

You're being followed

Electronic Monitoring and surveillance in the workplace



Report prepared by Andrew Bibby

Cover artwork by Jane Shepherd

UNI/GS/06-2006/0035/EN

Marta worked for a large multinational insurance company. Or, at least, her job involved processing insurance claims for them. The insurer itself had outsourced this aspect of its back office operation two years ago to a specialist company which made use of agency staff: to be precise, Marta's actual employer was an employment agency.

Marta had worked for the agency for approaching a year, one of a number of jobs she'd had since leaving school when she was 18. Her workplace was an office block on a nondescript industrial park. Every day, she'd swipe her staff pass through the gate at reception and make her way upstairs to her desk. Officially, she worked in a team but the faces in the nearby desks changed regularly. She didn't need to liaise with them anyway. The sets of new claims documents that she had to process came through automatically on to her computer, and her job was just to work through them. Each claim was supposed, on average, to take her 6 minutes 42 seconds to complete. The computer knew exactly how well she was doing and if she was below target at the week's end her team leader gave her a talking-to.

It was a monotonous job but it was at least a job: with her first baby on the way she needed the income. The first months of the pregnancy had been difficult, but she'd struggled in to work each day, even if she'd had to take more breaks. She was, she thought, doing her best.

But that's not what the company had thought. It was a Friday afternoon when she was called away from her desk to one of the manager's offices. The manager was surrounded by computer print-outs. "We've got to let you go," he said. "I've been checking the breaks you've been taking. Look here, four breaks in one morning last week. It's too much."

There, on the print-outs, was a detailed minute-by-minute breakdown of exactly what she had done at work over the past few weeks, including each time she'd left her desk. Marta was astonished. "I never knew I was monitored like this," she said eventually. Her manager looked up from the papers. "Didn't you?" he said. "We know where everyone in the building is all the time. Your staff name-tag has a radio device attached to it. Oh, talking of which, you'd better leave it here. You won't need it again.¹"

Marta Redding is not her real name – but the incident is genuine.

Foreword

Nobody likes the feeling of being spied on. For many workers, the sense that their employer may be surreptitiously monitoring them leaves a bad taste in the mouth. It hardly seems conducive to the feeling of trust on which successful employment relationships are based.

Unfortunately, as this report points out, there are plenty of new technological gadgets and gizmos available to employers who decide that they do want to subject their workforce to high levels of electronic monitoring and surveillance.

Take the minuscule Radio Frequency Identification (RFID) tags, for example, which can be used to track where individuals are every minute of the day, and which can be added to staff passes or even sewn into work uniforms.

RFID, together with other tracking technologies such as GPS satellite systems, can potentially mean that individuals are never able to feel genuinely off-duty, even during their breaks and time-off.

Then there is video surveillance (now much enhanced by the software capability of analysing digital images), keystroke monitoring, telephone call monitoring, email monitoring, and a host of other ways in which individual workers can feel themselves permanently being watched.

Far from information technology helping to release human potential and build a 'knowledge society', it sometimes seems as though it is being used to reduce the potential for independent thought and action in the workplace. At the same time, we are seeing the fundamental human right to respect and dignity at work being threatened.

Of course, new technology in itself is not something bad to be opposed. The aim of this report is rather to highlight some of the abuses which are occurring in the workplace, sometimes quite possibly because employers have simply

fallen into adopting options offered them by software programs without really thinking it through.

UNI is determined to help eradicate these abuses, whilst at the same time seeking to support the development of best practice.

A handwritten signature in black ink, reading "Philip J. Jennings". The signature is written in a cursive style. To the right of the signature is a vertical red line.

Philip J. Jennings
UNI General Secretary



Introduction

Recent years have seen a considerable increase in the extent of electronic monitoring and surveillance in the workplace, including the introduction of new and highly sophisticated digital technology tools.

These technologies can be used positively, in ways which make life easier and better both for employers and employees. But more often they are introduced in ways which are less benign. Sometimes the use by employers of these tools can be unthinking ('the software lets us do this'), sometimes the push may come from a (generally unsubstantiated) belief that a highly monitored workforce is somehow a more productive workforce. Some employers may simply want to use the opportunity to create a passive, quiescent workforce which is less able to exercise its rights to collective organisation and representation.

Almost all UNI's sectors are, in one way or another, directly affected.

This report looks in detail at seven ways in which electronic monitoring and surveillance are currently being undertaken at work:

- Radio Frequency Identification (RFID)
- Wearable computers and Voice Technology
- Satellite and cellular phone tracking
- Video monitoring
- Email and web monitoring; keystroke monitoring
- Telephone call monitoring and call centre working
- Monitoring through biometrics and implants

The report goes on to explore some of the implications for trade unions of electronic monitoring and surveillance, looking particularly at implications for organising and recruitment, health and safety, workers' privacy and the development of an agenda based on the International Labour Organisation's concept of decent work. It concludes with a number of concrete suggestions for future action by UNI and its affiliates.

1. Radio Frequency Identification (RFID)

Radio Frequency Identification is set to become one of the most pervasive new technologies. RFID tags are already used in a wide range of contexts; these include electronic payment cards used in many countries to pay road tolls, bus and metro fares, electronic security tags attached by retailers to clothes to discourage theft, 'intelligent' luggage labels now used in some airports and even electronic time chips worn by marathon runners. In commerce, RFID tags are widely used in logistics to keep track of warehouse stocks and they have been made obligatory for suppliers by major retailers such as Wal-Mart.

RFID 'tags' are tiny microchips, in some cases as small as a grain of sand, which hold unique data identifying the object tagged. These tags, which have a small antenna attached, are read remotely by an RFID reader. Depending on the radio frequency used and the type of tag, RFID tags can be read in some instances up to several kilometres away, although it is more typical for RFID to be used in situations where shorter transmission distances are adequate. Tags can be passive ('woken up' when read) or active, equipped with their own micro-battery and a transmitter.

The price of the cheapest RFID tags has fallen to well below 50 US cents, so that mass uses of the technology are increasingly viable. Retailers anticipate that RFID tags will shortly replace barcodes on supermarket shelves; the key difference is that, whilst barcodes are generic for each sales line, each *individual* item of shopping can be given its own unique RFID identifier. Pilots have been run in several countries.

This use of RFID is controversial. An active US consumer-based campaign CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) says that RFID tags will provide a mechanism for monitoring shoppers' individual behaviour patterns. CASPIAN claims that these 'spy chips' potentially provide a powerful mechanism for invading individual privacy².

RFID chips can be used to identify and track people as well as objects. They are also already in use in countries such as the US and Japan for tracking the movements of old people in residential homes, patients and staff in hospitals, babies in maternity wards and children in schools. This latter use has also proved controversial. An elementary school in California near Sacramento was recently obliged by parent pressure to stop tracking its children through RFID tags³.

In the workplace context⁴, concerns about RFID are likely to have two focuses: firstly, RFID tagging of goods and objects may result in deskilling of some jobs and in the imposition of working practices where employees increasingly have their work controlled by technological imperatives. We return to this below, in the context of changes in warehouse working.

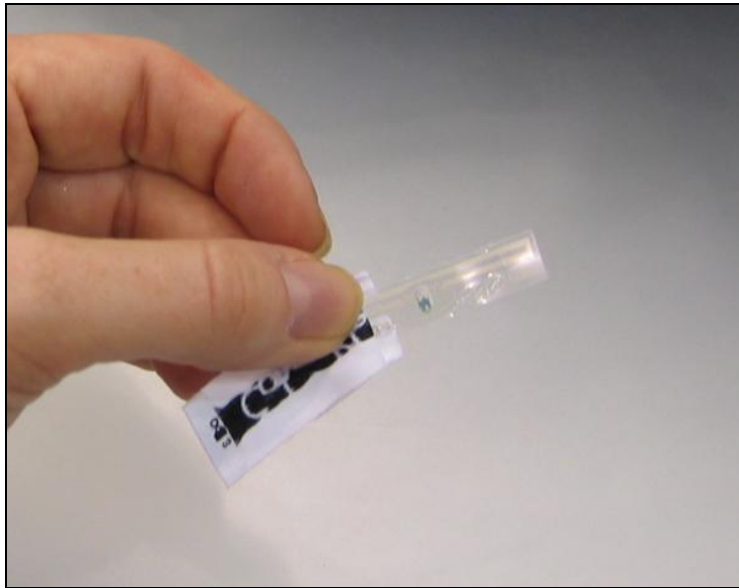
Rather more significant is the opportunity RFID offers to track workers throughout (and indeed, beyond) the working day. There are occasions when this may be desirable; for example, according to one report mineworkers in South Africa and Chile now have RFID tags attached to their breathing apparatus so they can be found in emergencies⁵. However, positive uses like this are likely to be the exception.

Take for example this report of RFID usage, combined with other forms of electronic surveillance, introduced by the Japanese electronics company Omron at its Kyoto factory:

“Omron’s new production management system exploits RFID tags, video cameras, access/security control systems etc to monitor how much employees contribute to the production. Employees carry mandatory RFID tags so that the system can monitor their whereabouts but also their work performance. Based on the previous steps, employee allocation is optimized and quality of products is improved.⁶”

One way of tracking employees via RFID is to place RFID tags in uniforms. Tags can be placed, for example, in labels (the photograph below⁷ shows the back of a small Calvin Klein label, showing the transparent RFID tag); the RFID industry is also working on using the actual fibres of garments to act as RFID

antennae. Clothes like these can be laundered in the usual way without damaging the RFID tags.



In one example, waitresses at one Las Vegas casino now wear uniforms equipped with RFID tags to monitor their work. A senior manager with the company was reported as saying that on almost the first day of the trial one member of staff was disciplined for 'loafing'⁸.

Casino workers in the large Star City complex in Sydney, Australia, also have RFID chips sewn into their uniforms⁹. However, this appears to be primarily for wardrobe management purposes and (although initially viewed with some concern by staff) has generally proved acceptable. Star City employees are unionised through UNI affiliate LHMU (Liquor, Hospitality and Miscellaneous Union). LHMU points out that uniforms are not worn home, so staff are not tracked when off-duty.

It is not necessary, however, to have an RFID chip in your uniform to be closely tracked throughout the working day. By far the commonest use of RFID chips in the workplace are in name tags and identity badges worn to control entry to buildings and rooms.

Although taken for granted as a normal security feature in many workplaces these days, RFID-equipped identity badges in reality provide data for far more than entry systems. Typically the data collected are linked to other company

databases, including HR and payroll records. One IT company, for example, offers software which uses entry system data to produce a range of reports “including attendance report, timecard report, wage report, overtime report, payroll summary, absence report, roll call, employee list, early out report...”¹⁰.

The RAND Corporation recently researched the use of data from RFID name badges in a survey of six US companies. It found that employees were almost universally being kept in the dark about the use being made of this technology. It summarised its findings as follows:

“Companies use RFID workplace access cards to do more than just open doors (eg for enforcing rules governing workplace conduct). Explicit, written policies about how such cards are used generally do not exist and employees are not being told about whatever policies are being followed. Using such systems has modified the traditional balance of personal convenience, workplace safety and security, and individual privacy, leading to the loss of ‘practical obscurity’. Such systems also raise challenges for the meaning and implementation of fair information practices.”¹¹

RAND’s researchers were clearly surprised and disturbed at the lack of written policies or of information being given to employees on these practices, and they conclude their study with the assertion “Any reader who uses an RFID-based access card ought to be uneasy after seeing these results”.

An initial discussion about the implications of RFID in terms of privacy and data protection was held in 2003 by the international conference of data protection and privacy commissioners¹², and the EU’s Data Protection Working Party has also addressed the issue¹³. This latter body calls for RFID monitoring to be undertaken according to data protection principles, including prior notification of the presence of RFID tags and the data subject’s right of access to personal data held. However, it is clear that in both cases these are still early days in terms of developing clear international policies.

Trade unions have also begun to address the issue of RFID tracking.



The British union GMB in July 2005 criticised the EU’s Data Protection Working Party for failing to address the privacy and personnel tracking implications of RFID in the workplace and

called for worker tagging via RFID to be outlawed in the EU. Workers' rights to privacy are being undermined, the union said.¹⁴



ver.di (Germany) suggests the following checklist is used when RFID technology is used in the workplace¹⁵:

- Are employees being given, with due notice, the necessary information regarding plans to introduce RFID technology and their implementation?
- Are there any health issues or risks associated with the use of radio frequencies, scanning devices or photoelectric barriers in the workplace?
- How does the technology affect work routines and how, in concrete terms, does it alter working conditions and the working environment?
- What effect will the introduction of RFID technology have on rationalisation?
- Will employees be given sufficient training in the use of RFID?
- What data, in particular what personal data, will be stored where, and for how long?
- Will data, as it accumulates, be used to control the behaviour and performance of employees?
- Who will ensure that such data is not misrepresented?
- How can workers defend themselves against misuse?

UNI Commerce has also adopted a statement on the introduction of RFID, calling for a serious social dialogue with companies at the forefront of moves to introduce the technology¹⁶.

2. Wearable computers and Voice Technology

Product identification through RFID and through traditional bar coding is being combined, particularly in retail warehouses, with new forms of voice technology and wearable computers to create a working environment where workers are increasingly being turned into automatons.

The GMB union (Britain) received considerable national and international media attention in mid-2005 when it drew attention to work conditions in some UK warehouses which, it said, resembled battery farms: “The only role for the worker is to do as the computer order requires. These devices calculate how long it takes to go from one part of the warehouse to the other and what breaks the workers need and how long they need to go to the toilet. Any deviation from these times is not tolerated. In effect, these devices to dispatch foods to supermarkets and shops have made workers the aid to the computer rather than the other way round.”¹⁷

A typical example mentioned by the GMB is a 12,000 sq metre warehouse in Wales, supplying 240 retail stores. The workers who pick goods are equipped with portable computers which fit over the wrist and lower-arm, to which is attached a scanner unit which is strapped to the index finger. The computer, manufactured by specialist IT company Symbol, weighs 320-350 grams (see illustration)¹⁸.



According to Symbol, “the wrist-mounted terminal receives picking instructions via the wireless LAN from [the company’s] host system. As empty trolleys arrive in the pick area, a picker scans its bar code and the terminal’s LCD screen tells the picker which aisle to go to, which location to pick from and which items to pick. When a picker arrives at the pick face, firstly he scans the bar code mounted at the end of the aisle. This verifies that he is in the correct aisle. He then scans another bar code at the product location to verify he is at the correct place. Finally, he scans each item as it is picked into the trolley.¹⁹” Or, in GMB’s words, “The only functions that the human do are the bits that have not yet been automated”.

Wearable computers currently come in two main categories, those (as in the illustration) which are worn on the wrist and/or finger and those which are worn on the head or belt. They are often combined with voice technology, which involves warehouse workers being given headsets to wear through which they receive oral computer-generated instructions telling them which items to pick. Voice technology systems usually work with order management or warehouse management software programs, with data from these systems being synthesized into speech²⁰.

Possible health and safety implications of this technology have been raised both by GMB and by Professor Michael Blakemore, the UK academic who has advised the union on this issue. Blakemore claims that, despite problems with past technology with Repetitive Strain Injuries (RSI), there is only limited acknowledgement of the possible health implications of this new equipment²¹.

Warehouse picking systems like these do not only automate the work process, they also provide a valuable tool for supervising workers. Blakemore quotes one company’s comment: “[it] is also very easy to use from a management perspective as the trackability and traceability of what each person does is fantastic.”

3. Satellite and cellular phone tracking

As well as RFID, there are various other technologies available which allow the current location of objects or people to be identified with considerable accuracy.

Satellite navigation at present relies on the US Global Positioning System. GPS uses a network of satellites originally introduced for military use and still run by the US Pentagon. Each satellite continually transmits data identifying its position. GPS receivers analyse these signals and by comparing transmissions from four or more satellites can identify their own precise position and height above sea level. (At least four satellites should be 'visible' to each receiver at any one time.)

The European Union is developing its own rival satellite navigation system known as Galileo; the first satellite for the Galileo network was launched in December 2005.

Cellular (mobile) phone technology also offers the ability to track down the locations where active mobile handsets are being carried. This works through identifying the distances from the handset to the nearest base transmitter masts, which together create the cell networks on which mobile telephony is based. Particularly in urban areas where base stations are close together, precise location targeting is possible, typically down to 10-25 metres. Phones don't need to be actively in use to be located.

These two technologies are coalescing, as mobile phones and personal organisers are increasingly GPS-enabled. In Japan, for example, 20% of mobile phones now also act as GPS receivers²².

Both GPS and cellular location services are already being exploited commercially, often in combination with digital mapping services. GPS is used increasingly for in-car navigation systems, for example. Mobile phone operators are exploring the potential of 'location-based services' (for example,

transmission to phone users of the location of nearby branches of fast food outlets, cash machines or even of friends and acquaintances).

In the workplace, as with other technologies, there are positive ways in which GPS and cellular phone tracking can be used which can make life easier for workers. For example:

- Tracking of vehicles can make life safer for the drivers of security vans, at risk of robbery
- Geo-locational tracking can contribute to the safety of mobile workers; this may be particularly true of those working by themselves in isolated or potentially dangerous places, or at night
- Tracking can also help locate mobile workers or drivers when bad weather strikes

Unfortunately, there is ample evidence that tracking is being introduced by employers in much less positive ways. Take this case, for example, quoted by the US National Workrights Institute:

Howard Boyle, president of a fire sprinkler installation company in Woodside, N.Y. presented his employees with cell phones to use, without informing them that they were equipped with GPS. Mr Boyle can find out where they are at all times including during breaks and while they are off duty. "They don't need to know," said Mr Boyle. "I can call them and say, 'Where are you now?' while I'm looking at the screen and knowing exactly where they are"²³.

Continual tracking can create insidious pressures on workers, who feel that they are being watched at every moment of the working day. One US driver whose truck is GPS enabled has been quoted as follows:

"It's kind of like Big Brother is watching a little bit... I get testy in the deli when I'm waiting in line for coffee, because it's like, hey, they're watching, I've got to go"²⁴.

In Canada, the Canadian Union of Postal Workers (CUPW) has warned its members to monitor closely the move by Canada Post to introduce GPS-linked on-board computers in several hundred delivery vans. These monitor (via GPS) the location of each van, and also whether the engine is running, whether the vehicle is moving and if so at what speed, and whether the doors are closed.

Canada Post told the union that its objective is to enable supervisors to find out (through so-called 'exception reports' generated by computer) whether drivers are driving safely and are following security guidelines²⁵.

The CUPW has invoked the current collective agreement with Canada Post to ensure that this monitoring is not used for disciplinary purposes.



The clause of CUPW's collective agreement with Canada Post which covers surveillance reads as follows: "At no time may such [watch and observation] systems be used as a means to evaluate the performance of employees and to gather evidence in support of disciplinary measures unless such disciplinary measures result from the commission of a criminal act."²⁶

Unions have also intervened in other countries to control the use of GPS monitoring. In the United States, the Teamsters union has negotiated with UPS so that GPS tracking data will not be used for employee evaluation or disciplinary purposes²⁷. The Teamsters have also challenged GPS use by other transportation and courier companies and by public authorities.

Where tracking systems are in place, it is particularly important for workers to be able to ensure that tracking ceases to operate during breaks, and at the end of the working day.



Amicus (UK/Ireland) has reported that it has successfully challenged a company's car tracking device as an invasion of privacy, allowing the employee to have the opportunity to override it²⁸.

Geo-tracking services, particularly GPS, have been increasing rapidly in recent years, although we are probably still in the first stages of the implementation of this technology. The 2005 electronic monitoring and surveillance survey undertaken by the American Management Association of 526 US companies reported that 8% were using GPS or GPS/cellular tracking of vehicles whilst 5% were tracking employee cell phones²⁹.

It is still relatively early days in terms of establishing adequate safeguards and good practice to protect what is being called 'locational privacy'³⁰. One guide to employers offered by Canadian legal adviser David Canton suggests a four point checklist for introducing GPS tracking³¹:

- determine the need
- establish a privacy policy
- monitor morale
- gain consent

He warns that, whilst GPS can lead to increased efficiency and productivity, "it can also lead to plummeting staff morale, employee backlash and potential lawsuits".

More general concerns about the need to ensure that individuals can protect their 'locational privacy', particularly in relation to their private life, have been raised by the US National Workrights Institute. As they say, "When an employee knows that his boss watches his day-to-day activities, he might think twice before he takes part in certain activities. For example, if one's boss was a vigilant Republican, an employee might choose not to go to the Democratic National Convention."³²

4. Video monitoring

Overt and covert monitoring of the workplace using video surveillance cameras has been an issue for trade unions for many years. Back in 1993, for example, the Communications Workers of America drew the attention of a US Senate Committee to a case where women staff had found that their management had concealed a camera in their locker room. The camera was monitored by male security guards who watched as the employees changed into their uniforms³³. Very similar cases of cameras covertly installed in washrooms or changing rooms have been reported from other countries as well³⁴.

Video surveillance continues to be an issue which regularly leads to workplace disputes, particularly when cameras are installed without prior consultation or are used surreptitiously for employee performance monitoring or disciplinary purposes. One recent example has been the installation of security cameras by Deutsche Post in the main sorting office in Berlin where 650 employees work. The plan was for the cameras to operate for up to fifty hours a week. This usage was ruled excessive by a federal German employment court³⁵.

In several key respects the use of surveillance cameras today poses greater concerns than in the past, when camera images would be monitored in real time or recorded on magnetic tape. These days, data from cameras is more likely to be in digital form, and as such can be stored on an indefinite basis along with other digitised data. Potentially, for example, digitised data from surveillance cameras focused on individual employees could be linked to other digital data on that individual, for example HR data or data taken from email monitoring or recorded telephone conversations, forming a very powerful integrated set of information available to an employer.

The European Union's Data Protection Working Party has drawn attention to the risks that could come from the development of software applications able to 'interpret' video images, for example by identifying individuals captured on image through facial recognition. In its 2004 report on video surveillance the Working Party states: "This trends applying to the evolution of video

surveillance techniques could be usefully assessed in order to prevent the development of software applications based both on facial recognition and the study and forecasting of the imaged human behaviour from leading inconsiderately to dynamic-preventive surveillance – as opposed to the conventional static surveillance, which is aimed mostly at documenting specific events and their authors. This new form of surveillance is based on the automated acquisition of the facial traits of individuals as well as their ‘abnormal’ conduct in association with the availability of automated alarms and prompts, which possibly entail discrimination dangers”³⁶.

It is increasingly necessary in other words to see video surveillance not simply as a stand-alone security measure but as a source of data which is available for searching and analysis using the full power of contemporary computing. One indication of this trend is Cisco Systems’s development of AVVID (Architecture for Voice, Video and Data) which it claims can be used by the banking industry not only for security but also for marketing and customer relations purposes in maximising the value of bank branches³⁷.

Given this sort of development, it becomes even more important to ensure that the use of video surveillance is adequately controlled. The EU Data Protection Working Party stresses the importance of key data protection principles, including the proportionality of use and prior notification of those subject to surveillance. In the particular context of the workplace, the Working Party calls for the safeguarding of employees’ “rights, freedoms and dignity”. It makes the following comments:

“Video surveillance systems aimed directly at controlling, from a remote location, quality and amount of working activities... should not be permitted as a rule...

“Implementing experience has shown additionally that surveillance should not include premises that are either reserved for employees’ private use or are not intended for the discharge of employment tasks – such as toilets, shower rooms, lockers and recreation areas: that the images collected exclusively to safeguard property and/or detect, prevent and control serious offences should not be used to charge an employee with minor disciplinary breaches; and that employees should always be allowed to lodge their counterclaims by using the contents of the images collected. Information must be given to employees and every other person working on the premises.”

Covert monitoring poses particular concerns, as an example from Sweden demonstrates. Currently UNI affiliate the Swedish Transport Union is engaged with negotiations with Securitas to control the company's recent use of undercover surveillance vans equipped with cameras, being used to film its own vehicles and staff.

Securitas already equips its vans with cameras; however, these begin filming only when vans are attacked or unauthorised doors opened, a practice which has union acceptance. The armed robbery of a Securitas van on the main highway south of Stockholm in December 2005 demonstrated the importance of appropriate security measures. However, the introduction of undercover filming from unmarked vehicles has been strongly criticised by Securitas staff.

The Swedish Transport Union anticipates that a successful outcome to the negotiations and an agreement with the company which will apply throughout the Nordic countries³⁸. Meanwhile, UNI's Danish affiliate DFF has already concluded an agreement with Securitas which restricts the purposes for which video can be used, and includes protection against the use of video footage for disciplinary purposes. Employees must be informed about the monitoring during the recruitment process.

More generally, there are already several examples of good practice in the control of video camera surveillance. A number of countries have legislation in place; in New South Wales, Australia, the protection to workers offered by the Workplace Video Surveillance Act 1998 (introduced following a series of labour disputes in the state) has recently been extended to other forms of electronic monitoring. In Austria, works council approval is necessary before permanent video monitoring is undertaken.³⁹

In Belgium, the use of workplace cameras is subject of a collective agreement negotiated between the social partners in 1998 and having force of law. It covers the whole private sector.



The Belgian agreement is based on the principles of proportionality and end purpose. Permanent surveillance is strictly controlled and is authorised only in cases where it is designed to protect workers' safety or company property. Covert video surveillance is banned, except

where there is considerable evidence of criminal activity. Cameras can only be introduced after consultation with trade unions, and workers affected must be informed in advance. The object of video surveillance must be clearly set out⁴⁰.

5. Email and web monitoring; keystroke monitoring

Issues associated with the monitoring by employers of employees' email and internet usage have received considerable attention in recent years, in part because they have led to practical problems in many workplaces and have formed the basis of a growing number of individual disciplinary cases.

UNI (and UNI's predecessor FIET) can take credit for the early work it undertook in this area, through the Online Rights for Online Workers campaign launched in 1998. UNI's Online Rights at Work Code of Practice has established good practice guidelines which have been taken up both by trade unions and other organisations.

UNI's Code identifies four interlocking issues associated with email and web usage in the workplace – the right of workers' representatives to have access to electronic facilities, the extent to which individual employees are able to use email and the web for their own personal purposes, the conditions under which such personal usage is permitted, and finally the issue of monitoring and surveillance of email and web usage. This report addresses just the last of these four points.



The UNI Code of Practice includes the following section, **monitoring and surveillance of communication**:

The employer undertakes that employees' use of the enterprise electronic facilities will not be subject to clandestine surveillance and monitoring.

Communication will be subject to surveillance and monitoring only if this is permitted by collective agreement, if the employer is legally obliged to do so, or if the employer has reasonable reason to believe that an employee has committed a criminal offence or serious disciplinary offence.

Access to surveillance and monitoring records relating to individual employees will only take place in the presence of a trade union representative or an employee-selected representative.

UNI's Code of Practice draws very much on the principles already widely established under data protection procedures for appropriate handling of individual personal data, as well as on ILO and human rights safeguards⁴¹.

Following UNI's lead, a number of affiliates have undertaken similar initiatives, in many cases producing their own Guidelines and Codes on good practice. Examples include GPA (Austria), MSF (now Amicus) (UK/Ireland), CFDT BETOR-PUB (France), FNV Bondgenoten (Netherlands)(see below).



FNV Bondgenoten's Model Protocol: Privacy in the use of the Internet and Email includes this clause:

The employer shall not read the content of either personal or commercial email messages. Neither shall personal data with regard to number of emails, email addresses or other relevant data be registered and/or checked. This does not affect his right to carry out occasional checks based on compelling reasons that are in the interest of the company. Such checks shall be reported to the works council⁴².

In Germany, ver.di has joined with IG Metall and the DGB (German union federation) to launch the www.onlinerechte-fuer-beschaefigte.de website, and an associated Online Rights campaign. The campaign, which was launched in March 2002 from an internet café in Berlin, has been widely reported in the media. The interactive website includes information on the law and a discussion forum⁴³. This initiative has been followed by a six-point Statement on Internet, Intranet and Email usage, agreed by the DGB Executive in February 2004⁴⁴.



This leaflet, produced by the German unions' Online Rights campaign reads "I'm writing letters, because my boss reads my emails"

Collective agreements covering this area have been agreed in various countries including Austria and Denmark (in the agreement between HK-Service and the Danish commerce employers)⁴⁵. The most important national collective agreement is that from Belgium, agreed between the social partners in April 2002.



The Belgian collective agreement⁴⁶ (which has the status of national law) sets down that monitoring of on-line use by employees is limited. In terms of the internet, employers can collect data on the length of web connections but not identify the sites visits by individuals. For email, the volume and number of emails can be recorded, provided these are not linked to individuals.

The issue of email and web usage by employees has also been the subject of attention in the European Union. The EU Data Protection Working Party has set down general principles applying to email and internet monitoring, which are summarised under the following headings: necessity, finality [ie, purpose], transparency, legitimacy, proportionality, accuracy and retention of data, and security⁴⁷. The European Commission's document for the second stage

consultation of the social partners on workers' personal data also proposes a European framework covering electronic monitoring⁴⁸. It includes the following:

- Secret monitoring should be permitted only in conformity with the safeguards laid down by national legislation or if there is reasonable suspicion of criminal activity or other serious wrongdoing
- Personal data collected by electronic monitoring should not be the only factors in evaluating workers' performance and taking decisions in their regard
- Prohibition in principle imposed on the employer as regards opening private email and/or other private files...

It would be wrong to think, however, that all this activity has satisfactorily resolved the issues of email and internet use. In Canada, for example, a recent academic survey found a very wide range of policies in place, even where collective agreements had been agreed. The weakest agreements, according to the researcher, featured explicit recognition by unions of employers' rights to use any forms of electronic monitoring when and where they wish⁴⁹.

In the US, too, electronic monitoring is widespread. According to the American Management Association, 76% of employers monitor employees' website connections; 55% store and review employee emails. The AMA 2005 survey found that more than one in four companies have sacked workers for alleged misuse of the Internet, and another 25% have sacked staff for email misuse. Despite this, the AMA also found that one company in ten did not tell their workers that internet usage was being tracked; 14% failed to notify workers that email was monitored⁵⁰.

It is hard to disagree with Hubert Bouchet of the French information commission CNIL who has drawn attention to the widespread ignorance among staff of the monitoring which is taking place in the workplace. "The necessary balance between legitimate control undertaken by the company and the respect for workers' rights does not appear to be operating in very many cases," he writes⁵¹.

It is interesting to note that the American Management Association monitoring and surveillance survey also finds that one in three employers (36%) monitor the number of keystrokes on keyboards, time spent at keyboards and/or the

content of inputted material. Union concerns with routine monitoring of keystroke depressions made by workers, especially low-paid staff undertaking basic data inputting work, date back many years. Demands for unrealistically high levels of productivity in keyboard use can be a contributing factor in the development of repetitive strain injuries, which have reached almost epidemic proportions in some countries.

A detailed investigation of software and hardware products which can be used to log keystrokes has been undertaken for German trade unions by Gerrit Wiegand, who has reported his findings in the book *Im Netz@work*⁵².

In retailing, similar concerns with automatic monitoring of check-out employees' scanning rates also date back to the time when barcode and electronic till technology was first introduced. The technology can be used to monitor in detail exactly how staff spend their working days, including such things as the precise time taken by staff for toilet breaks. However, just because the technology permits this sort of electronic snooping does not mean that it must be used like this. It is worth noting that in Metro's new 'future store' in Rheinberg staff have the facility to log in anonymously to operate such things as the in-store electronic scales, so that personal data are not collected.

6. Telephone call monitoring and call centre working

Telephone calls can be monitored in various ways. The number and duration of calls made and the numbers which are called can be recorded; the actual telephone calls can be listened to by supervisory staff, either covertly or openly; calls can be recorded; voice mail messages, too, can be stored and monitored.

In the US, almost exactly half US companies monitor telephone calls by recording numbers phoned and time spent in calls; two-thirds of these firms undertake this monitoring on a regular or on-going basis. However, according to the American Management Association, 22% do not inform their staff that this is occurring. Approaching one in four firms 'tape' calls made⁵³.

In some industries (for example, banking and insurance), there may be legal or regulatory reasons for recording telephone calls. However, this does not mean that recorded calls should necessarily be routinely used for other purposes, for example for monitoring individual employees' productivity or for disciplinary purposes. Telephone calls are increasingly stored in digital format; as with surveillance camera footage, this opens the possibility of data being integrated with other personnel data and being subject to minute analysis by computer software.

Employees should be informed that calls are being recorded.

Some companies say that they listen in or record calls for 'training' purposes. Whilst it may be legitimate in some circumstances for companies to do this to maintain telephone handling standards, staff who need assistance in this area should indeed have the opportunity to access adequate training. Again, this sort of monitoring should not be abused by employers and used for other purposes.

Workers in call centres experience these issues more intensely than most. As an early UNI report on call centre working pointed out, "In general call centre

technology gives employers the power to maintain quite astonishing levels of electronic surveillance and monitoring of their staff⁵⁴.

Furthermore, call centre workers have very little control over their working day, taking calls which are routed to them automatically using automated call distribution (ACD) technology and, in many cases, being obliged to follow scripts when talking to callers, and having rigid sales or performance targets. Typically, ACD technology records all aspects of calls handled, including time spent on breaks or toilet visits. UNI's Global Call Centre newsletter recently reported the case of one woman who was forced to tell her boss before her family that she was pregnant, to explain why she had taken 'too many' toilet breaks⁵⁵. (It was this case which was in part the inspiration for our fictional account of 'Marta', with which this report opens).

UNI's Call Centre Charter and the Action Plan drawn up as part of the 1st UNI Call Centre Conference in October 2005 both address the issue of monitoring and surveillance.



The UNI Call Centre Charter includes six points under the heading **surveillance, electronic monitoring and privacy**.

- Monitoring may only be allowed when the purpose is known and acceptable
- The collected data may only be used for that purpose
- The employee must know that he/she is being monitored or can be monitored
- Listening in may only occur incidentally and not continuously
- The employee must be allowed access to the registered data and be able to correct inaccuracies
- Tappings must be destroyed after a certain period.

Another concrete action, taken recently by UNI Telecom within the context of the European Social Dialogue with the employers' body ETNO, has been to ensure that a clause on monitoring has been included in the agreed Guidelines for Operating Customer Contact Centres. One of the key principles is that call centre workers must be made aware of any performance monitoring arrangements in force.

The experiences of UNI affiliates demonstrate that it is possible to negotiate better working conditions for call centre staff. Several unions in the telecoms sector, for example, have negotiated collective agreements with clauses on monitoring and surveillance.



In the US, the Communications Workers of America (CWA) has negotiated agreements with a number of telecoms firms, including AT&T, Qwest, Bell South and SBC⁵⁶.

The AT&T agreement controls the use of listening in to calls:

- Employees will be given prior notification the day sampling occurs, and each will have the option of remote or side-by-side monitoring
- Individual call sampling will be conducted within the work area of the employee being monitored.
- No employee shall be disciplined as a result of individual service sampling except for gross customer abuse, fraud, violation of privacy of communications, or when development efforts have not been successful.

The agreement with Pacific Bell (SBC) limits monitoring of staff to ten calls per month.

In Australia, the CEPU (Communication Electrical and Plumbing Union) has also tackled the issue of over-monitoring in call centres. Unions are pressing Australian states to sign up to minimum call centre working standards.

One reason why monitoring and surveillance is such an important issue for call centres is because it has been demonstrated in numerous surveys to be a major cause of stress for workers. As one UK academic report put it, “There is no doubt that many workers do see the mechanisms of surveillance and monitoring as contributing to the pressures of the job. Over one-third believed that having their calls taped contributed ‘a great deal’ or ‘to some extent’ to the pressures of the job.⁵⁷” We shall return to this issue again below.

7. Monitoring through biometrics and implants

The final section of this part of the report will look briefly at the scope for electronic surveillance of workers in an even more direct, and intrusive, way – by actually monitoring the individual's body.

The technology of biometrics (recognising individuals from their unique physical traits) is already being used in a variety of everyday settings. Fingerprint scanning has been introduced by the US for monitoring foreign travellers visiting the country. Iris recognition is considered a particularly promising area for future individual identification.

Unlike, say, the traditional way in which police took fingerprints from suspects by utilising ink pads and paper, biometric data are digitised – that is, the data which are recorded are held in digital form and can therefore be subject to detailed computer analysis. Biometrics potentially raises profound privacy implications. Trade unions will need to monitor very closely moves to bring in this technology in the workplace.

There are already examples of biometrics being introduced. McDonalds is reported to have introduced thumb and hand scans for staff in some of its Canadian outlets⁵⁸. Also in Canada, the postal workers union CUPW has challenged moves by the Canada Post Corporation to require some of its mail carriers to be fingerprinted, as part of a 'reliability check'⁵⁹.

Manufacturers of RFID tags have gone a stage further, with the concept of implanting tiny RFID chips within the actual skin of individuals. It would be reassuring to be able to report that, at present, this idea is still science fiction but unfortunately this is not the case. The US company Applied Digital already manufactures such a product, known as the VeriChip.

The VeriChip is marketed primarily as a means of permitting people to have their medical details always available. It has also been used by a night club,

which has encouraged regular clients to have a VeriChip implantation, to gain admission and pay for bar drinks. VeriChips have also already been used in the work context, where eighteen officials working for the Mexican Attorney General's office have voluntarily been implanted. The chips (shown below⁶⁰) are used to admit staff to restricted areas.



The possible health hazards of carrying an implanted RFID chip are considered below. Even leaving aside possible health issues, however, it is clear that new products like the VeriChip have major potential implications for privacy rights, both in the workplace and outside.

Some issues raised by electronic monitoring and surveillance

Why is this happening? Why does an electronically-assisted command-and-control management style seem to be becoming prevalent just at the time when, according to HR rhetoric, the information age requires 'smart work' and more collaborative forms of employee participation?

One cynical answer would be, simply because the technology now exists to undertake this surveillance. Prof Michael Blakemore, who has advised the UK union GMB, talks of the "reassuring" message which this sort of technology can seem to offer: "Deeply embedded in such rhetoric is the promise of security, safety and profits," he writes⁶¹. But he also points out that reliance on technology can have far-reaching results in the workplace: "The outcome is a changing relationship between managers and staff, where the former no longer engage the latter in conversations, but just monitor them".

He and other academics are increasingly using the concept of 'pervasive computing', defined as a process where computers are embedded in everyday life in such ways that they become invisible and taken for granted⁶². Pervasive surveillance by analogy is the situation (again using Blakemore's words) "where everything, or almost everything, that an employee does can be monitored, analysed, and checked".

As the ILO has pointed out in its landmark 1993 Conditions of Work report on workplace monitoring, some workers are more affected by this than others: the kinds of work most likely to be subject to highly intensive monitoring often turn out to be work which is undertaken by women, by workers from minority groups, and generally by the low-paid⁶³. In this context, it is significant that the GMB, in its campaign in the UK against 'battery farm' conditions in warehouses (see above), reported that many of the workers in the warehouses surveyed were migrant workers.

The point, therefore, may be that whilst some workers in an information age who are engaged in high-value knowledge work can indeed find themselves

released from the constraints of hierarchical supervision, many more may find themselves heavily constrained by technology – effectively, in the sort of relationship with technology previously most often identified with assembly line working.

Supervision by electronic monitoring may be ‘reassuring’ for companies, but is it actually effective? The answer very often, it seems, is probably not. Writing in 1999, Gary Marx from MIT made the following assessment: “At present the evidence supportive of the pro-monitoring rhetoric is not strong. As we will note, there are good reasons to expect unrestrained monitoring to be counter-productive. A possible negative impact on workers’ physical and mental well-being may cancel out profits from supposed increased efficiency as a result of monitoring.”⁶⁴

But whether or not surveillance is ‘effective’ for companies is not the point. Even if there were evidence to point firmly to business advantages of pervasive surveillance of workers, there are several powerful reasons why unions should oppose the practice. We will look at three in turn.

Right to collective representation

Firstly, and most pragmatically, unions have cause for concern that worker monitoring and surveillance can be used by unsympathetic employers as a tool to discourage effective collective representation.

There have been a number of cases where surveillance has been introduced just at the time when unions have been attempting to organise non-unionised workforces. One example is from the most notoriously anti-union company of them all, Wal-Mart, which trained surveillance cameras on ‘suspect’ workers at a store in Kentucky during moves by the UFCW to organise the store. The company seems to have followed a similar approach at an outlet in Indiana and very possibly elsewhere in the US⁶⁵

Even where unions are recognised, a working day which is subject to tight monitoring is not necessarily a conducive atmosphere for effective union work. As Eric Lee has pointed out, in times past workers could more easily whisper

concerns to union representatives whilst standing, for example, at a water cooler⁶⁶. The more controlled the working day, the less chance there is for this sort of informal liaison between worker and rep.

Health and safety issues

New technology brings new occupational safety and health hazards. The introduction of computer keyboard working for tasks such as data entry led to a widespread increase in the number of people suffering from repetitive strain injuries, whilst acoustic shock has been identified as a danger for call centre workers.

It is not necessarily easy to identify at present exactly what the implications for workers' health of the growth of 'pervasive computing' will be. It certainly doesn't help that manufacturers of the technology described in this report do not in general give much attention in the technical information they make available to issues of ergonomics or occupational health and safety.

However, some potential issues can be readily identified. Firstly, the use of wearable computers (such as those illustrated earlier in this report) raises concerns about possible physical effects of continued usage. As mentioned above, one popular wrist-mounted computer weighs 320gms, with the weight increasing to 350gms when a radio transmitter/receiver is included. Index finger-mounted scanners weigh typically about 50gms, with scanning operated by regular squeezes of the thumb⁶⁷.

The worldwide growth of cellular phones has led to concerns about possible dangers from electro-magnetic radiation, an area of research where findings to date are inconclusive. Little work appears to have been done about the implications of other tracking technologies. As regards implanted RFID chips, the US Federal Drugs Agency has licensed use of the VeriChip but has itemised potential risks to health as follows: "adverse tissue reaction, migration of implanted transponder, compromised information security, failure of implanted transponder, failure of inserter, failure of electronic scanner, electromagnetic interference, electrical hazards, magnetic resonance imaging incompatibility, and needle stick."⁶⁸

More generally, there is a considerable bank of research which suggests that there is a link between the introduction of performance monitoring and an increase in workers' safety and health problems. The most obvious health and safety issue raised by electronic monitoring and surveillance is the associated increase in workplace stress. As far back as 1993, the ILO report on workplace monitoring and surveillance made the following point:

A study conducted jointly by researchers from the University of Wisconsin and the Communications Workers of America on electronic monitoring and job stress confirmed earlier studies that implicated electronic monitoring as a major stress factor in the workplace, which is linked, in part, to the sense of powerlessness that monitored employees feel.⁶⁹

Stress has been identified as a major matter of concern in call centres, an issue which was discussed at UNI's 2005 Call Centre Conference. The Conference called for a drive to improve the health and well-being of staff at the world's call centres, including action to reduce stress, anxiety, burn-out and depression.



Performance measuring is based on team rather than individual performance at Verizon-South in New Jersey, a practice which was recommended by the CWA-Verizon Stress Committee⁷⁰.

In recent years, workplace stress has begun to be taken more seriously as an occupational safety and health issue. For example, in 2004 the European social partners formally agreed a framework agreement on work-related stress. Nevertheless, the links between electronic monitoring and stress still appear to be inadequately understood. The EU framework agreement does not make specific reference to the relationship between surveillance and stress, for instance.

Privacy and decent work

Perhaps the most substantive issue raised by monitoring and surveillance relates to the fundamental right to privacy for workers. As an EU report has put it, "Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace"⁷¹. In fact, privacy becomes even more

important given that the traditional clear boundaries between 'work' and 'personal' time and space are increasingly becoming blurred through developments such as teleworking and flexible hours contracts.

It is now almost ten years since the ILO tried to tackle the privacy issues raised by the storage of personal data on workers. Its (voluntary) Code of Practice included a short clause on monitoring⁷².



The ILO Code section 6.14 reads as follows:

If workers are monitored, they should be informed in advance of the reasons for monitoring, the time schedule, the method and techniques used and the data to be collected, and the employer must minimize the intrusion on the privacy of workers.

Secret monitoring should be permitted only:

- if it is in conformity with national legislation, or
- there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing

Continuous monitoring should be permitted only if required for health and safety or the protection of property.

Since then, issues of workers' privacy have tended to be dealt with tangentially, through more general data protection legislation. In the European Union, for example, member states have been required to legislate the requirements of the 1995 Data Protection Directive. The European Commission has proposed that the particular issues of workplace data protection should be addressed in social dialogue between the social partners. In 2002, the Commission drew up a detailed proposal for a framework agreement (see below) to be used in these discussions. However, an anticipated follow-up report from the Commission failed to appear in 2004 and this issue seems currently to have been quietly 'parked'.



The proposed European framework agreement lays down a number of principles, among them the right of workers' representatives to be informed and consulted before monitoring/surveillance is introduced or modified, restrictions on continuous monitoring, tight guidelines on secret monitoring, and the prohibition of routine monitoring of emails and internet

use. In addition, "personal data collected by electronic monitoring should not be the only factor in evaluating workers' performance"⁷³.

One notable example of a valuable legislative initiative comes from New South Wales (Australia), where the Labor-controlled state government last year (2005) passed the Workplace Surveillance Act. This Act extends the controls first introduced in the 1998 Workplace Video Surveillance Act to other, newer, forms of electronic monitoring. In the US, the Communications Workers of America (CWA) has been working for a similar bill, which would restrict the use of video and audio surveillance in the workplace, to be passed by Congress⁷⁴.

A number of union federations and individual unions have developed good practice codes covering workers' privacy. One example is FNV (Netherlands) which has developed a model privacy regulation⁷⁵ The IT Professionals Association (part of the UK/Irish union Amicus) also has produced a similar draft code of practice⁷⁶.

What initiatives like these help to demonstrate is that the collection by employers of electronic data on workers through different forms of monitoring and surveillance is not just a technical issue of meeting data protection standards. What is being addressed here are fundamental human rights questions. At root, the issue is one of human dignity.

Conclusion: the way forward for UNI

Although electronic monitoring and surveillance are on the increase in many different sectors, it is not necessary to fall into a technologically-determinist inspired gloom. There are already plenty of examples of good practice by unions and others in responding to these developments. UNI itself has the experience both of the successful Online Rights for Online Workers initiative and of the campaigning work around call centre working, including the recent Global Call Centre Conference. UNI affiliates and other union organisations have also positive experiences (some of which have been mentioned in this report) which can be shared.

Nevertheless, it is appropriate for UNI to consider how it can maximise the role it plays in addressing the issue of electronic monitoring and surveillance. In particular, a number of further steps could be considered.

1 There has been little attention paid to the very rapid development of RFID technology. RFID tracking is becoming increasingly common, particularly in relation to RFID-enabled name badges. A UNI Code of Good Practice (similar to UNI's successful Code of Practice on Online Rights) will be published to assist affiliates in their work.

2 RFID monitoring links also to broader issues of worker tracking, through the use of GPS and cellular phones. UNI will initiate broader global campaigning work (*Who's on Your Tracks?*) to help both affiliates and their members understand and address the issues here. The report will be tabled for discussion in each of the UNI Global Unions.

3 The ILO will be encouraged to address the issues of electronic surveillance and monitoring. It is more than ten years since the last substantive ILO research was undertaken in this area. The issue of electronic monitoring and surveillance can be directly linked to the ILO's call for decent work.

4 UNI will engage with the European Union and other regional organisations on these issues, and will participate in the European Commission's current consultation on RFID technology.

5 Publicity on the health and safety implications of excessive monitoring, particularly in relation to workplace stress, will be published by UNI on its website.

6 UNI will continue to promote vigorously the Call Centre Charter and the Code of Practice on Online Rights.

7 Electronic monitoring and surveillance are not issues which are unique to the workplace. UNI affiliates are encouraged to make common cause with civil liberty and privacy advocacy organisations, as well as with broader campaigns (such as the consumer campaign in the US against RFID use in customer monitoring) concerned at the way in which new technologies are being introduced.

-
- ¹ This story is based on real events and real issues
- ² <http://www.nocards.org>, <http://www.spsychips.com>
- ³ Alorie Gilbert, Elementary school nixes electronic ID, February 17 2005
http://news.com.com/2102-1029_3-5581275.html
- ⁴ Andrew Bibby, Invasion of the privacy snatchers, Financial Times, January 9 2006
- ⁵ Paul Tyrrell, Tuned in to the right frequency, Financial Times, December 15 2004
- ⁶ Posting on Smart Mobs,
http://www.smartmobs.com/archive/2005/05/04/rfid_employee_m.html. See also
<http://ubiks.net/local/blog/jmt/archives3/003741.html>
- ⁷ from <http://www.spsychips.com>
- ⁸ Will Sturgeon, Las Vega casino goes for RFID, April 15 2005
<http://software.silicon.com/security/0,39024888,39129583,00.htm>
- ⁹ Accenture, Silent Commerce Chips Away at Star City Casino Wardrobe Worries, case study,
http://www.accenture.com/Global/Services/By_Subject/Radio_Frequency_Identification/Client_SuccesSES/StarCityCasino.htm
- ¹⁰ WaspTime see http://www.waspbarcode.com/wasptime/wasptime_premium.asp
- ¹¹ RAND, Research brief, Privacy in the Workplace, 2005. See also RAND, Technical Report, 9 to 5: Do you know if your boss knows where you are? 2005 <http://www.rand.org>
- ¹² Resolution on Radio Frequency Identification, 20 November 2003
- ¹³ Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, January 19 2005, WP105
- ¹⁴ GMB Pres release, GMB seeks changes to European law to outlaw worker tagging, July 18 2005 <http://www.gmb.org.uk/Templates/Internal.asp?NodeID=92057>
- ¹⁵ Cornelia Brandt, Klüger als die intelligenten Dinge sein... Risikoabshätzung bei RFID-Anwendung fordert Handeln auf verschiedenen Ebenen, 2005
- ¹⁶ UNI Commerce, Technology and RFID must be negotiated January 26 2005
http://www.union-network.org/UNIsite/Sectors/Commerce/Social%20dialogue%20articles/EU_dialogue_increasingly_important.htm
- ¹⁷ GMB Press release, GMB Congress demands to electronic tagging of workers 'battery farm; workplaces, June 6 2005 <http://www.gmb.org.uk/Templates/Internal.asp?NodeID=91861>
- ¹⁸ http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
- ¹⁹ Case study, Hands-free Plus real-time, equals business advantage,
http://www.symbol.com/category.php?fileName=CS-27_Peacocks.xml
- ²⁰ See for example Katrina Arabe, Wearable Computers: the new warehouse wear, February 13 2003, http://news.thomasnet.com/IMT/archives/2003/02/wearable_comput.html
- ²¹ Michael Blakemore, I-DRA Ltd/GMB, Surveillance in the Workplace – an overview of issues of privacy, monitoring and ethics, September 2005
- ²² Eurotechnology Japan, Location Based Mobile Services in Japan,
<http://www.gii.co.jp/english/ek32275-mobile-services.html>
- ²³ National Workrights Institute, Privacy Under Siege: Electronic Monitoring in the Workplace, n.d.
- ²⁴ Adam Geller, Bosses keep sharp eye on mobile workers via GPS, Associated Press, January 3 2005 http://www.workrights.org/in_the_news/in_the_news_associatedpress.html
- ²⁵ On Board Computer – Big Brother Comes to CPC
- ²⁶ Agreement between Canada Post Corporation and Canadian Union of Postal Workers (expires January 31 2007)
- ²⁷ National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace n.d.; Gundars Kaupins and Robert Minch, Legal and Ethical Implications of Employee Location Monitoring, Proceedings of the 38th Hawaii International Conference on System Sciences
- ²⁸ David Hencke, AA to log cal centre staff's trips to loo in pay deal, The Guardian, October 31 2005
- ²⁹ American Management Association, 2005 Electronic Monitoring and Surveillance Survey
- ³⁰ See for example Jonathan Raper, Technology Trends- brave new world?,
<http://www.geoplace.com/ge/2001/0101/0101tt.asp>
- ³¹ David Canton, Employee Tracking and Monitoring,
<http://www.canton.elegal.ca/archives/2005/06/>. Another checklist for employers is offered by

Gundars Kaupins and Robert Minch, Legal and Ethical Implications of Employee Location Monitoring.

³² National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace n.d

³³ Hazards magazine, Stop Snooping, <http://www.hazards.org/privacy/>

³⁴ For example at Guy's Hospital, London. Hazards magazine, Stop Snooping, <http://www.hazards.org/privacy/>

³⁵ Gregor Wittich, Rechtsprechungsübersicht zur Verwendung neue Medien im Betrieb, in DGB, Internet und E-Mail: Neue Medien im Betrieb, 2004

³⁶ Article 29 Data protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, adopted February 11 2004. See also Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data by means of Video Surveillance, adopted November 25 2002.

³⁷ Anthony Hildebrand, Branching Out,

<http://www.smtdirect.co.uk/story.asp?sectioncode=0&storyCode=3060661>

³⁸ Information from the union, Jan 2006

³⁹ Prof Frank Hendrickx, Protection of workers' personal data in the European Union, Study 2: surveillance and monitoring at work

⁴⁰ FGTB, Surveillance par caméras: la CCT no 68,

http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0404.htm

⁴¹ <http://www.union-network.org/UNIsite/Sectors/IBITS/ICT/online.htm>

⁴² FNV Bondgenoten, Model Protocol: privacy in the use of the internet and e-mail, n.d.

⁴³ Cornelia Brandt, Onlinerechte für Beschäftigte, in DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004

⁴⁴ Eckpunkte der Nutzung von Internet, Intranet und E-mail im Arbeitsverhältnis, in DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004

⁴⁵ European Industrial Relations Observatory, New technology and respect for privacy at the workplace, 2003 <http://www.eiro.eurofound.eu.int>

⁴⁶ http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0405.htm

⁴⁷ Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, adopted May 29 2002, WP55

⁴⁸ European Commission, Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data 2002

http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdatapro_t_en.pdf

⁴⁹ Professor Vincent Mosco, What are Workers Doing about electronic surveillance in the workplace? An examination of trade union agreements in Canada, proposal for presentation at the 2005 Conference of IFIP Working Group 9-2 Conference

⁵⁰ American Management Association, 2005 Electronic Monitoring and Surveillance Survey

⁵¹ Hubert Bouchet, La cybersurveillance sur les lieux de travail, CNIL March 2004

⁵² Michael Sommer, Cornelia Brandt and Lothar Schröder (eds), Im Netz@work, VSA-Verlag, 2003

⁵³ American Management Association, 2005 Electronic Monitoring and Surveillance Survey

⁵⁴ Andrew Bibby, Organising in Financial Call Centres, UNI, 2000

⁵⁵ UNI Global Call Centre News, April 2004

⁵⁶ Communications Workers of America, <http://www.cwa-union.org/workers/customer/protections.asp>

⁵⁷ Philip Taylor and Peter Bain, Trade Unions and Call Centre Survey, for Finance Sector Unions, 2000

⁵⁸ Hazards magazine, Stop Snooping, <http://www.hazards.org/privacy/>

⁵⁹ http://www.cupw.ca/pages/document_eng.php?Doc_ID=595

⁶⁰ Photo from <http://www.spsychips.com>

⁶¹ Michael Blakemore, Every breath you take, every move you make, <http://www.unionweb.co.uk/view/PageView.aspx?Page=273>

⁶² Martin Dodge, Rob Kitchin, The ethics of forgetting in an age of pervasive computing, UCL, <http://www.casa.icl.ac.uk>. A Galloway, Intimations of everyday life: ubiquitous computing and the city, Cultural studies, 18 (2/3), 2004

-
- ⁶³ ILO, Conditions of work digest volume 12: Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993
- ⁶⁴ Gary Marx, Measuring Everything that Moves: the new surveillance at work, in I and R Simpson, The Workplace and Deviance, 1999, <http://web.mit.edu/gtmarx/www/ida6.html>
- ⁶⁵ How Wal-Mart keeps Unions At Bay, Business Week, October 28 2002
<http://72.14.207.104/search?q=cache:YRWfcqtIO2IJ:www.2110uaw.org/gseu/archive/How%2520WalMart%2520Keeps%2520Unions%2520at%2520Bay.htm+surveillance+cameras+workplace+union+organizing+drive&hl=en&gl=uk&ct=clnk&cd=2>
- ⁶⁶ Eric Lee, Trade Unions in the electronic workplace, April 13 2004
<http://www.ericless.me.uk/archive/000079.html>
- ⁶⁷ http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
- ⁶⁸ <http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt>
- ⁶⁹ ILO, Conditions of work digest volume 12: Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993
- ⁷⁰ Communications Workers of America, <http://www.cwa-union.org/workers/customer/protections.asp>
- ⁷¹ Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, adopted May 29 2002, WP55
- ⁷² ILO, Protection of Workers' Personal Data, 1997
<http://www.ilo.org/public/english/support/publ/pdf/protect.pdf>
- ⁷³ European Commission, Second stage consultation of social partners on the protection of workers' personal data,
http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdatapro_t_en.pdf
- ⁷⁴ CWA-Backed bill would protect workers' privacy in changing areas, CWA press release, March 1 2005. <http://www.cwa-union.org/news/cwa-news/page.jsp?itemID=27374804>
- ⁷⁵ http://home.fnv.nl/02werkgeld/arbo/wetgeving/privacy/Model%20Privacyreglement/model_privacyreglement1.htm
- ⁷⁶ <http://www.amicus-itpa.org/juneconf2.shtml>