LEGAL ISSUES AND RISKS IMPACTING WIRELESS WORKFORCE

ABDUL HAFEEZ BAIG & RAJ GURURAJAN

DEPARTMENT OF INFORMATION SYSTEMS, THE UNIVERSITY OF SOUTHERN QUEENSLAND, TOOWOOMBA, QLD 4350
email: **abdulhb@usq.edu.au**

ABSTRACT

The recent demand for wireless technology at enterprise level has attracted the attention of many CEOs in order to address any potential legal challenges arising due to ignorance from organisations' part, or address employee concerns with respect to health and safety issues, or to improve employee well-being, or just to avoid any expensive legal battles because these changing legal frameworks may have a profound impact on organisations. This has resulted in examining the behaviour of the workforce because the increased use of various mobile devices may result in the removal of the distinction between private and professional workplaces. Further, this mobility sometimes dictates the workforce to adapt flexible work styles according to external conditions to realise efficiency gains. These 'flexible' aspects have forced enterprises to support their work force with devices, tools, processes and collaborative internal and external frameworks in order to achieve efficiency. However, in real life environment, some of these frameworks may conflict with domestic and international laws, union agreements and other individual employment contracts. In the mobile domain, these issues also vary by regions, economic conditions and cultural attitudes. This paper introduces the changing IT workforce due to the influence of wireless technology and provides a discussion on various issues that need to be addressed by organisations.

INTRODUCTION

The proliferation of Information Technology (IT) has changed the way in which 'work' is conducted. The introduction of computers in the early 70s, followed by the concept of globalization in the early 80s, the financial crisis encountered in the 90s by many organisations, and the frontier technologies such as the Wireless Technology, resulted in a dramatic change in the way work is conducted. As a result of this, organisations favoured short-term contracts, changed the patterns of working, introduced new concepts such as 'self-regulated' teams, moved towards a flexible work force and included many skills and functions directly relating to the Information Technology (Tang & Cheung, 1996).

Employee well-being has been studied for over 40 years covering aspects from working conditions to wages as these have impact on organisations (Rozwell et al., 2002). Contractual issues associated with employment are studied by OECD and their impact on countries has been reported as these have cost implications on organisations (OECD, 1999). Literature also reports on patterns of working days, self-regulated hours and reliance on computer technology specific to working conditions and resulting health issues (Cox et al., 2000). Aspects of organisational psychology in terms of job insecurity, work hours, control at work and managerial style are also reported in the literature as these have impact on economic stability of societies

(Sparks et al., 2001). While these studies have concentrated on the 'physical' conditions of the workforce, some of the emerging concepts appear to be in classifying workforce based on the usage of technology, especially mobile devices (Dyer, 2003).

Due to these changes in the workplace, various studies explored issues such as job insecurity, work hours, control at work, and managerial styles. While these issues have a direct bearing on the work force, issues relating to the regulatory framework have also been studied due to the power exercised by unions on workforce in many countries. These studies indicate that, in the context of fixed work environment, legal and regulatory issues associated with work, health and safety are well regulated in most countries (Deitel & Deitel, 2001). For example, in Australia, regulations [1] exist for workplace agreements, issues concerning employee contracts, long service leave payment and for wages and conditions. These regulations comprehensively outline workplace agreements between employees and employers, specific employment conditions, state regulations governing labour relations and better practice for small businesses.

While these work practices are regulated in the context of physical work environment, the relevance of those regulations to an extended workplace, such as the Wireless Technology based work environment, is currently under researched. For example, some devices (PDAs) used by employees to access corporate databases have raised concerns in terms of security, health hazards and maintenance (Simpson, 2003). In terms of the wireless devices, the hazards are more likely connected with their use rather than the device itself. For instance, the possible adverse consequences of using a notebook computer provided by the organisation by members of family for their private use have created unpleasant results in certain organisational contexts. Therefore, it is necessary to introduce new regulations to avoid any potential damage to public, employees and organisations.

The objective of this paper is to establish the importance of regulatory issues applicable to the wireless workforce as limited details can be found in the existing literature applicable to the Wireless Technology based workforce. This paper is organised as follows. Initially the wireless workforce is discussed to provide an idea of various categories of this workforce. Then the organisational challenges resulting from the access to Wireless Technology is discussed. Based on this background, a comprehensive discussion on the mobile workforce legal issues is provided. Then a brief discussion is provided as to how risks can be mitigated, followed by the impact of regulations on the mobile workforce.

THE MOBILE[2] WORKFORCE

The current penetration of the Wireless Technology has given rise to the classification of the workforce based on access to organisational data as employees gain knowledge based on these data. The workforce, based on access to data, is classified into (a) workforce that remotely access organisational data, (b) workforce that gather information or knowledge needed to conduct one's work and (c) executives using their computers to communicate with others for decision making purposes (Rozwell et al., 2002). In essence, it may be possible to classify the workforce that relies on the Internet

[1] www.law.gov.au provides details of regulations associated with the work force.

[2] The terms mobile workforce and wireless workforce are used interchangeably to refer the same concept in this paper

(using wireless technology) into one of these three classifications. Various research firms, including Gartner Research, suggest that it is therefore possible to identify three distinct group of workforce using the Wireless Technology, namely, (1) fixed remote worker, (2) knowledge worker, and (3) executive with access to mobile services.

A fixed remote worker is characterized by a desktop in the office or at home as a predominant tool. This desktop is connected with a wireless device such as an access point. This wireless access point is used to connect to the Internet using a home computer network with access to the office. This worker typically accesses emails and other data by using this wireless network at home. In terms of legal issues, privacy and confidentiality of client data stored inside the computer hard disks of these employees is important.

A knowledge worker is primarily a corporate worker in a large, corporate building. The tools used by this worker include wireless notebooks and PDAs. This worker captures client data and other data associated with the organisation to conduct his/her work. This worker also 'synchronizes' the data captured using these tools onto one device. Usually any data required to support a transaction is appropriately integrated with organisational databases, and personal data are synchronised with the notebooks via PDAs or mobile phones. In terms of legal issues, the way in which the data is collected and used is important to this worker.

The executive usually travels by road or air and accesses corporate data as a primary requirement to conduct work related activities while travelling. This executive uses PDAs predominantly for data collection and access purposes. In the current climate, the PDA used by these executives consists of a phone, camera and a scheduler. In certain countries (for example Australia) sending pictures using PDAs is restricted by legal regulations. While issues such as these have legal significance, data security is important to this group because of potential security threats based on the data access (Gururajan, 2001).

ORGANISATIONAL CHALLENGES

While the Wireless Technology facilitates both content creation and access, organisations face a challenge in properly integrating this information into organisation databases. A number of studies in the past have singled out the email application as the most used application and this vital method of communication will facilitate access to corporate users resulting in significant productivity gains. The reason for this is, there is no need to identify a telephone or network connection to establish email connections in the wireless medium and the workforce can communicate using email applications. Further, with the advent of email response management software (ERMS), it is possible to integrate information originating from various devices using emails with corporate databases and this will provide the most needed data access (Leung, 2002). In recent months, costs have declined, interoperability has improved and access is faster - ensuring that WLAN can easily give enterprises a competitive advantage (Stevenson, 2001). Despite all these, it appears that a model to properly integrate information emerging from mobile devices is not yet available.

Despite the advantages offered by technologies such as the Internet, enterprises still need to cater for different types of technology depending on workforce's different levels of mobility and the frequency with which they access data. While a fixed remote worker needs access to data, speed may

not be a major issue. On the other hand, for executives using mobile devices, speed might be a crucial issue as their working time is expensive and they need access to data for decision making purposes. Therefore, organisations need to assess their Internet requirements carefully in order to satisfy the needs of their workforce. In addition to these technical challenges, organisations encounter legal challenges because they have a responsibility to meet the demands of the workforce using the Internet as a principal medium for data access. These legal challenges are discussed below.

THE MOBILE WORKFORCE LEGAL ISSUES AND RISKS

A key element for an organization is the ability to manage its Internet workforce that is geographically dispersed with blurred borders between private and professional lives and workplaces. As mentioned earlier, employees need to switch roles, locations and "work time" according to external conditions, and adapt their work styles accordingly in order to achieve high levels of efficiency. This requires the enterprise to provide them with devices, tools, processes and collaboration frameworks (internal and external) that may conflict with laws, union agreements and individual employment contracts.

Issues that must be addressed to minimize workforce risks vary by region, depending on legal frameworks, economic conditions and cultural attitudes. They include, but are not limited to the use of mobile devices in multiple contexts, location based mobile services, electronic appraisal, work time, and content and communication liability. These issues are now discussed below.

Multi Use of Devices

Organisations should be aware of issues associated with consumer protection and employment laws because employees in organisations use a multitude of devices such as mobile phones, laptops and a host of new portable devices as part of the normal toolset to access the Internet. The current practices include the use of these devices for personal use. In many organisations, this is tolerated. However, this personal use must be monitored closely for cost and liability. If these devices are not monitored properly, organisations could pay a heavy cost for usage pattern or for liability resulting from the improper use of these devices. While most enterprises absorb the cost component, they seldom encourage the liability aspect such as if a device malfunctions during private use and causes physical or financial damage to a worker. For example, a positioning device that is not calibrated accurately may transmit the wrong location coordinates via the Internet and this may result in the wrong identification of personnel using the device. This may be detrimental in certain contexts such as health where ambulances may use these devices to identify a person who is need of urgent health care. An ineffective antivirus at home computer level might allow personal correspondence files to be transformed to an organisational device and this can damage corporate networks. Depending on whether the worker is acting during or outside working hours, liability varies. Currently there are no uniform laws to address these issues and these are taken care of by contractual negotiations (Freeman, 2003; Kuechler & Grupe, 2003).

Electronic Appraisal

Employers should make greater use of technology for performance assessment because the advent of the Internet applications facilitates employees to move away from their fixed location and provides abundant freedom to perform. Employees' mobility and their freedom from enterprises' physical premises

suggest that there is scope to perform duties in conditions that address individual needs. This concept is emerging at the moment. In the future, it appears that electronic appraisal will be integrated with physical measures. It appears that such appraisal methods will become accurate with wider adoption of new wireless and mobile devices and applications. However, in several European countries, electronic appraisal as the sole means to evaluate employee performance is illegal. Data protection laws in several countries discourage this practice. Therefore, increased reliance on electronic appraisal may expose enterprises to significant tensions with unions (Dixon & John, 1989).

Work Time

When it comes to the mobile workforce, due to the undefined definition of working hours, issues such as what constitutes over-time, how it is calculated and what is normal working time will all arise (Cox et al., 2000). In countries such as Australia, the maximum work time is regulated by the legal system. However, it should be possible for an organisation to call upon employees at different times from different locations, and who can work overtime with flexibility. In most cases, organisations employ external contractors rather than with full-time employees to achieve flexibility (Cox et al., 2000). This is done to keep a close watch on salaries etc. On the other hand, trust and training concerns suggest that enterprises will use their own employees to react to emergencies. Currently the union agreements are not addressing these issues satisfactorily.

Content and Communication Liability

One of the greatest advantages of the mobile technologies is that employees can organize themselves into "virtual communities," sharing information and ideas through instant messaging or Internet discussion systems/forums. In fact, the Bluetooth protocol for wireless communication is developed primarily for these ad-hoc networks. Therefore, it is possible for employers to manage these networks outside the boundaries of the enterprise and into the public domain using tools[3] such as Microsoft Network Messenger. While the technology facilitates such ad-hoc communication easily, significant personal and enterprise liability risks occur as the border between private and public use is blurred where there is possibility for misuse of sensitive information, and with potential clashes between public-system and enterprise codes of conduct (Craig & Julta, 2001). The misuse can happen either by ignorance or deliberately by certain un-trusted parties within the network. There is no regulation to prohibit these situations currently.

Financial Risks

Traditional risks and non-traditional security risks can interrupt a business or literally shut it down. Today, most organisations rely on computers for their daily operations. For example, a security breach by a hacker can severely disrupt a business and those that depend on it. Most businesses using the Internet are dependent in several ways on the continued reliability and operation of computer controlled systems not within their control. This includes telephone networks managed by external parties. Businesses are dependent on their financial institutions that are also managed and controlled by computers. Organisations are dependent on their Internet service providers to establish mobile data access. Suppliers and customers depend on each other's electronic data systems and on mutual systems, such as a third-party

[3] Other tools include AOL Instant Messenger, or private chat rooms hosted by public server such as Yahoo.

commodity exchange to perform financial transactions. When one system fails, it may cause the other systems to fail as well. Failure may be a slowdown of the dependent system, also called the 'brownout' or a total denial of service, also called the 'blackout' (Andrews, 2001; Kuechler & Grupe, 2003).

These risks can result in many different types of losses. The losses that arise from reliance on a third party can generally be grouped into: (1) loss or damage to property, both tangible and intangible, (2) business interruption, and (3) extra expense. Property losses occur when loss or damage is suffered to a firm's own tangible property or to property for which the firm is responsible. Traditionally, this meant damage to a building or other business property, including computer equipment. In the Internet workforce world, the focus is on damage to computer networks and, more importantly, data. An important issue is whether data is considered tangible property under a typical property insurance policy. It appears that insurers will begin to address the issue of what is defined as covered property under these policies. More likely, courts will have to decide this issue.

Property losses can also occur when an organisation's intangible or intellectual property is infringed or violated. Copyrighted materials can be copied without permission, trademarks can be infringed upon or diluted, and patented property or ideas can be stolen. Today, a firm's intellectual property may be its most valuable asset. Organisations need to protect their intellectual property from hackers, crackers, competitors, and others, as well as make sure they do not infringe on the intellectual property rights of third parties. This could potentially expose a firm to third-party liability.

Time element losses typically include business interruption (BI) losses and service interruption losses. BI loss is the economic loss resulting from the interruption of business activities. Business interruption losses may result from the inability to access data, the theft of data, or a threat to the integrity of the database. For example, a security breach of a credit card database may cause the database owner to curtail activity on the system until a damage assessment is completed and the system integrity is re-established. Not only is there a disruption of the database operations, there is also a consequential effect on all third-party users of the system.

Service interruption losses include economic losses associated with the interruption of utilities. A service interruption incident can occur from an "off-site" exposure or event. There have been many incidents of communication cables inadvertently being cut. Long-distance telecommunication companies have experienced software problems in data routing that effectively crippled their networks for several days.

In addition to the business losses and service losses, mobility gives rise to new implications about doing business and being protected from interruptions in doing business. Businesses suffering losses related to server outages face the risk of losing customers for extended periods of time. In mobile settings, the increased reliance on suppliers is also exposing businesses to new risks for financial losses. These range from suppliers of goods (such as raw materials) to suppliers of services (such as server usage, delivery services, electricity, and telephones).

Business interruption may have several consequences such as loss of income, extra expenses to recover, loss of customer, partner, and shareholder confidence and ultimately, reduced

market capitalization. Third parties harmed by the denial of service may sue, adding liability losses to first-party damages. In some cases, business interruption may constitute a breach of contract.

Expenses incurred due to Business Interruptions

In the event of an interruption, a business may incur considerable expenses to resume operations as quickly as possible. Extra expense coverage is for those costs incurred by the policyholder in excess of the normal costs that would have been incurred to conduct business during the same period had no loss or damage occurred. An example of extra expense might be increased freight charges incurred to meet a customer's demand for an order due to delays in the production process associated with a loss event.

In the mobile workforce domain, there are new types of costs that may need to be considered in the context of risk and insurance, including additional costs of operating Web sites from alternative servers, costs of operating Web sites through alternative providers, costs to repair Web sites damaged by hackers or equipment failures, and costs of rebuilding other lost information. Thus, various security risks arising from a combination of issues warrants a closer scrutiny for assessment of an organisation's IT requirements in order to facilitate a secured financial transaction.

The potential legal issues are shown pictorially in the following diagram.

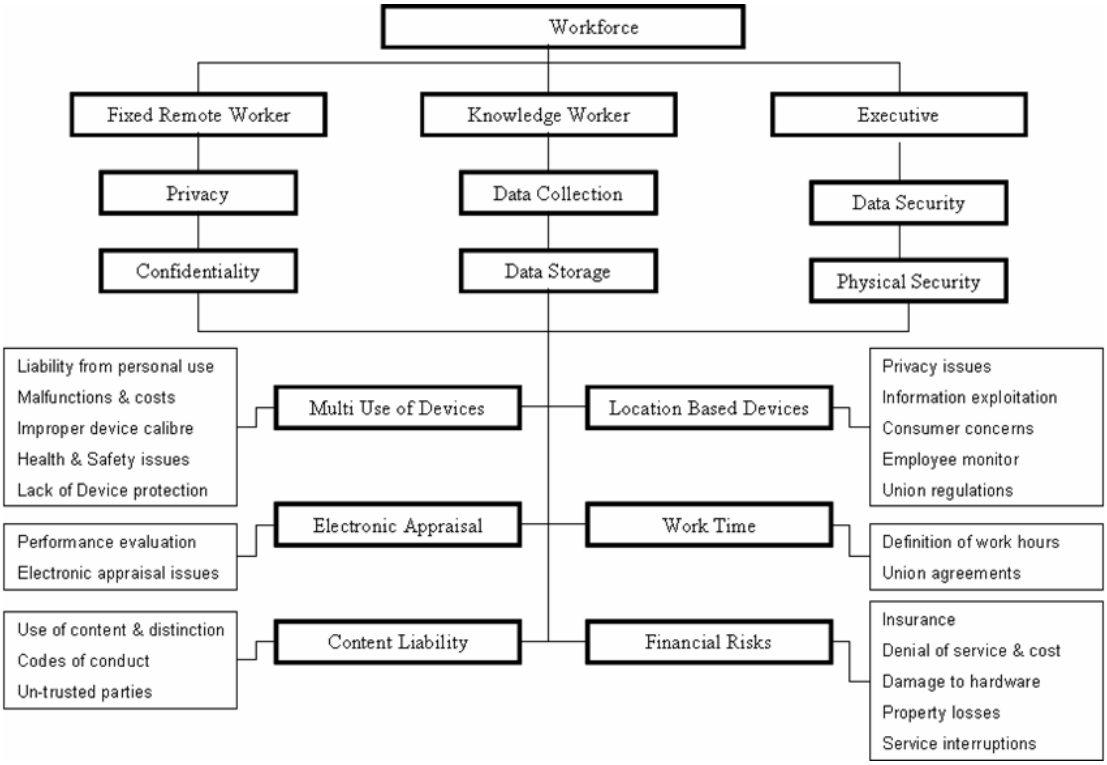

Figure 1: The Mobile Workforce Legal Issues and Risks

Risks discussed above, while recognised by organisations, are not uniformly dealt with in the international domain. For example, denial of service losses does not end up in financial compensation. In certain cases, court battles are waged to claim customer benefits that resulted from denial of services. Health and safety issues are dealt with differently in various domains and depending upon union negotiations, compensations may also vary. Organisations should be aware of these different regulations in order to save time and effort.

While the above paragraphs portray the potential legal problems, how to mitigate these risks is of interest to organisations. The following section provides a discussion on risk mitigation strategies.

OTHER ISSUES - Environmental issues

According to http://www.firstmonday.org/issues/issue8_8/critical/, there is a necessity to consider environmental issues of wireless technologies as these have profound implications on societies. It appears that developed countries where wireless technology is matured, have fewer regulations that can be enforced. According to this source, a recent report from INFORM, *Waste in the Wireless World: The Challenges of Cell Phones,* calls attention to the hazardous materials used in the phones and batteries including arsenic, antimony, beryllium, cadmium, and lead. This report indicates that rhetoric is shifted from the concept of "disposable" to "recyclable," by the manufacturers as the dangerous materials from the mobile devices are dumped into our soil and water.

OTHER ISSUES - Health issues

The health hazard to consumers is also discussed by this web source highlighting the impact of wireless technology on the body. The source highlights that the increase in use of different devices will result in interference of radio frequency problems. In some hospitals in Scandinavia, cell phones are banned because they have caused ventilators, defibrillators, and dialysis machines to fail. This source also reports that wireless devices have adverse effects on humans as there is evidence to suggest that the effects of wireless antennas is a cause for genetic damage in human blood.

ACTIONS TO MITIGATE RISK

The first issue that is of interest to organisations in mitigating risk is the 'remote workplace'. In addition to a number of technical and management issues highlighted in this area, an emerging issue is the non-compliance with local health and safety regulations. For instance, organisations may not have direct control on the remote user because of the remoteness of the user. Certain simple actions such as providing the employee with written advice about how to set up his/her home office may protect an organisation from any potential legal complication. Organisations can extend the insurance policy for the employee to include coverage for the home office issues. While the concept of extended insurance is not new (certain executives in countries like India are automatically covered for their home office by organisations), organisational policies need to be reviewed to cover the Internet workforce operating from a remote location.

The second risk arises from the multi-use of organisational resources such as mobile phones for personal use and other uses. The risks emerging from these types of use include illegal private use, costs and privacy implications. Organisations need to carefully review their policies and make employees to sign an agreement of compliance with these policies. It may be a good idea for organisations to review their fiscal policies and union agreements to address issues arising from the multi-use of organisational resources for private use.

In terms of location-based services, especially in the mobile commerce area, risks include privacy issues and surveillance. Organisations may benefit by classifying services and any privacy impact on those services in order to educate them. It is recommended that organisations continuously monitor only

risk areas and agreements with unions in this regard will ensure smooth operating environment. Other location-based services should be monitored only for the purpose of communication and not for policing the employees.

In the context of electronic appraisals, agreement with unions will ensure that the employee resistance is minimised by employees. One side effect of this method is the possibilities of issues arising from data protection laws. How do organisations plan to keep the appraisal data protected? Clear organisational policies are needed in this regard. If the policies are not clearly formulated, there will be problems from unions and the entire issue will be come sensitive.

Risks with work time issues involve possible conflict with work time laws and union agreements. Organisations may wish to employ contract employees to avoid sensitive issues here, however, this is not the correct solution. Again, organisations need to understand employees' work patterns and should device proper formula to accommodate changing work practices.

Finally, with content and access issues, possible risks arise from recent changes in privacy laws in various countries. While it is difficult to dictate employees as to what can be discussed and accessed using mobile technologies, it may be a good idea to have appropriate education and training to highlight the sensitive issues involved with content and access of information using mobile technology. An external person may be brought in to provide training and impart necessary knowledge to highlight the risks involved. In Australia, certain corporate sector organisations use an external person to highlight the risks involved in the improper use of emails to their employees and this process appears to be working well in minimising the improper use and access of email communication.

IMPACT OF REGULATIONS ON THE WIRELESS WORKFORCE

In Australia, 'flexible work arrangements' are recognised by many state governments and organisations to reflect the diverse needs of employees. One main issue addressed by this 'flexibility' is home based work recognising the fact that certain group of employees work greater 'out of hours' with the use of computer resources such as real estate agents. In Australia, regulations state that employees are provided with a safe working environment (by organisations) in accordance with the Occupational Health, Safety and Welfare Act, 1984. This Act states that the employer has the same obligation (as far as practicable) when the place of work is also an employee's home.

In this context, a number of issues impact organisations. For example, in Western Australia, an organisations' mobile workforce need to comply with these regulatory issues. Some general issues that come to one's mind are security of computer equipment and insurance policies. How does the organisation plan to control these two? To be effective, organisations need to hire 'inspectors' to ensure that home office is properly established and according to government standards. This will cost money and on occasions, may cost more than the revenue generated from home-based activity.

Another concern for organisations is the issues of reimbursement of expenses. For instance, the Internet workforce would use own computing equipment to conduct business from home after office hours. Organisations may need to reimburse expenses incurred by this Internet workforce. These expenses may include security to home office,

insurance charges, access to home office and use of communication equipments such as modems. Clear policy is urgently needed to address these issues.

In addition to these issues, management should consider policy making with regard to the issues mentioned in this paper: multi use of devices, location-based services, electronic appraisal, work time and content and communication liability. Employees of the Internet workforce should be educated to keep time records as some of them may claim over-time salary. Employee performance agreements should acknowledge work conducted from home. While current performance indicators are based on departmental performance system, in many organisations, work conducted from home or work done at home is not fully recognised. In the case of organisations this may become an important issue because many organisations in Australia operate from home premises.

Finally, the question of 'job characteristics' needs a new form of definition to accommodate a Internet workforce as more and more organisations will use the emerging mobile devices to conduct their daily businesses. The job characteristics should include the following:

- High degree of intellectual capability;
- Clear definition of areas of individual work;
- Work that has performance measurement indicators; and
- Work that does not need frequent input from other staff or central facilities.

BRIEF SURVEY OF CURRENT STATE OF LAW

A survey of various regulatory frameworks indicate that there are no specific provisions in Australian and New Zealand privacy legislation regarding the location aspects of wireless technology. Some telecommunications legislation covers inappropriate disclosure of location information regarding use of mobile phones. In Europe some states are moving towards explicit coverage, extending the general protection under the EU Data Protection Directives. UK data protection legislation does not privilege 'location' as one of the categories of 'sensitive' information However, there are some limits on disclosure under UK telecommunications legislation. In the US the Wireless Communications & Public Safety Act of 1999 (aka 911 Act) makes specific provision for "wireless location information privacy" regarding a telecommunication carrier's use and disclosure of customer proprietary network information (CPNI). 'Location' forms one of sensitive categories of data that require protection by carriers: apart from emergencies they are forbidden from accessing, using or disclosing wireless location information "without the express prior authorization of the customer".
(http://www.caslon.com.au/privacyguide19.htm)

CONCLUSION

Exploiting the flexibility of a workforce to achieve organisational objectives requires a number of trade-offs. Some of the trade-offs include current regulatory and union-related constraints in addition to assessing the enterprise's liability for employee misuse of devices, tools and processes. Organisations should follow these tactical guidelines in conjunction with obtaining legal counsel

to assess their exposure to different categories of liability, set policies and enforcement processes, and minimise risk. If this is not done properly, then organisations may find it difficult to properly manage a workforce that uses new technologies.

REFERENCE LIST

Andrews, W. (2001). *Portals and E-Commerce: Different Goals, Parallel Projects* (No. COM-13-6391): Gartner.

Cox, T., Griffiths, A., & Rial-Gonzalez, E. (2000). *Research on work-related stress*. Luxembourg: European agency for safety and health at work.

Craig, J., & Julta, D. (2001). *e-Business Readiness: A Customer Focused Framework*. Boston: Addison Wesley.

Davis, R. (2002). Pursue front end solutions to revenue problems. *Healthcare Financial Management, 56*(8), 30 - 36.

Deitel, D., & Deitel, N. (2001). *e-Business and e-Commerce - How to program*. New Jersey: Prentice Hall.

Dixon, P. J., & John, D. J. 1989. Technology issues facing corporate management in the 1990s. *MIS Quarterly, 13*(3), 247 - 255.

Dyer, O. (2003). Patients will be reminded of appointments by text messages. *British Medical Journal, 326*(402), 281.

Freeman, E. H. (2003). Privacy Notices under the Gramm-Leach-Bliley Act. *Legally Speaking* (May/June), 5-9.

Gururajan, R. (2001). *Wireless Applications: Influences and Risks of Location Identification Technologies.* Paper presented at the Australian Conference on Information Systems, Coffs Harbour, NSW.

Kuechler, W., & Grupe, F. H. (2003). Digital Signatures: A Business View. *Information Systems Management*(Winter 2003), 19-28.

Leung, H. (2002). Organisation factors for successful management of software development. *Journal of Computer Information Systems, 42*(2), 26-37.

OECD. 1999. Implementing the OECD job strategy: Assessing performance and policy.

Redman, P. (2002). *Wait to Invest in Next-Generation Wireless Services* (Research Note No. T-15-2354): Gartner Research.

Rozwell, C., Harris, K., & Caldwell, F. (2002). *Survey of Innovative Management Technology* (Research Notes No. M-15-1388): Gartner Research.

Simpson, R. L. (2003). The patient's point of view -- IT matters. *Nursing Administration Quarterly, 27*(3), 254-256.

Smith, D., & Andrews, W. (2001). *Exploring Instant Messaging*: Gartner Research and Advisory Services.

Sparks, K., Faragher, B., & Cooper, C. L. (2001). Well-Being and Occupational Health in the 21st Century Workplace. *Journal of Occupational and Organisational Psychology, 74*(4), 481-510.

Stevenson, S. (2001). Mobile computing places data in the palm of the hand: Devices deliver real-time access to information. *Ophthalmology Times, 26*(4), 15 - 18.

Tang, L. K., & Cheung, J. T. (1996). Models of workplace training in North America: A review. *International Journal of Life Long Education, 15*(4), 256-265.