resent the one phone call I made home on the company. Ben Willmott of the Chartered Institute of Personnel and Development argues "if employees feel they are being treated fairly and paid adequately, they are less likely to push the boundaries of what is acceptable" (BBC 2004a). Yet mass surveillance will pick up the most trivial of misdemeanours, and as the BBC article concluded "you may not be a thief in the eyes of the law, but you will be pocketing a P45" (BBC 2004a). Ben Willmott called for clear employer policies on what is, and is not unacceptable, and many larger employers do set the boundaries clearly. But, with the prices of surveillance technologies becoming cheaper more and more SMEs can now engage in worker surveillance, and it may be important that they enter into a dialogue with employees, and to set clear boundaries of practice both on employee and employer ethics. As Privacy International found in 2004 the increasing use of surveillance IT was because "it is actually the low cost of surveillance technologies more than anything else that contributes to the increased monitoring" (Privacy 2005), although it would be inconceivable for most profit-oriented firms not to be focused on the bottom-line first, as is

the case for those retailing voice-recognition picking systems (Farrar 2001; Gomm 2004; Microlise 2005), where arguments in favour include the ease of using voice, rather than paper, in hostile environments such as cold stores where employees are wearing gloves (Lacefield 2004).

In the recent case of the suicide of Richard Chang highlights further contradictions in the ethical process, and Pettit cites Mike Ball, employment partner at law firm Halliwells, who argues that covert surveillance of employees is increasing:

The courts have applied a balancing test in cases where human rights are in issue. The right will be upheld to the extent that it does not infringe upon another right. There is also the implied term of mutual trust and confidence. This is included in all contracts of employment. If it is breached, the employee may resign and claim constructive dismissal ... Invasive surveillance would be likely to breach {the implied term} but the employee would have to resign in order to enforce any right to compensation. (Pettit 2004)

Ethics are then strongly linked to trust, and the building of trust between employers and employees is a critical function of trade unions. As David Canton recommends: "Gain consent. Allow employees access to the data that is collected on them... Encourage feedback on how processes could be improved, and generally make employees feel in control of the technology" (Canton 2005). In a large study of RFID and surveillance in the workplace, the Rand Corporation argued "Fair information practices argue that employees ought to be informed about uses of access control system records and have the right to inspect and correct records about their activities", yet the pessimistic following statement noted that "None of the enterprises in our study subscribes to these arguments" (Balkovich, Bikson, and Bitko 2005, p.20). Such resistance is hardly conducive to the building of mutual trust, although Argos is reported to recommend combining the introduction of wearable voice-recognition wireless computers in its warehouses with a need to "engage the staff as early as possible. Emphasise working smarter, not harder", and the accuracy rates of picking products is reported as "improved to 99.8 per cent, compared with 98.5 per cent on non-voice sites", and the 1% increase for a large employer such as Argos is regarded as commercially significant (Anon 2005b).

The surveillance assemblage that confronts employees "marks the progressive 'disappearance of disappearance' – a process whereby it is increasingly difficult for individuals to maintain their anonymity, or to escape the monitoring of social institutions" (Haggerty and Ericson 2000, p.619). In the 2002 Reith Lectures Onora O'Neill talked about a 'crisis of trust' that had been caused by a "culture of accountability", where we are being monitored constantly. As she concluded, Plants don't flourish when we pull them up too often to check how their roots are growing: political institutional and professional life too may not go well if we constantly uproot them to demonstrate that everything is transparent and trustworthy". (O'Neill 2002). Mass employee surveillance constantly pulls up the plant to see what is beneath it, and in so doing damages the building of trust. Trust, built through 'partnership' in the process of technology implementation, was researched by Graham Dietz, who noted that while there are successful examples, a partnership approach is "fraught with risk, centring around its reliance on behavioural consistency and integrity and regular delivery of mutual benefits". He cites the example of "a Unison union representative posing 'the unanswered question' what will happen when they (the employers) want something very badly and we want very badly to stop it?" (Dietz 2004).

In a review of his 'Dataveillance' theory 15 years on in 2003, Roger Clarke was similarly pessimistic. He was saddened by the lack of understanding of business and government about the implications of technologies and technological change. He concluded that "simple-minded, authoritarian corporatism reigns supreme", and that "we're stuck in the old politics of thesis and counter-thesis, the morass of adversarial systems (Roger Clarke 2003). It's simply too easy to say that 'we have no alternative' to mass surveillance. It's too easy to say that the employer has the right to monitor all employees so that they comply totally with law and company policy. It is too easy to assume that mass surveillance leads inevitably to a positive outcome in profitability and efficiency. It's far more difficult to build a 'demos' in the workplace. As Carrico argues, "technological progress without progress toward a more just distribution of the costs, risks, and benefits of that technological development will not be regarded as true 'progress' at all" (Carrico 2005).

From the research literature covered in this briefing, it is clear that there are debates to be developed regarding the accuracy of surveillance technologies, over the quantifiable cost benefits and dis-benefits, over ergonomics and the well-being of employees, and over corporate and employee ethics. As McPhail notes, there is benefit in moving the debates to constructively confront the fears of employees that "processes are streamlined by the simultaneous creation of records and databases at the point of transaction. Second, the same process records a footprint of the activities and performance of agents in minute detail. In this way agents are located in a cycle of accountability which aims to increase reliability and performance accuracy" (McPhail 2001, p.76).

17. Sources of Imagery

<http://www.bcpsoftware.com/solutions/voice/index.php>

<http://www.ferret.com.au/articles/8c/0c035c8c.asp>

<http://www.vocollect.com/>

<http://www.fkilogistex.com/warehouse-distribution/cold-frozen-foods-distribution/31/markets.aspx>

<http://www.metrologic.com/corporate/products/pos/IS4225.htm>

http://www.symbol.com/news/reporters_only/ph_lib_barcode_srs1rs.html

http://www.symbol.com/news/reporters_only/ph_lib_sol_manufacturing.html

http://www.symbol.com/category.php?fileName=CS-27_Peacocks.xml

http://www.voxware.com/index.php?st=products&st1=products_9&st2=

http://www.voxware.com/media/pdf/Product_Literature_VoiceLogistics_02.pdf

<http://www.transmetazone.com/articleview.cfm?articleID=436>

<http://www.mindfully.org/Technology/2005/Worker-Radio-Tags11jun2005.htm>

http://www.peaktech.com/html/products/barcode_scanner/wearable.htm

<http://www.zetes.com/elink/04Q4/uk/voice-recognition-DHL.htm>

http://www.axis.com/products/cam_station_software/index.htm

18. Sources

Acespy. (2005). *Monitor and Control Your Entire Network From ANYWHERE!* (August) Acespy.com, [cited August 24 2005]. <http://www.acespy.com/net-spy-pro-details.html>

ADT. (2005). *Retail Security - Electronic article surveillance (EAS)* ADT plc, [cited August 18 2005]. http://www.adt.co.uk/retail_overview.html

AndyFisher. (2005). *Background Investigation* (August) Andrew Fisher Investigations, [cited August 24 2005]. <http://www.andyfisher.net/backgroundinvest.htm>

Anon. (2005a). *Checkpoint Systems Introduces Security Technology System to "Foil" Shoplifters as They Enter the Store; MetalPoint Detects Presence of Foil-Lined Bags and Clothing Favored by Professional Shoplifters* (June 27) Tmcnet.com, [cited July 12 2005]. <http://www.tmcnet.com/usubmit/2005/Jun/1158446.htm>

Anon. (2005b). *How Argos streamlined store picking with voice* (May/June) Mlogmag.com, [cited August 24 2005]. <http://www.mlogmag.com/magazine/17/argos-streamlined.shtml>

Anon. (2005c). *Human RFID: Medical Gain or Privacy Loss?* (August 4) Top Tech News, [cited August 5 2005]. http://www.toptechnews.com/news/RFID--Medical-Gain-or-Privacy-Loss-/story.xhtml?story_id=01000111V1IW

Anon. (2005d). *Marketing with phone numbers* Startups.co.uk, [cited August 23 2005]. <http://www.startups.co.uk/YZZV5TZoR078sg.html>

Anon. (2005e). *The scourge of Till Fraud - It happens more than you think* (August) Successful Security, [cited August 23 2005]. <http://www.successfulsecurity.com/typesoffraud/>

Axis. (2005). *A new look at retail surveillance* Axis.com, [cited August 18 2005]. <http://www.axis.com/solutions/video/retail.htm>

Baard, M. (2004). *RFID Keeps Track of Seniors* (March 19) Wired Magazine, [cited March 20 2004]. <http://www.wired.com/news/medtech/0,1286,62723,00.html>

Baber, C., and K. Baumann. (2002). *Embedded human computer interaction. Applied Ergonomics* 33 (3): pp. 273-287.

Baden, S. (2005). *Spying bosses will have to come clean* (August 26) Australian Associated Press Pty Ltd, [cited August 27 2005]. http://www.zdnet.com.au/news/security/soa/Spying_bosses_will_have_to_come_clean/0,2000061744,39208891,00.htm

Balkovich, E., T. K. Bikson, and G. Bitko. (2005). *9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace*. Washington DC: Rand Corporation, Report, viii+28 p. http://www.rand.org/pubs/technical_reports/2005/RAND_TR197.pdf

- BALTIC. (2003). *Eva Grubinger, Visualisation of the installation Dark Matter* (November) Baltic Mill Art Gallery, [cited November 14 2003].
<http://www.balticmill.com/html/viegru.html>
- Bamfield, J. (2004). *Key results of the European Retail Theft Barometer 2004* Centre for Retail Research, [cited August 24 2005].
http://www.chant4.co.uk/retailresearch2003/theft_barometer/index.php
- Batista, E. (2003). *Chilly Forecast for Smart Fridge* (August 2) Wired Magazine, [cited August 5 2003]. <http://www.wired.com/news/technology/0,1282,59858,00.html>
- BBC. (2003a). *Inquiries focus on Soham blunders* (December 18) BBC, [cited December 18 2003]. <http://news.bbc.co.uk/1/hi/uk/3329595.stm>
- BBC. (2003b). *Mobile users told to 'chase Bush'* (November 18) BBC, [cited November 18 2003]. <http://news.bbc.co.uk/1/hi/technology/3280611.stm>
- BBC. (2004a). *Are you stealing from your boss?* (April 21) BBC, [cited April 21 2004].
<http://news.bbc.co.uk/1/hi/magazine/3645523.stm>
- BBC. (2004b). *How the boss can monitor you* (March 12) BBC, [cited March 15 2004].
<http://news.bbc.co.uk/1/hi/magazine/3503468.stm>
- BBC. (2005a). *Ethics issue for citizen snappers* (August 5) BBC, [cited August 5 2005].
<http://news.bbc.co.uk/1/hi/technology/4746633.stm>
- BBC. (2005b). *FBI 'missed chances to stop 9/11'* (June 10) BBC, [cited June 10 2005].
<http://news.bbc.co.uk/2/hi/americas/4080554.stm>
- BBC. (2005c). *Software watching while you work* (January 25) BBC, [cited January 27 2005].
<http://news.bbc.co.uk/1/hi/technology/4188747.stm>
- Beales, T. (2005). *Voice Directed Picking: Expected ROI* Business Computer Projects Ltd, [cited August 28 2005]. <http://www.bcpssoftware.com/solutions/voice/whitepaper.php>
- Biever, C. (2004). *RFID chips watch Grandma brush teeth* (March 17) New Scientist, [cited March 18 2004]. <http://www.newscientist.com/news/news.jsp?id=ns99994788>
- Blunkett, D. (2002). *Civic rights* (September 14) Guardian (London), [cited September 14 2002].
<http://www.guardian.co.uk/bigbrother/privacy/statesurveillance/story/0,12382,790138,00.html>
- Boggan, S. (2005). *Big Brother: the spy in your shopping trolley* (April 28) Times (London), [cited April 29 2005]. <http://business.timesonline.co.uk/article/0,8209-1587835,00.html>
- Bohn, J., V. Coroama, M. Langheinrich, F. Mattern, and M. Rohs. (2005). *Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing* Institute for Pervasive Computing, ETH Zurich, Switzerland, [cited August 25 2005].
<http://www.vs.inf.ethz.ch/publ/papers/socialambient.pdf>
- Bristow, H., C. Baber, J. F. Knight, and S. I. Woolley. (2004). Defining and evaluating context for wearable computing. *International Journal of Human-Computer Studies* 60 (5-6): pp. 798-819.

- Firstepos. (2005). *The affects of Till Fraud - It happens more than you think* (August) Firstepos.co.uk, [cited August 24 2005]. <http://www.firstepos.co.uk/TypesofFraud.asp>
- Ford, M. (1998). *Surveillance and privacy at work*. London: Institute of Employment Rights.
- Gomm, K. (2004). *Grocery wholesaler reduces stock errors to almost zero with voice recognition system* (October 29) Computer Weekly, [cited August 24 2005]. <http://www.computerweekly.com/Articles/2004/10/29/206381/Grocerywholesalerreducesstockerrorstoalmostzerowithvoicerecognitionsystem.htm>
- Greenberg, J. (2002). Who stole the money, and when? Individual and situational determinants of employee theft. *Organizational Behavior and Human Decision Processes* 89 (1): pp. 985-1003.
- Haggerty, K. D., and R. V. Ericson. (2000). The surveillant assemblage. *British Journal of Sociology* 51 (4): pp. 605–622.
- Hilty, L., S. Behrendt, M. Binswanger, A. Bruinink, L. Erdmann, J. Fröhlich, A. Köhler, N. Kuster, C. Som, and F. Würtenberger. (2003). *The precautionary principle in the information society. Effects of Pervasive Computing on Health and Enviroment*. Berne: TA-Swiss, Report, 353 p. http://www.ta-swiss.ch/www-remain/reports_archive/publications/2005/050311_STOA125_PvC_72dpi_e.pdf
- INTERMEC. (2005). *Retail Intermec plc*, [cited August 28 2005]. <http://www.intermec.co.uk/>
- Johnston, J. (2003). *CCTV proves 'useless' in fight against shoplifting* (October 19) Sunday Herald (Scotland), [cited August 18 2005]. <http://www.sundayherald.com/print37565>
- Jones, A. R. (2005). *Monitoring Technologies Put Developers in an Ethical Hotseat* (July 13) Devx.com, [cited August 24 2005]. <http://www.devx.com/opinion/Article/28657/1954?pf=true>
- JRF. (2005). *New neighbourhood information websites 'risk widening the gap between rich and poor'* (August 17) Joseph Rowntree Foundation, [cited August 18 2005]. <http://www.jrf.org.uk/pressroom/releases/170805.asp>
- Kablenet. (2005a). *Bichard reveals IT concerns* (March 15) Kable Government Computing, [cited March 16 2005]. <http://www.kablenet.com/kd.nsf/Frontpage/D6A5EB09F9FED44580256FC5003D930F?OpenDocument>
- Kablenet. (2005b). *ViSOR picks up non-offenders* (August 19) Kable Government Computing, [cited August 19 2005]. <http://www.kablenet.com/kd.nsf/Frontpage/B25F5E35C4214672802570610049C63B?OpenDocument>
- Kaupins, G., and R. Minch. (2005). *Legal and Ethical Implications of Employee Location Monitoring* Proceedings of the 38th Hawaii International Conference on System Sciences, [cited August 24 2005]. <http://csdl2.computer.org/comp/proceedings/hicss/2005/2268/05/22680133a.pdf>
- Lace, S. (2004). *Radio frequency identification technology in retail* (February 5) National Consumers Council, [cited August 19 2005]. <http://www.ncc.org.uk/technology/rfid.pdf>

- Lacefield, S. (2004). *Warehouse and DC* (October 1) Voxware.com, [cited August 24 2005]. http://www.voxware.com/media/pdf/LM_10-01-04_01.pdf
- Lacy, S. (2005). *RFID: Plenty of Mixed Signals* (January 31) Business Week, [cited February 11 2005]. http://www.businessweek.com/technology/content/jan2005/tc20050131_5897_tc024.htm
- Lin, R., and J. G. Kreifeldt. (2001). Ergonomics in wearable computer design. *Journal of Evolution and Technology* 27 (4): pp. 259-269.
- Marx, G. (2003). Some Information Age Techno-Fallacies. *Journal of Contingencies and Crisis Management* 11 (1): pp. 25-31.
- McPhail, B. (2001). *What is 'on the line' in call centre studies? A review of key issues in the academic literature*. Toronto: Faculty of Information Studies, University of Toronto. February 21, Report, 109 p. <http://www.fis.utoronto.ca/research/iprp/publications/mcphail-cc.pdf>
- Meijer, A. J. (2005). 'Public eyes': *Direct accountability in an information age* (Volume 10, number 4 (April)) First Monday, [cited April 14 2005]. http://firstmonday.org/issues/issue10_4/meijer/index.html
- METRO. (2004). *The METRO Group Future Store Initiative* (April) METRO Group, SAP, Intel an IBM, [cited April 30 2004]. <http://www.future-store.org>
- Microlise. (2005). *RFID in the Warehouse - An Overview* Microlise.com, [cited August 24 2005]. http://www.microlise.com/microlise_rfid_warehouse.html
- Millar, M. (2005). *Internet use hits productivity costs for employers* (June 2) Personnel Today, [cited August 24 2005]. <http://www.personneltoday.com/Articles/2005/06/02/30156/Internet+use+hits+productivity+costs+for+employers+.htm>
- MiTech. (2005). *Peripheral Applications* (August) MiTech plc, [cited August 22 2005]. http://www.mitech.co.uk/voice/content_peripheral_applications.htm
- Mosco, V. (2002). *From Here to Banality: Myths About New Media and Communication Policy*. Ottawa: Carleton University. November, Report The Institute of European and Russia Studies (EURUS) Europe-Russia Conference Series Conference: Cultural Traffic: Policy, Culture, and the New Technologies in the European Union and Canada, 20 p.
- Mosco, V. (2004). *The Digital Sublime: Myth, Power and Cyberspace*. Cambridge, MA: MIT Press.
- NCR. (2005). *NCR Extends Reach of Checkout Software* NCR Corporation, [cited August 29 2005]. http://www.ncr.com/media_information/2005/feb/pr021005.htm
- NORWICH. (2005a). *Health fears over 'wearable computers'* (June 8) Norwich Union plc Risk Services, [cited August 23 2005]. http://www.nu-riskservices.co.uk/news/articles/cms/1118308605212694732450_1.htm
- NORWICH. (2005b). *Stresses and strains 'not taken seriously'* (January 7) Norwich Union plc Risk Services, [cited August 23 2005]. http://www.nu-riskservices.co.uk/news/articles/cms/1105560755212694732331_1.htm

- NRFID. (2004). *Sainsbury's tagged for security and logistics* National RFID Centre, [cited August 28 2005]. <http://www.rfiduk.org/case/view.php?id=17>
- O'Neil, R. (2005). *Stop Snooping* Hazards.org, [cited August 18 2005]. <http://www.hazards.org/privacy/>
- O'Neill, O. (2002). *Lecture 1: Spreading Suspicion* (April) BBC, [cited April 24 2002]. <http://www.bbc.co.uk/radio4/reith2002/1.shtml>
- Opera. (2005). *Inbound Call Management - Inbound Call Centre* (August) Opera Telecom Ltd, [cited August 22 2005]. http://www.operatelecom.com/data_page.asp?pageID=260&mid=54
- Peissln, W. (2003). *Surveillance and Security: A Dodgy Relationship. Surveillance and Security* 11 (1): pp. 19-24.
- Pepperell, R. (2005). *Posthumans and Extended Experience. Journal of Evolution and Technology* 14 (April). <http://jetpress.org/volume14/pepperell.html>
- Pettit, L. (2004). *The usual suspects: what to consider if covertly monitoring your employees* (August 23) Personnel Today, [cited August 24 2005]. <http://www.personneltoday.com/Articles/2005/08/23/31298/The+usual+suspects+what+to+consider+if+covertly+monitoring+your.htm>
- Privacy. (2005). *PHR2004 - Threats to Privacy* (December 11) Privacy International, [cited August 24 2005]. <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-82586>
- Pruitt, S. (2004). *Managers misuse tech to control workers, study says* (December 2) IDG News Group, [cited December 3 2004]. http://www.infoworld.com/article/04/12/02/HNmanagersmisuse_1.html
- Purcell, J. (2005). *Techno-generation: Cash, card or microchip?* (August 20) Independent (London), [cited August 30 2005]. http://news.independent.co.uk/world/science_technology/article305059.ece
- RetailFraud. (2005). *Retail loss prevention - Maximise profit by reducing losses* Retailfraud.co.ukq, [cited August 18 2005]. <http://www.retailfraud.co.uk/>
- RETEK. (2005). *Tesco Case Study* Retek Inc, [cited August 29 2005]. <http://www.retek.com/solutions/Default.asp?s=5>
- Reuters. (2004a). *Mexican Officials Get Chipped* (July 13) Reuters, [cited July 18 2004]. <http://www.wired.com/news/technology/0,1282,64194,00.html>
- Reuters. (2004b). *Microsoft's Gates Is World's Most 'Spammed' Person* (November 18) Reuters, [cited November 18 2004]. <http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=6853210>
- Robins, K., and F. Webster. (1999). *Times of the Technoculture: from the information society to the virtual life*. London: Routledge.
- Robson, R., and A. Teague. (2005). *Cracking Business Crime*. London: Federation of Small Businesses. August, Report.

- <http://www.fsb.org.uk/policy/assets/FSB%20Cracking%20Business%20Crime%20Report%20web.pdf>
- Shury, J., M. Speed, D. Vivian, A. Kuechel, and S. Nicholas. (2005). *Crime against retail and manufacturing premises: Findings from the 2002 Commercial Victimization Survey*. London: Home Office. July, Report, 113 p. <http://www.crimereduction.gov.uk/business42.htm>
- Symmetry3. (2005). *Tracking - Covert Tracking* Symmetry3, [cited August 24 2005]. http://www.symmetry3.com/covert_tracking.htm
- TEXAS. (2005). *Focusing on Retail Visibility* Texas Instruments, [cited August 30 2005]. <http://www.ti.com/tiris/docs/solutions/epc/retail.shtml>
- Torex. (2005). *Smart Retail Product Overview* Torex Retail, [cited August 18 2005]. <http://www.torexretail.com/english/solutions/retail/in-store/smart-retail.php?navid=28>
- TUC. (2005). *Sicknote Britain?* London: Trade Union Congress. January, Report, 21 p. <http://www.tuc.org.uk/extras/sicknote.doc>
- Voicepicking. (2005). *Frequently Asked Questions* Voicepicking.com, [cited August 24 2005]. <http://www.voicepicking.com/>
- Whittle, S. (2000). *Stop your staff from abusing the internet* (September 8) Vnnet.com, [cited August 24 2005]. <http://www.vnnet.com/vnnet/features/2129825/stop-staff-abusing-internet>
- Williams, R. D., and M. Williams. (2002). *Technology Issues In Restaurants - Summary Of FS/TEC 2002 Presentation* HVS International, [cited August 23 2005]. <http://www.hospitalitynet.org/news/4013801.search?query=%2225%25+of+employees%22+honest>
- Wolrich, C. (2005). *Top Corporate Hate Web Sites* (March 8) Forbes Global, [cited March 9 2005]. http://www.forbes.com/technology/2005/03/07/cx_cw_0308hate.html
- Xpert. (2005). *Retail* Xpertcommunications.co.uk, [cited August 18 2005]. <http://www.xpertcommunications.co.uk/markets/retail/solutions/>
- York, J., and P. C. Pendharkar. (2004). Human-computer interaction issues for mobile computing in a variable work context. *International Journal of Human-Computer Studies* 60 (5-6): pp. 771-797.
- ZEBRA. (2005). *Retail: Keep customers coming back and keep stock from running out*. Zebra.com, [cited August 28 2005]. http://www.zebra.com/id/zebra/na/en/index/industry_solutions/industries/retail.html
- Zeller, T. (2005). *When the Blogger Blogs, Can the Employer Intervene?* (April 18) New York Times, [cited April 18 2005]. <http://www.nytimes.com/2005/04/18/technology/18blog.html?oref=login>
- Zetter, K. (2004). *Jamming Tags Block RFID Scanners* (March 1) Wired Magazine, [cited March 1 2004]. <http://www.wired.com/news/business/0,1367,62468,00.html>
- Zetter, K. (2005a). *Driving Big Brother* (June 21) Wired Magazine, [cited June 22 2005]. <http://www.wired.com/news/privacy/0,1848,67952,00.html>

Zetter, K. (2005b). *School RFID Plan Gets an F* (February 10) Wired Magazine, [cited February 11 2005]. <http://www.wired.com/news/privacy/0,1848,66554,00.html>

Zetter, K. (2005c). *Surveillance Works Both Ways* (April 14) Wired Magazine, [cited April 18 2005]. <http://www.wired.com/news/privacy/0,1848,67216,00.html>