FROM WORKPLACE WATCH TO SOCIAL SPY:

SURVEILLANCE IN (AND BY) THE WORKPLACE

An updated Briefing Paper for GMB

September 2011

Professor Michael Blakemore

About the Author

Michael Blakemore (http://michaelblakemore.co.uk/) is, among other things, Emeritus Professor of Geography at the University of Durham and for many years was closely involved in the development of geographical information databases (for example the UK labour market system Nomis www.nomisweb.co.uk) and the use of geographic information in location based services. That took him into areas of access to information (freedom of information, charging for government information etc.) the social history and use of the information, and the development of e-Government services, and social inclusion, within the electronic Information Society.

Mike relies on surveillance to make his work and life easier. He can remember the days before mobile phones when contact with family was not instant, as it is now, but really difficult – on a research visit to the Sudan in the early 1990s he 'disappeared' for two weeks once removed from email and direct phone lines. He needs to have his financial transactions closely monitored by his bank and card companies – this allows him to travel frequently and to use his cards with ease and with the minimum risk of fraud occurring. However, he has seen the downsides of management by spread-sheet and micro-monitoring of performance targets.

He worries that he is leaving a vast electronic trace of his life and that others know more about him than he can remember. He does not remember for example what he purchased last weekend in a supermarket, but they do to the minute and by the item, but he is not sure whether his inability to remember it is more a function of ageing. He delights in the utility value of interconnected information technologies to work in ways that were simply not conceivable back at the start of his career, but do not expect to find him on Twitter or Facebook.

1. LOOKING BACK AND LOOKING FORWARD

It is six years to the month since the first version of this paper was prepared for GMB in 2005. It is also ten years to the month since the events of 9/11 set in train a significant growth in monitoring and surveillance by governments of their citizens within the context of strategies to combat global terrorism. As has ever been the case with the technologies of surveillance, what was created for military and security purposes has often been utilised beyond those sectors (the process of **function-creep**), and the industry that has serviced that growth has produced products has been used ever more pervasively in surveillance and monitoring in the workplace.

POST 9/11 AND THE 'FLUID' WORKPLACE

However, other things have happened that complicate what six years ago was a picture of workplace monitoring, and the past five years have not been ones just of more surveillance by employers of their employees. A significant development has been the widespread blurring of the boundaries of work and home, with high-speed broadband access to the Internet and the dramatic development of social networks has led to the workplace often being a place where employees access their online private lives (email, social networking, online shopping etc.). Writing in the Financial Times on September 7th 2011 Richard McGregor noted that in the USA:

> "*the 9/11 attacks prompted a surge in US national security spending, and led to legislation that gave the government more tools than ever to monitor its citizens*", concluding that "*with a new social contract at home, trading off surveillance for safety. The land of the free is being watched over like never before*" (McGregor 2011)

Substituting the UK for USA into those phrases resonates with what has happened also in the UK, with its strong links to the USA and its own experiences of the impact of global terrorism with the 7/7 attacks in London, associated with the legacy of IRA terrorism on the British in past decades.

Back in 2005 the 'organisation' or the 'workplace' had often ceased to be a dominantly physical entity where, for example, organisational property moved in and out of the factory gates and where physical searches of employees could take place. Organisations increasingly had 'fluid' boundaries where property (in particular intellectual property or confidential information stored in electronic databases) could be transmitted beyond the organisation through a simple email attachment – there were many different 'factory gates'.

The workplace of 2005 was increasingly electronic, with employers increasingly reliant on high-speed and interconnected electronic networks where the risks that sensitive information could move beyond the organisational boundary within milliseconds. In that context staff who had access to electronic information could be subject to surveillance of their activities to see if they had (it was difficult to predict intentions, although as we will see later there are new developments that try to predict likely behaviours) done something unethical or illegal.

More nefarious for the workforce, however, was the development of technologies that pervasively and persistently monitor workplace activity, ranging from wearable computers in retail distribution centres (monitoring the movement and activity rates of employees, with the information system managing their movements) to the monitoring of computer activity such as typing speeds and spelling errors in a process of increasing productivity by staff.

The rapid development of the Information Society presented threats that employees could use information communication technologies (ICTs) unethically (for example accessing pornography or sending organisational confidential information to others via email). It also presented opportunities to persistently monitor (control and performance) what employees were doing, and to increase productivity both through performance monitoring and through increasing task automation. This was seen in 2005 where there were investments into automated warehouse management systems – in effect removing the perceived inefficiencies of humans (and at the same time removing ethical criticism when the humans were persistently monitored) by using robotics to undertake the tasks. Robots after all do not demand holidays, are not unionised, and can be easily replaced.

2005, then, was the time of '**Workplace Watch**' where what went on in the workplace could be the subject of intense electronic scrutiny by employers.

THE PRIVACY PARADOX – WHY WORRY ABOUT SURVEILLANCE?

A **Privacy Paradox** was present – the extent to which electronic surveillance was both needed and acceptable, against the extent to which it impacted on the privacy rights of the individual employees. The surveillance industry frequently cited 'research' which claimed to show the extent to which employees were not to be trusted. Mantras were often used to demonise those who promoted privacy over surveillance, most commonly arguing '*you have nothing to fear about surveillance if you have nothing to hide*'[1], an argument sometimes cited by proponents of city-wide surveillance schemes where, as in the case of the London Congestion Charging (Anon 2011a) scheme, the benefits are seen as outweighing the surveillance risks.

Therefore workers in supermarkets should accept that there are software systems looking at their throughput of items (productivity), the extent to which sales are voided or items not scanned (checking whether they are not scanning items for friends), and checking for till fraud (theft of money). The argument given is that by identifying those who are carrying out fraud, and deterring others, the jobs of those who are ethical are better protected. It's a simple argument, especially since the business profits also are better protected. The ethical concern about function-creep is that it is not just those who are fraudulent who are identified, but also those whose productivity is below a particular norm.

There is lot of history in the privacy paradox, and to a large extent anyone who uses a debit or credit card is de-facto accepting that their purchase history (where, when, and what they purchased) is being tracked and analysed so that they can both purchase easily when they travel, and that the banks can detect rapidly if their cards have been stolen. The persistent surveillance of our activities empowers us to be mobile. Our 3G mobile phones need to know where we are so that we can receive phone calls, messages and emails. That information is stored for a long time and is accessible to the Police and security services under legislation such as the RIPA Act[2]. The Act states clearly the conditions under which covert surveillance can take place and our electronic audit trails (emails, phone records etc.) can be acceded.

Workplace surveillance is often justified for the positive outcomes it can bring, such as the monitoring of key-workers when they travel from client to client, through monitoring for health and safety reasons, or through collaborative surveillance of risks and dangers. It has, and continues to involve, a set of electronic technologies that over the past six years have shown a new set of characteristics in addition to those covered in 2005 – and which are still relevant today.

[1] See Daniel Solve's elegant debunking of this argument http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

[2] Regulation of Investigatory Powers Act (2000). http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

FROM WORK SPACE TO SOCIAL SPACE – NEW BEHAVIOURS

In 2011 the first of two emerging characteristics is ‘**inter-visibility**’. Six years ago high-speed mobile broadband was limited and expensive, and mobile phones were relatively basic compared to the ‘smart’ 3G phones (Blackberries, iPhones etc.) used today which have considerable computational power as well as being integrated communication devices. Social networks were in their infancy, with MySpace (launched in 2003) being the precursor to the currently dominant Facebook, Twitter, and photo/image sharing resources such as Flickr.

Increased access to information means that both employees and citizens, and employers and organisations are able to ‘see’ much more about each other than ever before, and to collaborate more effectively. The recent political changes in countries such as Tunisia, Yemen and Egypt in part were assisted by the **ability of citizens to self-organise** across information and communication networks (BBC 2011c; Preston and Stelter 2011), and the regimes being threatened by the protests tried to switch off access to the Internet (BBC 2011c; Mims 2011), and put pressure on mobile phone operators to restrict access (Parker 2011).

One response to censorship comes through organised hacking of government Web sites (BBC 2011g), activities views in this instance very much as being a part of democratic protest, but which in another context would be deemed a criminal act. Similarly, the case of Wikileaks (WIKILEAKS 2009a, b) excites both support and condemnation depending on the whether people support totally open and free information, or whether there is acceptance for the relevance of state secrets (Menn 2011; Scott 2011).

Whatever the ideological position, there are strong lessons for individuals – if people can ‘see’ and can liberate information that was being securely held by organisations, then **organisations can often ‘see’ and can use information that you place on the Web** about your own social and professional activities, personal habits and lifestyle etc. This has potential ramifications if employers can see what you are saying about them on social network sites. There has been **a rapid blurring of the boundaries between the private and the public information** and communication channels.

This has led to the **extension of Workplace Watch** into a new **Social Spy** where your personal life is more easily surveilled than ever before. The ramification of this is the need for employees, as well as employers, to build ethical behaviours and to be aware of the consequences of their behaviours – advice and best practice are vital.

The second new characteristic is **a deeper integration and power of surveillance technologies**. In 2005 biometric surveillance was at an early stage, and the volume of potential information about individuals was presenting analytical challenges and required a lot of computing power. Indeed, there were some views, this author included, that the sheer volume of information, and its distributed nature across many data sources and producers/domains (Phone companies, social Web sites, Internet Service Providers etc.), meant that ‘information overload’ was a protection against the information being used coherently. That has not been the case, and while the information volumes have increased the computing power and software sophistication have more than matched it, and **new and ‘smarter’ technologies are making it easier to develop integrated surveillance** across many domains. Surveillance power is keeping ahead of the information volume.

2. LEARNING FROM HISTORY - SURVEILLANCE IS NOT NEW, BUT ITS NATURE CONTINUES TO CHANGE

Electronic snooping is as old as electronic communication technologies – in the very early days of telephone exchanges an operator in the exchange could easily overhear conversations between callers. In 1987 Time Magazine was warning that *“for a relatively small outlay it is possible to eavesdrop on the microwave frequencies that computer equipment use to transmit data for example from disk to visual display unit within a desktop microcomputer”*(Church 1987). Checking up on employees is nothing new whether it is through physical or electronic surveillance. 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.

PROPORTIONALITY AND CONSENT

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 practices 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, and there was to a large degree proportionality in the process – not every employee was intercepted and checked either for good reason, or as part of a random sample for searching.

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) – proportionality was becoming subjugated to pervasiveness. The computing environment could now collect information that is more ‘context aware’ (knowing not what we do, but when and where (Huw Bristow *et al.* 2004)), and this created 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). This tension was evident in the 1990s and Johnson, reviewing workplace monitoring laws and practice in Colorado, observed that workplace surveillance needed to be proportional to the risk, not pervasive, and that ‘horror stories’ did exist: “*an express-mail company employee whose computer logged the length and frequency of her trips to the restroom, and who was reprimanded for using the restroom four times in one day*” (Johnson 1995).

The rapid growth of mobile and ambient technologies in the past decade introduced 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 argued that the embedding of technologies into our persona (worn computers, RFID chips in clothing for example), take us into a ‘post-human’ environment where “*we are physically grounded but conceptually extended*” by the information systems that tell us what to do (Pepperell 2005).

That said, if there is consent then the embedding of technology does not in itself render us post-human, and the Baja Beach Club in the UK had offered the possibility for VIPs to be microchipped (90 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). In recent years the miniaturisation of IT has led to significant potential benefits in health monitoring, for example with a temporary tattoo which has technology to monitor wirelessly the vital signs of patients in hospitals (BBC 2011d; Fleming 2011), and which could avoid the distressing signs of patients wired up to lots of machines. There are even workplace surveillance technologies emerging which focus on maintaining the well-being of staff, as in the case of devices that monitor the physical inactivity of desk-bound staff, and which can alert them to the need to move or exercise (Singer 2011b)[3].

So running through these discussions are fundamental issues proportionality (is the surveillance justified, targeted, or pervasive?[4]), privacy (is it secret or clandestine, or is it 'visible' in that the employees are aware?), and is the purpose clearly stated and accepted? For example, the rapid growth of IT devices for the monitoring of healthcare requires that as far as possible there is acceptance by patients – this is being studies within a '*Chain of Trust*' project funded by the European Commission (EAHC 2011).

3. TECHNOLOGICAL SURVEILLANCE AND THE ORGANISATIONAL 'BOUNDARIES'

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. In the post 9-11 security and surveillance context both things are happening together – everything can be logged and vast resources allocated to its analysis. The US National Security Agency "*needs all the storage space it can get. According to James Bamford, author of numerous books on the agency, it will store data roughly equal to a septillion – a 1 followed by 24 zeroes – pages of text by 2015*" (McGregor 2011).

Electronic surveillance became deeply embedded in the US Homeland Security response to 9-11, such as proposals to embed RFID chips into the I-94 immigration form that must be carried by immigrants. While this would allow security services to identify the immigrant remotely, the Electronic Privacy Information Center (EPIC) warned that if unauthorised scanning of the tag was undertaken "*foreign visitors could be identified as such merely because they carry an RFID-enabled I-94 form*" (Komp 2005). In recent years the information demanded by US security has increased, causing political tensions with Europe (EUPARL 2011; EUROPE 2011a).

UNDERSTANDING PERVASIVE SURVEILLANCE

Access to comprehensive information that is joined up has been vital for the prevention (such as the massively integrated surveillance system used by the US in Afghanistan (Shanker 2011)) and detection of terrorism (such as the new 'theatre' of war in cyberspace between governments and hackers (BBC 2011k, m; KABLE 2005b;

[3] And such technologies can be used to 'self-track' and monitor your health pervasively. For example, for the self-employed the priority is to stay well, and to avoid illness Dembosky, A. (2011) Singer, E. (2011c).

[4] This was clearly evident in the development of Google Street View where there were early concerns over the privacy of people who were photographed by the camera cars and whose images were then shown online Agger, M. (2007) BBC. (2008) BBC. (2009), or where the images could allow people to look into properties and for criminals to examine properties remotely and assess the potential to burgle them Agger, M. (2007).

Schmitt 2011)), 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 (KABLE 2005a). In 2011 The UK Information Commissioner expressed concerns over the rise of integrated information for vetting people by the police and other authorities, and the potential disproportionality of use:

> "*However, by saying that the vetting scheme 'is about making sure we can stop that very rare risk, because if it led to harm, the harm could be devastating', the previous Government revealed an approach to risk that established an elaborate system to guard against events that, they admitted, were highly improbable. This raises concerns about the disproportionality of a Scheme that, according to some, reverses the assumption of innocence regarding the individual and may lead to decisions being influenced by 'soft' information*" (COMMONS 2011).

Even if all the information is available, then, 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 at that time meant that the IT systems, combined with the inefficient human procedures, 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. As already noted the brute force of computing is increasingly capable of processing vast information resources.

Roger Clarke warned that the underlying data from the separate sources are often not robust and accurate to the same levels, 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 was even the subject of art (BALTIC 2003).

So, surveillance can be 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, and MIT's Agelab is researching the use of remote monitoring of health for an ageing population so that relatives can constantly check the well-being of relatives beyond physical visits or phone calls (MIT 2011);

- **Audit trails**, such as the IT evidence trail that helped convict Harold Shipman, but which also led to calls for patients to have access to their own health records (KABLE 2008);

- 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, which is extending to many areas such as tracking clothes and what is becoming known as a sea of sensors and the 'Internet of Things' (Bustillo 2010; Kroes 2010);

- Linking material in **global supply chains** – rapid re-ordering (Torex 2005), and linking sales data to customer data (FT 2011; Hammond 2011; 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 2005a). 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 2005d). 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. A response from the technology industry is to have the recognition devices discriminate between living or dead human tissue (Marks 2011);
- **Citizen surveillers** are 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). In 2011 the Mass media now invite us to send our pictures and videos from our camera phones, to post our comments to their articles online, to phone in a 'participate', but Walter Kirn does worry that we become observers of society rather than participants within it[5]: "*Ours is a fragmentarian society, infinitely divided against itself and endlessly disrupted from within by much the same technologies that, in Orwell's somber novel, assured a dull and deadening stability*" (Kirn 2010).

The process of surveillance of the workplace 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 back in 2005 involved:

- **Defamation** of an employer using workplace blogs (Zeller Jr 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).

[5] And even the Pope has expressed concerns over the potential societal harm of social networking and other participatory and observant activities. Benedict XVI, P. (2011) Pullella, P. (2011).

There was a set of counter play activities emerging that, in addition to unexpected behaviour changes noted earlier, were a response to surveillance in the workplace:

- Those carrying out surveillance could themselves be counter-surveilled. Steve Mann used the term "*equiveillance through sousveillance*" (Zetter 2005b). **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 Jr 2005).

- More extreme was the development of **corporate hate sites** (Wolrich 2005)

- Those who are required to be surveilled could demand intrusive surveillance from those who are carrying out surveillance. Steve Mann, for example "*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 2005b).

- There was a 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). This was, of course, seen powerfully in the political changes that recently occurred in countries such as Egypt and Tunisia (BBC 2011l; Palfrey 2011; Preston and Stelter 2011).

- **Overloading** executives who are seen as central to information technologies, or who impose surveillance and surveillance technologies with communication overloads. Bill Gates was in 2005 the most spammed person in the world, and Microsoft invested 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. Currently this activity includes monitoring the Twitter activities of MPs (Eyespymp 2010).

- **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 in itself directly lead to productivity benefits that are stable. However, the sophistication of the privacy paradox and the risks of function creep are not issues that the surveillance industry and military complex promotes, tending to prefer rather more 'black and white' arguments, and these are reviewed in the next section.

FIND 'EVIDENCE' TO JUSTIFY PERVASIVE SURVEILLANCE

Gary Marx, a leading researcher 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*". (19) "*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 prevailed 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 if 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 an ethical challenge for co-workers, for to be part of the '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*", and this fallacy is often linked to the statement that 'why worry since all your information is available anyway'[6] (Havery 2005). Such statements are easy to make, but hold credibility only if you are confident that total surveillance will not deliver negative outcomes. Over-surveillance may lead 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).

But the myths provided by Gary Marx are a bit too complex, and invite debate. It is easy to grab onto something that becomes a credible truism. The simpler the message the better, especially if it is a myth that is allegedly grounded in research. As Vincent Mosco says in his influential critiques of the global information society, "*myths are not true or false, but are dead or alive*" (Mosco 2004, p.29), and a particularly pervasive myth has been promoted by the surveillance industry for ten years without any clear reference to a research or evidence base to substantiate the claims. For example: (Williams and Williams 2002) (Anon 2005f) (AndyFisher 2005) (RetailFraud 2005) (Firstepos 2005) (Anon 2011c; ESCO 2011) (RetailFraud 2011). The alleged statistics are conveniently rounded to 25% segments, and the mantra that is repeated without citation is "*Research shows that 25% of employees are totally honest, 25% are totally dishonest, and the remaining 50% are swayed by opportunity".*

The myths help to demonise employees and to label them as being systemically dishonest (CM 2005) (TEXAS 2005), as regarding theft as a perk of their job (Anon 2005f), and therefore "*There is no such thing as too much security*", (Baden 2005). Now add to that the portfolio of new evils that are allegedly manifested through employee usage of Internet bandwidth while at work. In the USA it is alleged that "*90% of employees use office email for personal reasons. 70% of all web traffic to Internet pornography sites occurs during the work hours of*

[6] This is a strange statement, since there is everything to fear if the information is 'out there', and can potentially be joined up to profile you.

9am-5pm" (SPYSURE 2011). 'The Profit Experts' focus on a geographical connection, linking two separate observations into a spurious causal link: they cite that most shoplifters live within a 5-7 mile radius of a store, and that most employees live within the same radius. Thus, rather than to observe simply that it is preferable both to minimise journey to work (employees) and journey to store (customers) the two observations are conveniently conflated:

> "*If your employee and shoplifters live in the same community, eat in the same restaurant, swim in the same pool and play football together, can you really trust all of your employees?*" (Anon 2011b).

Gary Marx's fallacies appear clearly in the demonization of employees. While employee theft does occur, as does unethical use of the Internet, the material above relates strongly to the 'nothing to hear if you have nothing to hide' arguments, so why not check everything:

> "*What can you do to stop this abuse and prevent staff from stealing your time and eating into your profits? Keylogger software allows you to record every keystroke made on a computer. As an employer a spy keylogger, together with encryption and security tools, will let you see what your staff are doing on the office computer – working or gaming and downloading internet pornography?*" (SPYSURE 2011).

To paraphrase the famous TV series Hill Street Blues catch-phrase from Sergeant Esterhaus, employees are painted as being pervasively evil in the workplace, so "*let's be careful out there*". What we will see now as the material moves on from 2005 to 2011, is the need for care by both employers and employees has increased dramatically.

4. THE INTEGRATION OF SURVEILLANCE AND BLURRING OF WORK AND HOME – THE EMERGENCE OF THE SOCIAL SPY

The 2005 report was characterised by increasingly sophisticated surveillance technologies, but they were generally operating independently of each other. For example CCTV systems and electronic point-of-sale (EPOS) solutions were not joined up. One software package may have been able to monitor what people were typing on their keyboard, but not what they were typing on their phones and posting online. With the emergence of increasing staff access to external Internet resources, and also using mobile technologies, the monitoring capabilities have become more integrated, more real-time, and more individualised. CATAPHORA now provides solutions to monitor not just employee activity, but also monitors their behaviours to try and predict problems. It checks:

> "*e-mail, instant messages, calendar events, documents, and even phone logs … Cataphora tracks use of exclamation points, font color, capitalization, punctuation "cursing," the way people sign off in an e-mail, and the overuse of certain words, such as "please."*"' (CATAPHORA 2011; Greene 2011)

The integration of surveillance is made much easier by the sophistication of Internet networking and mobile phones. In 2005 phones had cameras and some mobile Internet, but now "*come packed with sensors capable of tracking them as they move. The digital compasses, gyroscopes, and accelerometers embedded in such devices have spawned a wide range of location-based services*" (Graham-Rowe 2011) – services that both can benefit the user and can provide detailed and sophisticated audit trails to others. Networking and real-time monitoring is central to the BRULINES service where pervasive monitoring of drink dispensing and sales records is implemented in over 22,000 pubs (one-third of all pubs in the UK (BRULINES 2011).

Broadband networking now enables remote surveillance of activity, and some solutions are sold for both workplace and domestic use – potentially relevant for people who work at home. For example "Realtime Spy Remote Spy" is a software solution that runs invisibly to users:

> "*view activity logs from any location at any time! Log Keystrokes typed, Email Activities, Website Visits, Chat Conversations; Log Files and Documents Viewed, Desktop Screenshots; Monitor your PC from Anywhere, View Logs from any Location at any time; Run in Total Stealth, Remotely Installable with Popup Notification*" (AWOSOFT 2011).

Networked solutions build on top of the more conventional approaches in retail stores combining electronic anti-theft approaches (RFID etc.) with visible or concealed alarm systems at store entrances and exits, and a range of video monitoring with real-time analytics, for example checking for suspicious movement (ADT 2011).

But it is the newer monitoring facilities and associated 'forensics' and analytics which mark out the big changes since 2005. Glen Derene itemises the detailed evidence trail left behind even when we think something is deleted from an electronic device such as a phone or computer. Unless a security 'scrubbing' programme is used 'deleted' files are deleted from a file-system but the contents can remain on a disk:

> "*In fact, it's relatively easy for security software to salvage sections of documents that you created, thought better of, then rewrote, because the automatic save features of Microsoft Office may have committed them to disk before you backspaced. Cellphones, too, can be forensically examined for data, documents, contact lists and call logs*" (Derene 2009)

Any activity on a company VPN (virtual private network) will almost certainly be logged, and company phones can have a security setting where contents can be wiped remotely if an employee misuses it, and where the location of the phone can be tracked all the time.

NEW BEHAVIOURS

Recent years have seen a continued contradiction between private desires for privacy and anonymity and the diversity of fly-on-the-wall television programmes where the privacy (and often the dignity) of individuals is sacrificed for the production of programmes such as 'Big Brother', about people with obesity, dysfunctional families, security agencies (Police, Border Agency), emergencies (Accident and Emergency). However, it is not television which has been the stimulus for behaviour changes in surveillance, but the combination of the mobile phone and social networking. Already noted above is the detail and depth of information left as evidence by phone use.

However, combine the phone with the social networking resources such as Facebook, Twitter and Flickr and there is a powerful combination of mass production and communication outlets. For example, newspapers and other publications are harnessing the power of individuals to report stories and provide images taken with their phones (ECONOMIST 2011b; Newman 2009; Shiels 2010). An individual person is endowed with considerable power by a mobile phone and a social networking or Web site outlet, as was the case with a person who shamed British Airways about an allegation of bed-bugs in a business-class bed (Bradshaw and Clark 2011).

So, businesses that previously monitored customer activity can now experience the customers (from individuals to self-organising groups whose like is an issue and an online outlet) monitoring them. This has led to businesses monitoring social networks to see what is being said about them, to identify emerging customer issues, and to be more proactive in resolving the issues (Bird 2011; Singer 2011a) (Groeger 2011; Naone 2011; Wakefield 2011). While this can be positive, however, it is accompanied by the potential for companies to check not just what their customers are saying on social networks, but what their employees also are saying and doing. As Brian Stelter warns it is:

> "*more and more likely that every embarrassing video, every intimate photo, and every indelicate e-mail is attributed to its source, whether that source wants it to be or not. This intelligence makes the public sphere more public than ever before and sometimes forces personal lives into public view*" (Stelter 2011).

The extensive audit trail left by individuals and organisations is not overwritten each time a Web site changes. Apart from databases that store information, and which can be accessed through legally approved channels, Web sites themselves are archived as part of the 'Internet Archive[7]', and its 'WayBack Machine[8]'. Putting in www.tuc.org.uk into the WayBack Machine it returns the text "*http://www.tuc.org.uk/ has been crawled 774 times going all the way back to January 3, 1997. A crawl can be a duplicate of the last one. It happens about 25% of the time across 420,000,000 websites*". So the Archive has 774 captures of the TUC Website over a period of 14 years – evidence of past activity that the TUC probably does not hold itself, and which is probably true for most organisations with Web sites.

The detailed and expanding archival evidence trail, and the expanding use of online presence through social networking sites in particular, combined with the use of employment resources beyond the organisational boundary (for example working from home or when travelling) and personal resources within the organisational boundary (e-shopping or sending emails while at work for example, means that:

> "*the lines between work, and the rest of life have never been more blurred. This muddling of professional and personal identities can be disruptive in the workplace*". (Gelles 2011)

Making comments about work on a social site can be problematical as a US police officer found when following a fatal shooting he changed his occupation on Facebook to "human waste disposal", and this was noticed and publicised by a local TV company and led to him being disciplined (Goode 2011). That situation was the result of a human process linking bits of information, but increasingly that process is automated, and it can involve linking and analysing information in innovative ways, for example:

> "*Researchers at Hewlett Packard showed that they can accurately predict a Hollywood movie's box office takings by counting how often it is mentioned on Twitter before it opens*" (Weber 2010).

As well as leaving rich personal evidence trails individuals also embrace the surveillant processes in ways that may seem prurient – such as Tubecrush.net where commuters take photographs of "*strangers they find attractive or eye-catching*", upload them to the Web without the permission of the person (Cooke 2011). In the US an artist collected images from a publically-accessible Webcam in an Apple store and displayed them on a Website (BBC 2011i). At the more social level local communities can now establish their own CCTV networks in a private form of 'neighbourhood watch' (Blake 2011; JABBAKAM 2011).

This social surveillance approach has been extended into the monitoring of the activities of politicians (MEPRANKING 2010), to shoplifting where citizens can watch CCTV cameras in stores and be rewarded if they report a crime – free entertainment is being swapped for free working as a surveillance agent, although the Information Commissioner required changes after images had been shared via YouTube, and "*the firm must also ensure that no viewer can access footage from cameras located within a 30 mile radius of the viewer's location*", presumably to avoid recognising neighbours and friends from their own locality (BBC 2011a).

[7] http://www.archive.org/

[8] http://wayback.archive.org/web/

The act of surveillance is therefore not something that is good or bad, but it is along a continuum of acceptability, where acceptability often is determined by opportunities that are identified by organisations and individuals. Coupled with the rich evidence trail left by professional and social activity on the Web it is little surprise the services exist to track Your employees or potential employees (FORBES 2011; Preston 2011) across their social network and media history, and people are sometimes finding that their past Web activity can be an impediment when applying for jobs (Preston 2011). For example, regarding services provided by Social Intelligence Corporation in the USA:

> “*in a given pool of candidates they screen, there are usually 20% who don’t pop up in an Internet/social media screen … 60% have a neutral or positive Internet footprint … and 5-20% of applicants have something negative out there about them.*” (Hill 2011; SOCIALINTELLIGENCE 2011)

‘Social Sentry’ is a comprehensive service for employers to track any employee across their internet activity

> “*to make sure that employees don't leak sensitive information on social networks or engage in any behavior that could damage a company's reputation … Social Sentry only tracks information that is already public*” (Lardinois 2010).

Some organisations are addressing these issues more positively by setting clear standards of ethics and behaviour – what is termed digital etiquette (Bourzac 2011) and accepted use policy (Lipowicz 2011). Prevention is better than cure given the risks incurred by the speed at which comments and misinformation can flow across the Internet causing rapid and widespread damage (BBC 2011h). Some emerging business models have identified a potential market where individuals store in detail their digital activities, attempting to overcome the existing problem that databases and other information sources currently know more about them than they do themselves – for example where supermarkets ‘remember’ more about a purchase history through loyalty schemes than individuals can possible remember.

A German politician requested that Deutsche Telekom provide him with the audit train of information they held about his mobile phone use, and:

> “*In a six-month period — from Aug 31, 2009, to Feb. 28, 2010, Deutsche Telekom had recorded and saved his longitude and latitude coordinates more than 35,000 times. It traced him from a train on the way to Erlangen at the start through to that last night, when he was home in Berlin*” (Cohen 2011)

Seeing this as an opportunity for people to retain their own evidence base First Location Bank allows you to

> “*check your location account. Review your runs, rides and trips on the map. Monitor your movements to simplify your expense claims. Get a hard copy record of where you've been*” (FLB 2011).

SMART TECHNOLOGIES

Whereas the 2005 review looked at technologies that collected data in sophisticated ways, the 2011 situation shows more technologies that both collect and analyse data in sophisticated ways. There are many positives in the ability of new technologies to monitor beneficially, particularly in the medical context:

> “*Researchers have made stretchable, ultrathin electronics that cling to skin like a temporary tattoo and can measure electrical activity from the body. These electronic tattoos could allow doctors to diagnose and monitor conditions like heart arrhythmia or sleep disorders noninvasively*” (BBC 2011d; Vezina 2011).

However, there also are artificial intelligence techniques where a CCTV camera locks onto a person and their behaviours can be assessed through evaluating aspects such as motion, temperature and body language, and cameras can connect to follow the person (BBC 2011j). Fingerprint can be analysed not only to identify a person, but also can "*show if a criminal suspect has taken drugs or been in contact with explosives*" (BBC 2011e). There has even been research to differentiate fingerprint recognition between live or dead tissue, since there have been cases of fingers being cut off hostages where security systems are dependent on fingerprint recognition (Marks 2011).

As in the past these smart technologies, developed more for the security industry, will eventually find applications in businesses and organisations. For example in Iraq a version of national Big Brother is being trialled:

> "D*ata have been gathered on roughly 2.2 million Iraqis, or one in every 14 citizens — and the equivalent of one in four males of fighting age. To get the information, soldiers and police officers take digital scans of eyes, photographs of the face, and fingerprints. In Iraq and Afghanistan, all detainees and prisoners must submit to such scrutiny. But so do local residents who apply for a government job, in particular those with the security forces and the police and at American installations. A citizen in Afghanistan or Iraq would almost have to spend every minute in a home village and never seek government services to avoid ever crossing paths with a biometric system*" (Shanker 2011).

EPOS surveillance is now more fully integrated across tills, cameras, and financial audit trails which check back on refunds or cancelled purchases (TILLS4CHANGE 2011). However, such smart functions can still be undertaken with combinations of surveillance technologies and 'workplace infiltration' by agents who are engaged as employees within the organisation (INTIMES 2011; JUNO 2011).

In 2011 voice-recognition in retail distribution centres used rather basic vocabularies, whereas now there is wider ability for systems to recognise 'natural language', accents, and multiple languages (VOCOLLECT 2011). Combined with the real-time monitoring of computer access and usage by employees – "*track any user's keystrokes on your screen in real time mode. Passwords, email, chat conversation - you have the full picture*" (SOFTACTIVITY 2011). Other applications can record in detail the surfing habits of employees, alerting if they send emails with attached files, check their usage levels to see if they are downloading music etc., or identifying if they access confidential company files (SNAPGUARD 2011).

The monitoring of employees therefore extends beyond the organisational boundaries into private life, largely because employees are now presumed increasingly to be blurring the boundaries between private and public in their use of information communication technologies, and the surveillance needs to be real-time. For example "Social Intelligence℠ Monitoring" will check for critical comments made about colleagues and managers, unacceptable material being accessed or passed on, or "*Associating with questionable Internet groups or Web pages … Regularly updating personal sites while on the clock ("cyber slacking")*". The monitoring activity is linked also to "Social Intelligence℠ Hiring" to check the activities of potential employees (Derene 2009; SOCIALINTELLIGENCE 2011).

Forthcoming developments to smart-phones will allow companies to issue phones that track location to ever finer resolution, and tiny gyroscope sensors will be able to detect position and elevation within buildings – something that currently requires access control mechanisms using devices such as smartcards – the mobile phone therefore eats up yet another device (Bilton 2011). On a wider scale such technologies are components in the emergence of 'real-time cities' where "*The increasing deployment of sensors and hand-held electronics in recent years is allowing a new approach to the study of the built environment*" (MIT 2010).

Stephen Graham writes of the results of pervasive surveillance being 'Cities under Siege' and "*the spread of political violence through the sites, spaces, infrastructure and symbols of the world's rapidly expanding metropolitan areas*" (Stephen Graham 2010). It was in the built environment of UK cities in the summer of 2011, where the 'Blackberry riots', involved rapid communication using social networks and mobile phones. That led to some calls for Government to have the ability to cut-off the phone networks in a time of emergency

(ECONOMIST 2011c; Fleming 2011). As ever, the unexpected use of the technologies leads to potential legislative function creep.

Function creep also occurs when organisations go beyond what is normally acceptable as surveillance. For example:

> "*Hammersmith and Fulham checked on their employees claiming sick time, while Darlington made sure employees were following parking regulations. Great Yarmouth Council used RIPA powers to check up on someone suspected of illegal tattoing*" (eGovmonitor 2010)

Lastly, function creep has been starkly evident in the News International phone-hacking scandal of 2010, and it is not regarded as being just limited to that organisation: "*The information commissioner says the trade in personal data extends far beyond tabloid journalism. Dealers will supply anyone who pays*" (Christopher Graham 2011).

MORE AUTOMATION, LESS EXPLOITATION, MORE DILEMMAS?

The 2005 report noted moves towards full automation in some areas of employment, such as warehouse distribution centres. On one hand this removed the risks of employee exploitation where they were required to wear surveillance devices while they worked – after all robots do not complain. Whether the employees who were not needed have other job opportunities to move to is another issue altogether, and it is one which affects directly members of the Union. Developments continue however, such as:

> "*Intelligrated® … complete material handling automation solutions, including conveyor systems, IntelliSort® sortation systems, Alvey® palletizers and robotics, Real Time Solutions® order fulfillment systems, warehouse control software and advanced machine controls*" (Intelligrated 2011).

After protests about alleged worker exploitation in Chinese factories by Foxcomm the company reacted by announcing an acceleration of plans to replace workers by robots, and "*The company plans to have 300,000 robots by next year, Chairman Terry Gou was quoted as saying by local media*"(BBC 2011f; Hille 2011). So, no exploited workers at all, but it would be too easy to then say 'no workers at all' and risk a luddite reaction.

Within Europe the privacy and surveillance and ethics dilemmas continue to challenge legislators. The European Commission has developed "*The RFID Privacy Impact Assessment (PIA) Framework {which} sets an example for industry in Europe and in the world by taking legitimate privacy concerns of people seriously and proactively addressing them*" (EUROPE 2011b; Kroes 2011). The Commission also has proposed the development of a single electronic tachograph, linked to global positioning satellites, which they claim balances both business and employee needs by saving on administrative costs and protects drivers from (EUROPE 2011c). In 2011 the EU also is promoting a "*new legal right to be forgotten -- it says this is one of "four pillars" to strengthen citizens' rights over their own data*" (Mayes 2011). However, the downside of such a right could be to exclude oneself from the information networks that in part enable rapid physical and financial mobility.

So, it is seldom a simple win-win or lose-lose situation when surveillance technologies are concerned. Surveillance can be seen as a form of listening to customers through sophisticated databases and analysis (Manzerolle and Smeltzer 2011), a process seen as marketing-cum-surveillance" (Palmås 2011). The more information we produce the more organisations rely on automated analysis of the data and "*the machines themselves will increasingly make the decisions, … and smart technology will ultimately lead to greater inequality*" through concentrating information power in 'information priests' and through increasing technological productivity at the expense of human employees when "*We are likely to see more jobless recoveries*" (ECONOMIST 2010). Complex analytical techniques (algorithms) will empower the automated monitoring and analysis systems (Amoore 2009).

There consequently is a risk that mathematical algorithms can demonise activities such as gossiping (wasting time), or surfing for personal purchases online (stealing organisational time). The realities of time, activity, and productivity vary profoundly across organisations and employment sectors. A study of office workers by MIT and New York University:

> "*discovered that those employees who had in-person conversations with co-workers throughout the day also tended to be more productive … employees at an IT company who completed tasks within a tight-knit group that communicated face to face were about 30 percent more productive than those who did not communicate in a face-to-face network*" (Greene 2009).

There is therefore a powerful link with information communication and productivity, and people and networks matter, especially where complex problems need solving. Simon Reilly researched the role of middle managers are responsible for 'managing' staff through performance monitoring and related surveillance practices. He called them:

> "*Performance Intermediary Executives or PIE, where 'performance is everything'. Instead of managing people, some of these PIE men and women are increasingly managing processes by diktat, preferring power typologies of obedience and domination over that of reciprocity*". (Reilly 2010).

His research leads to the final rueful observation by the Economist:

> *"Although workforce-monitoring software may provide what seems like useful information, it is no help when it comes to addressing the problems it uncovers. It may also undermine morale and mutual trust. Mr Cheese warns: 'If you have to check up on employees all the time, then you probably have bigger issues than just productivity'."(ECONOMIST 2009)*

Human agency and collaborative behaviours therefore remain powerful mechanisms to achieve both productivity and an effective workforce in the modern information society. However, the recent developments in social networking, in the blurring of boundaries between private and employment/public can threaten employer/employee relations as much as the sophisticated and pervasive surveillance of employees by employers.

Ben Willmott of the Chartered Institute of Personnel and Development argued "*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 continuing to decline, and their sophistication and functionality increasing, 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.

5. THE 2005 CONTEXT: SURVEILLANCE IN THE RETAIL SECTOR

The 2005 briefing looked 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 concluded, 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.

Routine surveillance in a retail situation was promoted as a form of employee protection – whether it realistically protects employees, or at least helps in the detection of criminal activity:

- "*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 produced 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 guard*[9]*, 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 was 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 ''smart'

[9] http://captology.stanford.edu/Examples/hygieneguard.html

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. Smart homes are high on some political agendas, for example to ensure that all homes are linked to electronic services, or that they are designed and function to meet the needs of certain groups, such as the elderly (EUROPE 2010; Simmons 2006).

It is one thing to know that you are being monitored, and another if it is covert, so should we know whether we are being watched? 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 were 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 monitor the behaviour of customers. Theft from stores was 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 key workers in mobile healthcare, or 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. This was covered in a separate 2005 report for GMB regarding regional distribution centres. Some of the retail companies report ‘reductions in staff training’ times, for example Bentwood, a large supplier of clothing to Marks and Spencer Plc, noted that “*new warehouse operatives can be trained to use basic scanner functions within an hour*” (Anon 2005b). 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 had been one mechanism to reduce employee levels, but at the same time offer customers the ability to self-check-out and to actually preserve privacy. For example, if you are embarrassed about purchasing contraceptives, sex toys or haemorrhoid cream at the supermarket you no longer have to suffer the indignity of a check-out operator ‘knowing’ what you are purchasing.

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 in reduced. A logical end-point will be the full automation of warehouses and distribution centres, with robotic[10] machines doing the work. This process is clearly similar to the automation of car manufacturing. Such fears were 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.

For example NGK Spark Plugs (UK) Ltd used such as system where "*picking requirements are automatically routed to individual pickers within the warehouse, based on their suitability and availability*" (Indigo 2005). 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 obtains 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).

6. THE 2005 'WORKPLACE WATCH' - AREAS OF EMPLOYEE SURVEILLANCE

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

CHECK-OUT STAFF

CCTV systems were the most familiar, but they were 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 was 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 management as consumer activity can be observed, recorded and measured leading to better staff planning and store layout*" (Axis 2005; Xpert 2005).

Checkout tills provided 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 tags*[11]*. Integration with EPOS systems will inhibit internal shrinkage by the removal of 'sweet hearting'*" (Microlise 2005).

[10] Indeed, the automated home is closer, Google Android "devices—dubbed "Tungstens"—act as an intermediary between an Android phone or tablet and a suitably enabled home appliance. They would allow users to remotely control everything from lighting to refrigerators" Simonite, S. (2011).

[11] 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). However, shoplifters use devices such as foil-lined

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). One 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 had 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 AND LOGISTICS

The justification for pervasive monitoring technologies in warehouses was based on historic inefficiencies in paper-based systems where warehouse workers spent time searching for the location of goods (Ballard 1998). Voice-picking and wearable computers were the main trends, the motivators were increased productivity by speeding up picking and making it more accurate (AstuteDiligence 2005; Piasecki 2001), reduced staff training overheads (Voicepicking 2005) of up to 50% (McCoy 2005), constant staff utilisation through "*Individual Accountability* "(Rangegate 2005) where "*staff know in real time how they are performing as they go through their shift or on a cumulative basis*" (Jack 2005), and greater profits because "*employees are now able to focus more on building the business rather than just on manual tasks*" (Microsoft 2003).

This group of approaches was given the new euphemism of "*warehouse management disciplines*" (Exel 2005), and these were being implemented in many sectors, for both the US Department of Defense and Wal-Mart were mandating their suppliers to use RFID technology "*to track products without human interaction, resulting in fewer misplaced shipments and the ability to restock shelves as soon as a product runs out*" (Foley 2005).

The promise of the technology was 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).

In the distribution process, on-board computers that are linked to GPS tracking monitor "*route, fuel and engine diagnostics are also combined in these units, which ultimately leads to more efficient use of the vehicle*". (Stobart 2005).

shopping bags to make the tags invisible, and so the technology must innovate to overcome the innovations of the criminals Anon. (2005a).

Productivity increases were 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 2005c).

The implications for employee surveillance were 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, and of efficiency gains, through ubiquitous surveillance. Sometimes the surveillance is used as a justification for training needs identification, such as the Eddie Stobart distribution depot for Tesco, where the technology:

> "*enables us to monitor labour efficiency with a high degree of accuracy, ensuring that resources are directed appropriately throughout the warehouse, and any need for further staff training and support is immediately highlighted*." (Anon 2003)

Ubisense was working on "*precise tracking of warehouse workers in an indoor environment*", arguing that there is a need for "*continuous evaluation of the worker's assistance needs in order to provide the most suitable, proactive and personalised support in a dynamic working context*" (UBISENSE 2005).

More research was needed to identify whether this generally leads to individual training and development packages for workers, or perhaps the more general outcome is the low performing workers lose their jobs. For example, check-out surveillance, however, could go beyond monitoring 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.

CALL CENTRES

Some of the most pervasive surveillance was carried out in Call Centres. Their very technological infrastructure, comprising sophisticated communications technologies and advanced software systems (Anon 2005e; MiTech 2005; Opera 2005), provide an ideal environment for the micro-monitoring of employees. The New York Times (Dhillon 2005) had 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 noted 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.

Nevertheless, Dhillon clearly differentiated 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 cited 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.

Furthermore, it is curious that the main UK customer reaction about off-shoring call centres was less a desire to protect jobs, and more a desire to speak to a native English-speaker, and some companies now loudly trumpet their guarantee that you will speak to a person in a UK call centre(Winterman 2007). So that's ok then – as long as it is not a foreigner and we are not really worried about the employment conditions of the person we are speaking to.

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 phone 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 built 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 targets. While these case studies indicate the levels of workplace stress in call centres, other research indicates that they are not necessarily markedly more stressful places to work than others. Dr David Holman, research fellow at Sheffield University's Institute of Work Psychology, concluded in 2000 that:

> "*staff working in the call centre with least control over their jobs reported the highest stress and lowest job satisfaction*" (Moore 2005)

> and "*the issue is not the technology per se, but rather the way the technology has been deployed and manipulated by firms to increase workloads and speed-up work practices*" (van den Broek 2002).

PERFORMANCE MANAGEMENT, IMPACTS AND ETHICS

Furthermore, Trevor Wood, director of the HRD Group, a Nottingham-based HR consultancy was quoted as stating that:

> "*Poor culture can arise from autocratic leadership; lack of effective communication; low decision-making participation; inadequate developmental systems or the opportunity to apply new skills; unrealistic and imposed target-setting; mechanical and therefore meaningless performance appraisals; and vision and value statements as customer window-dressing rather than to guide the organisation in the achievement of its goals*". (Nash 2005)

Researchers as Stanford University write about pervasive technology also being persuasive technology[12]. 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, warned 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).

Other functions in call centre management involved 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 could, it was 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 been 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 surveille 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*

[12] http://captology.stanford.edu/

> *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.

The 2005 context showed clearly that 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. Consent and audit had 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).

People with 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) had 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)

7. YOUR ELECTRONIC FOOTPRINT CONTINUES TO EXPAND

In 2005 the major concern was the surveillance assemblage that confronted employees, and which "*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 a review of his 'Dataveillance' theory 15 years on in 2003, Roger Clarke was also 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*” (Roger Clarke 2003)

The rich supply of surveillance technologies are seen in large developments such as the ‘Great Firewall of China’, and show how governments can try to build strong surveilled borders around freedoms in cyberspace (Anon 2010; BBC 2011b; Michael Bristow 2010; Lemos 2011). 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 inevitable 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).

So, in the end, the 2011 situation is much more complex than 2005, and it requires careful consideration of practices and ethics from all the workplace stakeholders, for example the advice published by GMB (Magazine, October 2011) about “*Networking or Not Working: How and when to use Facebook and other social media at work*”:

GMB’s dos and don’ts of social networking

Do:

- Think carefully before posting anything online.
- Have a clear understanding of what comments about your work will be tolerated by your employer.
- Take time to understand the privacy policies and controls for any social networking or blogging site that you use.
- Use access controls to limit who can see your information – and don’t forget who you have granted most detailed access!
- Use a separate email address to register with networking and blogging sites – preferably one that does not include your name.
- Check your privacy settings often. Think about who you allow as friends, and remember who they are.
- Consider that some people may not be who they say they are.
- Report users who violate the terms of use for the sites you are on.
- Be aware of your employer’s policy on the use of electronic communications. You might not be allowed to use sites like Facebook in work hours.
- Clearly state in your bio that all views are your own personal opinions and not those of your employer.

Don’t

- Publish your email address, telephone number or home address.
- Choose an email address that reveals private information about you.
- Make public other identifying information, such as your date of birth.

In an interconnected world, where our broadband access allows instant transmission of large amounts of information, employers will be ever more reluctant to react after an event and will want to avoid the event. And it should be the same with employees who indulge in social networking and other electronic communication tools, because one of the defences you give up is ‘plausible deniability’. It something you said was in a conversation to a friend it is more easy to deny it than if it was typed as an email – once you put it into text it's almost impossible to deny or recall it. The Social Spy may be watching, so 'be very careful out there'.

8. SOURCES

A personal note about the sources

It is quite likely that some of the older references from the 2005 report are no longer accessible at the URLs. That's in part the chaotic nature of the Web, and owners of a site can re-structure it, sites can cease to be used, and businesses can change name or go out of business. As the 'cited' date indicates, these were the dates that I accessed the material and structured it in my electronic bibliography, so it's not my fault if you cannot access a link, although I'm sure you will blame me. I can only think back to the start of my career when everything was on paper, reference details were on '5 by 3' cards, and the average academic risked a hernia every time they walked back from the Library with a pile of books. Now I have the luxury of an integrated bibliography with over 33,000 structured references and documents on my computer, backed up of course at my mother's house, with one of our sons, and buried in secret at a remote location. I'm not completely scared about my computer stopping working, honestly, I'm just paranoid. But, what a joy it is to work in the Information Society with access to all this information in an integrated fashion, but please will everyone stop watching me all the time ….

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

ADT. (2011). *Employee and Customer Theft* ADT plc, [cited July 25 2011]. http://www.adt.co.uk/retail/retail-customer-and-employee-theft-risks

Agger, M. (2007). *Google Spy: Zooming in on neighbors, nose-pickers, and sunbathers with Street View* (June 8) Slate Magazine, [cited June 25 2007]. http://www.slate.com/id/2168127/fr/flyout

Amoore, L. (2009). Algorithmic War: Everyday Geographies of the War on Terror. *Antipode* 41 (1): pp. 49-69.

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

Anon. (2003). *Keeping track at Eddie Stobart* (Feb/Mar) Mlogmag.com, [cited September 9 2005]. http://www.mlogmag.com/magazine/04/stobart.shtml

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). *Garment Distribution - Maintaining A Competitive Edge. Bentwood Show How its Done* XeBusiness Ltd, [cited September 8 2005]. http://www.xebusiness.com/case%20studies/bentwood%20wms%20case%20study.html

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

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

Anon. (2010). *China seeks to reduce Internet users' anonymity* (July 13) Globe and Mail (Toronto), [cited July 13 2010]. http://www.theglobeandmail.com/news/technology/china-seeks-to-reduce-internet-users-anonymity/article1638127/

Anon. (2011a). *Central London Congestion Charging, United Kingdom* Net Resources International, [cited July 25 2011]. http://www.roadtraffic-technology.com/projects/congestion/

Anon. (2011b). *The Most Effective Retail Employee Theft Reduction Strategies* The Profit Experts, [cited July 25 2011]. http://theprofitexperts.co.uk/the-most-effective-retail-employee-theft-reduction-strategies/

Anon. (2011c). *The scourge of Till Fraud - It happens more than you think* Successful Security, [cited July 25 2011]. http://www.successfulsecurity.com/typesoffraud/index.htm

AstuteDiligence. (2005). *Logistics* Gaebler Ventures, [cited September 8 2005]. http://www.astutediligence.com/Diligence_Deliverables_Logistics.htm

AWOSOFT. (2011). *Imonitor Employee Activity Monitor* Awosoft Software and Design Inc., [cited July 23 2011]. http://www.pc-remote-monitoring.com/

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.com, [cited March 20 2004]. http://www.wired.com/news/medtech/0,1286,62723,00.html

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

Ballard, R. (1998). *Managing Warehouse Processes to Ensure Accuracy and Control* (13-15 October) Supply Chain Efficiency Seminars, [cited October 7 2005]. http://www.logistics.co.uk/db_pdf/suppcheffpaper_31.pdf

BALTIC. (2003). *Eva Grubinger, Visualisation of the installation Dark Matter* (Noember) 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.com, [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

BBC. (2008). *Google accused on privacy views* (August 1) BBC, [cited August 1 2008]. http://news.bbc.co.uk/1/hi/technology/7536549.stm

BBC. (2009). *Google pulls some street images* (March 20) BBC, [cited March 23 2009]. http://news.bbc.co.uk/1/hi/technology/7954596.stm

BBC. (2011a). *CCTV website rapped on privacy* BBC, [cited June 14 2011]. http://www.bbc.co.uk/news/technology-13765136

BBC. (2011b). *China: 1.3 million websites shut in 2010* BBC, [cited July 14 2011]. http://www.bbc.co.uk/news/world-asia-pacific-14138267

BBC. (2011c). *Egypt severs internet connection amid growing unrest* BBC, [cited January 28 2011]. http://www.bbc.co.uk/news/technology-12306041

BBC. (2011d). *Electronic tattoo 'could revolutionise patient monitoring'* BBC, [cited August 12 2011]. http://www.bbc.co.uk/news/health-14489208

BBC. (2011e). *Fingerprint breakthrough offers new forensic evidence* BBC, [cited August 6 2011]. http://www.bbc.co.uk/news/technology-14386520

BBC. (2011f). *Foxconn to boost use of robot machines in manufacturing* BBC, [cited August 2 2011]. http://www.bbc.co.uk/news/business-14368244

BBC. (2011g). *Hacktivists target Egypt and Yemen regimes* BBC, [cited February 5 2011]. http://www.bbc.co.uk/news/technology-12364654

BBC. (2011h). *Online defamation cases in England and Wales 'double'* BBC, [cited August 26 2011]. http://www.bbc.co.uk/news/uk-14684620

BBC. (2011i). *Secret agents raid Apple store webcam 'artist'* BBC, [cited July 8 2011]. http://www.bbc.co.uk/news/technology-14080438

BBC. (2011j). *'Smart' CCTV could track rioters* BBC, [cited August 23 2011]. http://www.bbc.co.uk/news/technology-14629058

BBC. (2011k). *Sudan to unleash cyber jihadists* BBC, [cited March 23 2011]. http://www.bbc.co.uk/news/technology-12829808

BBC. (2011l). *Twitter and web video site face clampdown in Egypt* BBC, [cited January 26 2011]. http://www.bbc.co.uk/news/technology-12284649

BBC. (2011m). *US Pentagon to treat cyber-attacks as 'acts of war'* BBC, [cited June 1 2011]. http://www.bbc.co.uk/news/world-us-canada-13614125

Beales, T. (2005). *Voice Directed Picking: Expected ROI* Business Computer Projects Ltd [cited August 28 2005]. http://www.bcpsoftware.com/solutions/voice/whitepaper.php

Benedict XVI, P. (2011). *Truth, Proclamation and Authenticity of Life in the Digital Age* The Vatican, [cited January 24 2011]. http://www.vatican.va/holy_father/benedict_xvi/messages/communications/documents/hf_ben-xvi_mes_20110124_45th-world-communications-day_en.html

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

Bilton, N. (2011). *The Sensors Are Coming!* New York Times, [cited May 20 2011]. http://bits.blogs.nytimes.com/2011/05/19/the-sensors-are-coming/?ref=technology

Bird, J. (2011). *Social media: The worst thing is to ignore your customers* Financial Times (London), [cited March 16 2011]. http://www.ft.com/cms/s/0/18a1af06-4eb0-11e0-874e-00144feab49a,dwp_uuid=99d34b5a-4eb2-11e0-874e-00144feab49a.html#axzz1Go1o6EZD

Blake, M. (2011). *A new social network – communities use CCTV to crack crime* Independent (London), [cited July 30 2011]. http://www.independent.co.uk/news/uk/crime/a-new-social-network-ndash-communities-use-cctv-to-crack-crime-2328655.html

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

Bourzac, K. (2011). *Attending to Digital Etiquette* Technology Review, [cited August 29 2011]. http://www.technologyreview.com/business/38184/

Bradshaw, T., and P. Clark. (2011). *BA bitten in web protest over bed bugs* Financial Times (London), [cited February 25 2011]. http://www.ft.com/cms/s/0/acbaa5f0-402b-11e0-811f-00144feabdc0.html#axzz1EybtaWiH

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.

Bristow, M. (2010). *China defends internet censorship* (June 8) BBC, [cited June 8 2010]. http://news.bbc.co.uk/2/hi/americas/8727647.stm

BRULINES. (2011). *Brulines Group Investors Info* Brulines Ltd, [cited July 23 2011]. http://www.brulines.com/group/

Bustillo, M. (2010). *Wal-Mart Radio Tags to Track Clothing* (July 23) Wall Street Journal, [cited July 24 2010]. http://finance.yahoo.com/family-home/article/110152/wal-mart-radio-tags-to-t

Carrico, D. (2005). *Technoprogressivism: Beyond Technophilia and Technophobia* (June 30) Ieet.org, [cited August 26 2005]. http://ieet.org/writings/Carrico20050630.htm

CATAPHORA. (2011). *People can outsmart the rules. So can we.* Cataphora.com, [cited August 30 2011]. http://www.cataphora.com/

Church, G. J. (1987). The art of high-tech snooping. *Time*, pp. 13-15.

Clarke, R. (1994). Dataveillance by Governments: The Technique of Computer Matching. *Information Technology & People* 7 (2): pp. 46-85.

Clarke, R. (2003). *Dataveillance - 15 Years On* (March 31) Xamax Consultancy Pty Ltd, [cited August 18 2005]. http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html

CM. (2005). *Employee Monitoring* Computer Monitoring, [cited August 24 2005]. http://www.computer-monitoring.com/employee-monitoring.htm

Cohen, N. (2011). *It's Tracking Your Every Move and You May Not Even Know* New York Times, [cited March 28 2011]. http://www.nytimes.com/2011/03/26/business/media/26privacy.html

COMMONS. (2011). *Information Commissioner's Annual Report to the House of Commons* House of Commons, Home Affairs Committee, [cited March 6 2011]. http://www.publications.parliament.uk/pa/cm201011/cmselect/cmhaff/702/70202.htm

CONGRESS. (2004). *The 9/11 Commission Report*. Washington DC: US Congress. July, Report, xviii+567 p.

Cooke, M. (2011). *Tube and train commuters caught on camera* BBC, [cited August 25 2011]. http://www.bbc.co.uk/news/technology-14650757

CRR. (2004). *Staff theft and......Fighting Retail Crime* Centre for Retail Research, [cited August 2005]. http://www.chant4.co.uk/retailresearch2003/crime_and_fraud/employee_theft.php

Dearne, K. (2004). *Blocker tag protection from RFID* (April 6) Australian IT, [cited April 8 2004]. http://australianit.news.com.au/articles/0,7204,9197418%5E15321%5E%5Enbv%5E15306,00.html

Delio, M. (2004). *Hacktivism and How It Got Here* (July 14) Wired.com, [cited July 18 2004]. http://www.wired.com/news/infostructure/0,1377,64193,00.html

Dembosky, A. (2011). *Invasion of the body hackers* Financial Times (London), [cited June 12 2011]. http://www.ft.com/cms/s/2/3ccb11a0-923b-11e0-9e00-00144feab49a.html

Derene, G. (2009). *Is Your Boss Spying on You? Inside New Workplace Surveillance* Popular Mechanics, [cited July 25 2011]. http://www.popularmechanics.com/technology/gadgets/news/4223564

Dhillon, A. (2005). *"Big Brother' keeps eye on call centers* (August 25) New York Times, [cited August 27 2005]. http://www.dailybulletin.com/Stories/0,1413,203~21482~3026950,00.html

DMicros. (2005). *DM Solutions for the Retail Sector* Dedicated Micros, [cited August 18 2005]. http://www.dedicatedmicros.com/uk/application_details.php?application_id=1

Dodge, M., and R. Kitchin. (2005). *The ethics of forgetting in an age of pervasive computing*. London: Centre for Advanced Spatial Analysis, University College London. March, Report Paper 92, 24 p.

EAHC. (2011). *Chain of Trust Project* Executive Agency for Health and Consumers, [cited July 7 2011]. http://www.chainoftrust.eu/

ECONOMIST. (2004). *Move over, Big Brother* (December 2) Economist, [cited December 3 2004]. http://www.economist.com/science/tq/displayStory.cfm?story_id=3422918

ECONOMIST. (2009). *Big Brother bosses* (September 10) Economist, [cited September 17 2009]. http://www.economist.com/businessfinance/displaystory.cfm?story_id=14413380

ECONOMIST. (2010). *Horror worlds: Concerns about smart systems are justified and must be dealt with* Economist, [cited November 8 2010]. http://www.economist.com/node/17388328?story_id=17388328

ECONOMIST. (2011a). *The Leaky Corporation* Economist, [cited February 24 2011]. http://www.economist.com/node/18226961?story_id=18226961

ECONOMIST. (2011b). *The people formerly known as the audience* Economist, [cited July 7 2011]. http://www.economist.com/node/18904124?story_id=18904124&CFID=167016031&CFTOKEN=24031595

ECONOMIST. (2011c). *Technology and disorder: The BlackBerry riots* Economist, [cited August 11 2011]. http://www.economist.com/node/21525976

eGovmonitor. (2010). *Local Councils Abuse RIPA To Snoop on More Than 8500 Targets Including Own Staff* (May 25) Egovmonitor.com, [cited May 25 2010]. http://www.egovmonitor.com/node/36609

ELTIMA. (2005). *Powered Keylogger 1.35* Eltima Software GmbH, [cited August 24 2005]. http://www.eltima.com/products/powered-keylogger/

ESCO. (2011). *POS and ePOS Systems* Esco.co.uk, [cited July 25 2011]. http://www.ecso.co.uk/pos/index.htm

EUPARL. (2011). *SWIFT implementation report: MEPs raise serious data protection concerns* European Parliament, [cited March 16 2011]. http://www.europarl.europa.eu/en/pressroom/content/20110314IPR15463/html/SWIFT-implementation-report-MEPs-raise-serious-data-protection-concerns

EUROPE. (2010). *Digital Agenda: review shows strong SME interest and government backing for ICT to assist the elderly* European Commission, [cited December 16 2010].

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1726&format=HTML&aged=0&language=EN&guiLanguage=en

EUROPE. (2011a). *Data protection: EU and United States move closer to agreement* European Union, [cited April 16 2011]. http://www.eu2011.hu/news/data-protection-eu-and-united-states-move-closer-agreement

EUROPE. (2011b). *Digital Agenda: new guidelines to address privacy concerns over use of smart tags* European Commission, [cited April 6 2011]. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/418&format=HTML&aged=0&language=EN&guiLanguage=en

EUROPE. (2011c). *Road transport: new tachograph rules will save companies more than €500 million per year* European Commission, [cited July 19 2011]. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/903&format=HTML&aged=0&language=EN&guiLanguage=en

Exel. (2005). *Store logistics* Exel Logistics, [cited September 7 2005]. http://www.exel.com/exel/home/solutions/sectorsolutions/retail/storelogistics/

Eyespymp. (2010). *Hey there! eyespymp is using Twitter* (February 1) Eyespymp, [cited February 1 2010]. http://twitter.com/eyespymp

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

FLB. (2011). *First Location Bank* First Location Bank, [cited August 23 2011]. http://metapos.positium.ee/

Fleming, N. (2011). *Why Rioters Won't Be Protected by BlackBerry Messaging System* Technology Review, [cited August 11 2011]. http://www.technologyreview.com/communications/38297/

Foley, R. J. (2005). *Debate rages over radio-chip tracking* (September 5) Associated Press, [cited September 8 2005]. http://www.stltoday.com/stltoday/business/stories.nsf/technology/story/34C21B68571A0A91862570710032D8ED?OpenDocument

FORBES. (2011). *How Embarrassing/Job-Threatening Facebook Photos Are Part Of Your Job Application* Forbes Global, [cited July 23 2011]. http://blogs.forbes.com/kashmirhill/2011/06/20/now-your-embarrassingjob-threatening-facebook-photos-will-haunt-you-for-seven-years/

Ford, M. (1998). *Surveillance and privacy at work*. London: Institute of Employment Rights.

FSB. (2011). *Crime Against Business* Federation of Small Businesses, [cited July 25 2011]. http://www.fsb.org.uk/policy/businesscrime

FT. (2011). *The Connected Business* Financial Times (London), [cited January 25 2011]. http://www.ft.com/reports/connected-business-jan2011#

Gelles, D. (2011). *Social media: The personal at work can be a disruptive mix* Financial Times (London), [cited April 20 2011]. http://www.ft.com/cms/s/0/1ad329f2-68a1-11e0-81c3-00144feab49a,dwp_uuid=0aa251dc-68a8-11e0-81c3-00144feab49a.html#axzz1K6IW8Pvp

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

Goode, E. (2011). *Police Lesson: Social Network Tools Have Two Edges* New York Times, [cited April 7 2011]. http://www.nytimes.com/2011/04/07/us/07police.html

Graham-Rowe, D. (2011). *A New Direction for Digital Compasses* Technology Review, [cited July 14 2011]. http://www.technologyreview.com/computing/38034/

Graham, C. (2011). *They're all at it* Prospect Magazine, [cited August 20 2011]. http://www.prospectmagazine.co.uk/2011/07/illegal-trade-personal-data-tabloid-journalism/

Graham, S. (2010). *Cities Under Siege: The New Military Urbanism*. London: Verso.

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.

Greene, K. (2009). *Wearable Sensors Watch Workers* (May 13) Technology Review, [cited May 17 2009]. http://www.technologyreview.com/communications/22642/

Greene, K. (2011). *Finding Office Buck-Passers, Heroes, and Shirkers* Technology Review, [cited August 25 2011]. http://www.technologyreview.com/business/38187/

Groeger, L. (2011). *Spies Want to Mine Your Tweets for Signs of the Next Tsunami* Wired.com, [cited July 7 2011]. http://www.wired.com/dangerroom/2011/07/spies-tweets-tsunami/

Haggerty, K. D., and R. V. Ericson. (2000). The surveillant assemblage. *British Journal of Sociology* 51 (4): pp. 605–622.

Hammond, E. (2011). *Risk mitigation: There is no substitute for local staff or knowledge* Financial Times (London), [cited January 25 2011]. http://www.ft.com/cms/s/0/6fbb69cc-274a-11e0-80d7-00144feab49a,dwp_uuid=5b05aa68-274c-11e0-80d7-00144feab49a,s01=1.html#axzz1C4NNHhGN

Havery, B. (2005). *RFID: There you are!* (September 6) Technology & Business Magazine, [cited September 8 2005]. http://www.zdnet.com.au/news/hardware/soa/RFID_There_you_are_/0,2000061702,39210050,00.htm

Hill, K. (2011). *Feds Okay Start-up That Monitors Employees' Internet and Social Media Footprints* Forbes Global, [cited July 23 2011]. http://blogs.forbes.com/kashmirhill/2011/06/15/start-up-that-monitors-employees-internet-and-social-media-footprints-gets-gov-approval/

Hille, K. (2011). *Foxconn looks to a robotic future* Financial Times (London), [cited August 2 2011]. http://www.ft.com/cms/s/2/e5d9866e-bc25-11e0-80e0-00144feabdc0.html#axzz1Tr3n2R00

Indigo. (2005). *Interactive Warehousing* Indigo.co.uk, [cited September 8 2005]. http://www.indigo.co.uk/solutions/addinfo.php?id=3&link=3

Intelligrated. (2011). *About Us* Intelligrated Inc., [cited July 25 2011]. http://www.intelligrated.com/

INTERMEC. (2005). *Retail* Intermec plc, [cited August 28 2005]. http://www.intermec.co.uk/

INTIMES. (2011). *Intimes Investigations* Intimes Investigations, [cited July 25 2011]. http://www.intimeinvestigations.com/company_infiltration.html

JABBAKAM. (2011). *What is Jabbakam?* Jabbakam.com, [cited July 30 2011]. http://www.jabbakam.com/

Jack, S. (2005). *Supply chain - Tools for better teamwork* (May 21) Drapers Record, [cited September 8 2005]. http://www.paconsulting.com/news/about_pa/2005/Supply_Chain_Tools_for_better_teamwork.htm

Johnson, B. T. (1995). *Technological Surveillance in the Workplace* Fairfield and Woods, P.C., [cited May 9 2000]. http://www.fwlaw.com/techsurv.html

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

JUNO. (2011). *Solutions* Juno Group, [cited July 24 2011]. http://www.juno-group.com/solutions.aspx

KABLE. (2005a). *Bichard reveals IT concerns* (March 15) Kable Government Computing, [cited March 16 2005]. http://www.kablenet.com/kd.nsf/Frontpage/D6A5EB09F9FED44580256FC5003D930F?OpenDocument

KABLE. (2005b). *ViSOR picks up non-offenders* (August 19) Kable Government Computing, [cited August 19 2005]. http://www.kablenet.com/kd.nsf/Frontpage/B25F5E35C4214672802570610049C63B?OpenDocument

KABLE. (2008). *GPs offered free patient access system* (July 9) Kable Government Computing, [cited July 12 2008]. http://www.kablenet.com/kd.nsf/Frontpage/A2782C28D2A67BBF80257480005578B5?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

Kirn, W. (2010). *Little Brother is Watching* New York Times, [cited October 18 2010]. http://www.nytimes.com/2010/10/17/magazine/17FOB-WWLN-t.html

Komp, C. (2005). *Electronic Tags Used to Track Immigrants* (September 6) The NewStandard, [cited September 8 2005]. http://www2.csoonline.com/blog_view.html?CID=11513

Kroes, N. (2010). *Bringing European values to the Internet of Things* (June 1) European Commission, [cited June 1 2010]. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/279&format=HTML&aged=0&language=EN&guiLanguage=en

Kroes, N. (2011). *Smart tags - working together to protect privacy* European Commission, [cited April 6 2011]. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/236&format=HTML&aged=0&language=EN&guiLanguage=en

Lace, S. (2004). *Radio frequency identification technology in retail* (February 5) National Consumer 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

Lardinois, F. (2010). *Social Sentry Lets Employers Track Their Workers Across the Internet* (Mach 24) New York Times, [cited March 24 2010]. http://www.nytimes.com/external/readwriteweb/2010/03/24/24readwriteweb-social-sentry-lets-employers-track-their-wo-19289.html

Lemos, R. (2011). *How China and Others Are Altering Web Traffic* Technology Review, [cited March 24 2011]. http://www.technologyreview.com/web/37074/

Lipowicz, A. (2011). *VA policy seeks to increase use of social media* Federal Computer Week, [cited August 17 2011]. http://fcw.com/articles/2011/08/16/va-issues-policy-encouraging-social-media-use.aspx

Manzerolle, V., and S. Smeltzer. (2011). *Consumer Databases, Neoliberalism, and the Commercial Mediation of Identity: A Medium Theory Analysis* Surveillance and Society, [cited June 14 2011]. http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/mediation

Marks, P. (2011). *Fingerprint scanner to spot the living dead* New Scientist, [cited August 22 2011]. http://www.newscientist.com/article/mg21128225.100-fingerprint-scanner-to-spot-the-living-dead.html

Marx, G. (2003). Some Information Age Techno-Fallacies. *Journal of Contingencies and Crisis Management* 11 (1): pp. 25-31.

Mayes, T. (2011). *Fight for privacy, not to be forgotten about* Wired.com, [cited July 25 2011]. http://www.wired.co.uk/magazine/archive/2011/08/ideas-bank/tessa-mayes

McCoy, G. (2005). *Warehouse automation* (July 8) Aftermarket Business, [cited September 7 2006]. http://www.aftermarketbusiness.com/aftermarketbusiness/article/articleDetail.jsp?id=169731

McGregor, R. (2011). *America after 9/11: A nation fixated with its security* Financial Times (London), [cited September 7 2011]. http://www.ft.com/cms/s/0/60886c9e-d892-11e0-8f0a-00144feabdc0.html#axzz1XH1Ilvbd

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

Menn, J. (2011). *Hacking group aims to expose state secrets* Financial Times (London), [cited June 21 2011]. http://www.ft.com/cms/s/0/f88061f4-9b8f-11e0-98f2-00144feabdc0.html#axzz1Pvci0htS

MEPRANKING. (2010). *MEP activity* MEPRanking.eu, [cited November 18 2010]. http://www.mepranking.eu/state.php

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

Microsoft. (2003). *Arthur Schuman, Inc. New Software Saves $15M and Achieves an ROI of 679 Percent; Payback Comes in 1.6 Months* Microsoft, [cited September 7 2005]. http://www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=14373

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

Mims, C. (2011). *Egypt Turns Off the Internet. Now What Happens?* Technology Review, [cited January 31 2011]. http://www.technologyreview.com/blog/mimssbits/26330/

MIT. (2010). *Senseable City Lab* Massachusetts Institute of Technology, [cited December 9 2010]. http://senseable.mit.edu/

MIT. (2011). *About AgeLab* Massachusetts Institute of Technology, [cited July 13 2011]. http://agelab.mit.edu/

MiTech. (2005). *Peripheral Applications* (August) MiTech plc, [cited August 22 2005]. http://www.mitech.co.uk/voice/content_peripheral_applications.htm

Moore, W. (2005). *Call Centres Under Pressure* (April) Channel 4 News, [cited September 8 2005]. http://www.channel4.com/health/microsites/0-9/4health/stress/saw_callcenter.html

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.

Naone, E. (2011). *Tracking Down Twitter's Best Rumor Spreaders* Technology Review, [cited June 8 2011]. http://www.technologyreview.com/web/37712/

Nash, H. (2005). *1-20 ways to motivate your staff (without paying them more)* Harvey Nash Research & Insight, [cited September 8 2005]. http://www.harveynash.com/pdf/2005/1-20waystomotivateyourstaff.pdf

NCR. (2005). *NCR Extends Reach of Checkout Software* NCR Corporation, [cited August 29 2005]. http://www.ncr.com/media_information/2005/feb/pr021005.htm

Newman, N. (2009). *The rise of social media and its impact on mainstream journalism* (September) Reuters Institute For The Study Of Journalism, [cited February 10 2010]. http://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/The_rise_of_social_media_and_its_impact_on_mainstream_journalism.pdf

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/

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

Palfrey, J. (2011). *Middle East Conflict and an Internet Tipping Point* Technology Review, [cited March 3 2011]. http://www.techreview.com/web/32437/

Palmås, K. (2011). *Predicting what you'll do tomorrow: Panspectric surveillance and the contemporary corporation* Surveillance and Society, [cited June 14 2011]. http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/panspectric

Parker, A. (2011). *Vodafone faces pressure over Egypt protests* Financial Times (London), [cited July 26 2011]. http://www.ft.com/cms/s/0/3316685a-b6d8-11e0-a8b8-00144feabdc0.html#axzz1TFItm9sv

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

Piasecki, D. (2001). *Order Picking: Methods and Equipment for Piece Pick, Case Pick, and Pallet Pick Operations* Inventory Operations Consulting L.L.C., [cited September 7 2005]. http://www.inventoryops.com/order_picking.htm

Preston, J. (2011). *Social Media History Becomes a New Job Hurdle* New York Times, [cited July 22 2011]. http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html

Preston, J., and B. Stelter. (2011). *Cellphones Become the World's Eyes and Ears on Protests* New York Times, [cited February 20 2011]. http://www.nytimes.com/2011/02/19/world/middleeast/19video.html

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

Pullella, P. (2011). *Pope warns of alienation risk in social networks* Reuters, [cited January 24 2011]. http://uk.reuters.com/article/idUKTRE70N24J20110124

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

Rangegate. (2005). *Rangegate Performance Management: FACT SHEET Visibility, compliance and execution for Warehouses & Stores* Rangegate Mobile Solutions plc, [cited September 8 2005]. http://www.rangegate.co.uk/Brochures/Rangegate%20Performance%20Management.pdf

Reilly, S. M. (2010). *The Use of Electronic Surveillance and Performance Measures in the Workplace: A Qualitative Investigation* University of Durham, [cited July 25 2011]. http://etheses.dur.ac.uk/429/1/Reilly_Thesis_2010_Hard_Copy.pdf

RetailFraud. (2005). *Retail loss prevention - Maximise profit by reducing losses* Retailfraud.co.uk, [cited August 18 2005]. http://www.retailfraud.co.uk/

RetailFraud. (2011). *Welcome to www.retailfraud.co.uk* Retailfraud.co.uk, [cited JUly 25 2011]. http://www.retailfraud.co.uk/Retail_Fraud_Prevention_Ltd/Homepage.html

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

Schmitt, E. (2011). *Governments Go Online in Fight Against Terrorism* New York Times, [cited January 31 2011]. http://www.nytimes.com/2011/01/31/world/middleeast/31terror.html

Scott, K. (2011). *Hacktivists versus governments: A war of attrition?* Wired.com, [cited June 14 2011]. http://www.wired.co.uk/news/archive/2011-06/14/governments-versus-hacktivists

Shanker, T. (2011). *To Track Militants, U.S. Has System That Never Forgets a Face* New York Times, [cited July 14 2011]. http://www.nytimes.com/2011/07/14/world/asia/14identity.html

Shiels, M. (2010). *Getty taps into Flickr snappers* (June 17) BBC, [cited June 20 2010]. http://news.bbc.co.uk/1/hi/technology/8744817.stm

Shury, J., M. Speed, D. Vivian, A. Kuechel, and S. Nicholas. (2005). *Crime against retail and manufacturing premises: Findings from the 2002 Commercial Victimisation Survey*. London: Home Office. July, Report, 113 p. http://www.crimereduction.gov.uk/business42.htm

Simmons, D. (2006). *Smart homes a reality in S Korea* (November 24) BBC, [cited November 26 2006]. http://news.bbc.co.uk/1/hi/programmes/click_online/6179868.stm

Simonite, S. (2011). *Google Wants to Control Your Home* Technology Review, [cited May 11 2011]. http://www.technologyreview.com/communications/37555/

Singer, E. (2011a). *Harvesting Business Ideas from Inside and Out* Technology Review, [cited February 23 2011]. http://www.technologyreview.com/business/32426/

Singer, E. (2011b). *Tackling the Dangers of Workplace Inactivity* Technology Review, [cited August 12 2011]. http://www.technologyreview.com/business/38178/

Singer, E. (2011c). *Two New Tools for Self-Tracking* Technology Review, [cited June 13 2011]. http://www.technologyreview.com/biomedicine/37721/?p1=A3

SNAPGUARD. (2011). *Spector 360 Overview* Snapguard.co.uk, [cited July 23 2011]. http://www.snapguard.co.uk/spector_360.html

SOCIALINTELLIGENCE. (2011). *About Social Intelligence Corp* Social Intelligence Corp, [cited July 23 2011]. http://www.socialintelligencehr.com/home

SOFTACTIVITY. (2011). *Employee Monitoring Software - Activity Monitor* Softactivity.com, [cited July 23 2011]. http://www.softactivity.com/em_l.asp

SPYSURE. (2011). *Employee Monitoring Software* Spysure.com, [cited July 23 2011]. http://www.spysure.com/index.php?main_page=page&id=31

Stelter, B. (2011). *Upending Anonymity, These Days the Web Unmasks Everyone* New York Times, [cited June 21 2011]. http://www.nytimes.com/2011/06/21/us/21anonymity.html

Stobart. (2005). *Warehousing* Eddie Stobart, [cited September 7 2005]. http://www.eddiestobart.co.uk/corporate/Page-warehousing.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

TILLS4CHANGE. (2011). *EPOS Software* Tills4Change.co.uk, [cited July 25 2011]. http://www.tills4change.co.uk/nebula.htm

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

UBISENSE. (2005). *Fraunhofer FIT brings the Ubisense technology to the attention of leading global software and communication companies* (July 1) Ubisense Ltd, [cited September 9 2005]. http://www.ubisense.net/news/PR%20pages/FIT%20PR%20July%2005.htm

van den Broek, D. (2002). *Surveillance* University of Sydney, [cited September 8 2005]. http://www.econ.usyd.edu.au/wos/worksite/surveillance.html

Vezina, K. (2011). *Stick-On Electronic Tattoos* Technology Review, [cited August 12 2011]. http://www.technologyreview.com/computing/38296/

VOCOLLECT. (2011). *Mobile Computing Devices* Intermec IP Corp, [cited July 25 2011]. http://www.vocollect.com/mobile-computing-devices

Voicepicking. (2005). *Frequently Asked Questions* Voicepicking.com, [cited August 24 2005]. http://www.voicepicking.com/

Wakefield, J. (2011). *TEDGlobal: Technology to crowd-source clean water* BBC, [cited July 14 2011]. http://www.bbc.co.uk/news/technology-14129592

Weber, T. (2010). *Why companies watch your every Facebook, YouTube, Twitter move* BBC, [cited November 3 2010]. http://www.bbc.co.uk/news/business-11450923

Whittle, S. (2000). *Stop your staff from abusing the internet* (September 8) Vnunet.com, [cited August 24 2005]. http://www.vnunet.com/vnunet/features/2129825/stop-staff-abusing-internet

WIKILEAKS. (2009a). *UK government database of all 1,841,177 post codes together with precise geographic coordinates and other information, 8 Jul 2009* (September 15) Wikileaks.org, [cited September 17 2009]. http://wikileaks.org/wiki/UK_government_database_of_all_1%2C841%2C177_post_codes_together_with_precise_geographic_coordinates_and_other_information%2C_8_Jul_2009

WIKILEAKS. (2009b). *Wikileaks:About* (September) Wikileaks.org, [cited September 17 2009]. http://wikileaks.org/wiki/Wikileaks

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

Winterman, D. (2007). *Just returning your call... to the UK* BBC, [cited September 3 2011]. http://news.bbc.co.uk/2/hi/uk_news/magazine/6353491.stm

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 Jr, 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.com, [cited March 1 2004]. http://www.wired.com/news/business/0,1367,62468,00.html

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

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