# Emergence For The Need Of New Legal And Regulatory Issues For Mobile Workforce

**Raj Gururajan, The University of Southern Queensland**

## Abstract

Many CEOs and enterprise executives are interested to gain insights into existing and emerging legal frameworks for Mobile workforce. The main objective of gaining such insights is in order to develop enterprise's management strategies as these legal frameworks have profound impact on organisations. In recent months, the behaviour of the workforce has come under scrutiny because of the increased usage of mobile devices. As these devices provide mobility to the workforce, they remove the distinction between private and professional workplaces. For example, employees use organisational resources such as laptop computers at home for their private use. Due to 'globalisation', workforce is made to switch roles between private and professional lives with short lead time according to various conditions such as differing time zones dictated by external conditions. The mobility and flexibility offered by the mobile devices facilitate the current workforce to adapt their work styles according to these external conditions. These 'flexible' aspects have forced enterprises to support their mobile 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 and depend upon varying legal frameworks, economic conditions and cultural attitudes. This paper provides a theoretical framework on these emerging legal and regulatory issues specific to mobile workforce.

## Keywords

*Mobile workforce, wireless technology.*

## 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 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).

Due to these changes in the workplace, 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[3] exist for workplace agreements, issues concerning employee contracts, long service leave payment and for wages and conditions. These regulations comprehensively detail workplace agreements between employees and employers, details concerning minimum employment conditions, state legislations governing labour relations and better practice for small businesses.

While these issues are regulated in the context of physical work environment, the relevance of those regulations to an extended workplace, such as a mobile work environment, is currently under researched. For example, some devices used by mobile employees have raised worries for possible health hazards in recent months (Simpson, 2003). These hazards are more likely connected with their use rather than the device itself. One example is the possible lethal consequences of using a mobile phone while driving a car or crossing a street. Therefore, it is necessary to introduce new regulations to avoid any potential damage to public, employees and organisations. This paper builds a theoretical framework on the need for the emergence of new regulations to address issues arising from the mobile workforce.

The objective of this paper is to establish the importance of regulatory issues applicable to a mobile workforce as limited details can be found in the existing literature applicable to the use of wireless devices.

## Anatomy of Mobile Workforce

Employee well-being has been studied for over 40 years covering aspects from working conditions to wages. Contractual issues associated with employment are studied by OECD and their impact on countries has been reported (OECD, 1999). Literature also reports on patterns of working days, self-regulated hours and reliance on computer technology (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 (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).

The current penetration of mobile devices has given rise to the classification of mobile workforce and a mechanism to identify such a workforce. Currently, mobile devices are used by workforce to access organisational data. A close examination of the usage of mobile devices shows that workforce relies on mobile devices to (a) remotely access organisational data, (b) gather information or knowledge needed to conduct one's work and (c) executives using their mobile telephone and computers fitted with wireless protocols to communicate with others for decision making purposes (Rozwell et al., 2002). In essence, the entire workforce that relies on the mobile devices

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

can be loosely classified 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 mobile devices, namely, (1) fixed remote worker, (2) knowledge worker, and (3) executive with access to mobile services. Each of these is now discussed in detail.

A fixed remote worker is characterized by a desktop in the office or at home as a predominant tool. This desktop may be connected to various devices using a home wireless network or wireless access at the office. This worker typically accesses emails and other data by remote access using the Internet. A major concern with this type of worker is associated with data and how to integrate the data with corporate databases. 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 complex. The tools used by this worker include notebooks, PDAs and mobile telephones. 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 with access to mobile services travels by road or air and this access is 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, location identification devices associated with mobile devices also are important to this group because of potential security threats based on location identification (Gururajan, 2001).

The three categories and their characteristics are summarised below in pictorial form:

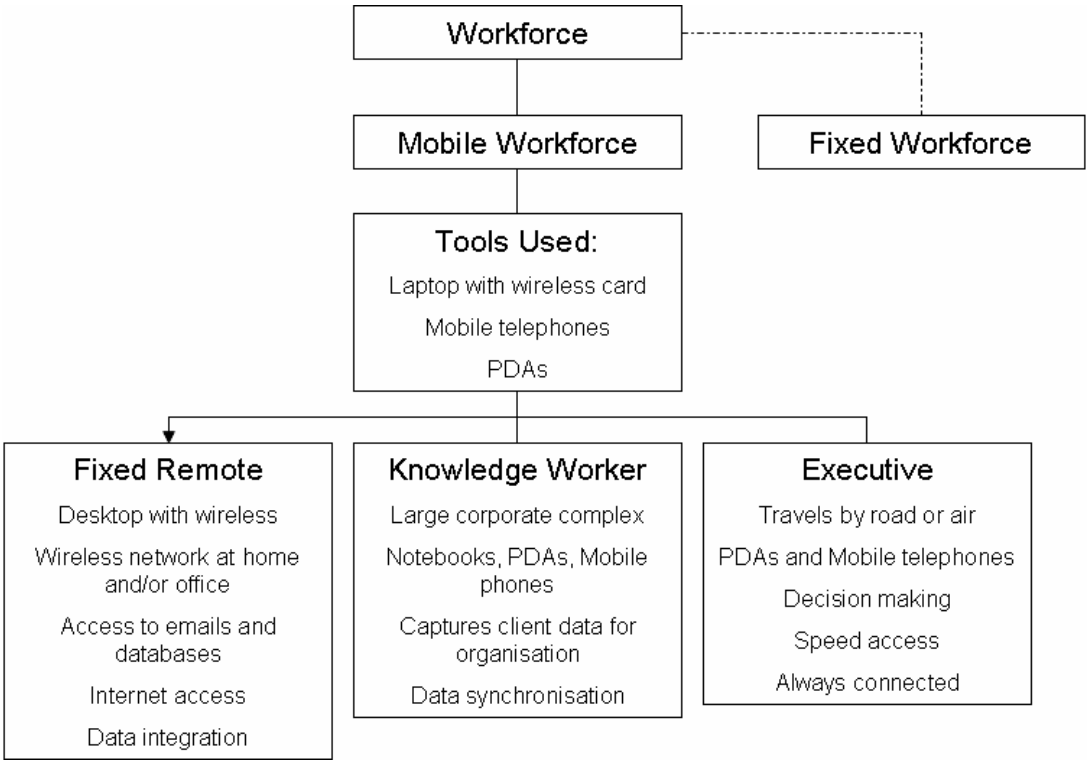


**Figure 1: An initial anatomy of mobile workforce**

## Content AND Access using wireless devices

Common to the three types of worker is a set of mobile devices, primarily consisting of a notebook with wireless access, a mobile telephone and a PDA (Smith & Andrews, 2001). The three groups of mobile workforce use these three dominant platforms for both content creation and content access. The content creation involves initiating a simple conversation for data gathering purpose. The content access involves accessing different data repositories to verify either client data or organisational policies. In the total system of wireless access, the content creation is the input, the data access is the process and the output realised by the workforce is the work produced. This process is shown below in detail.

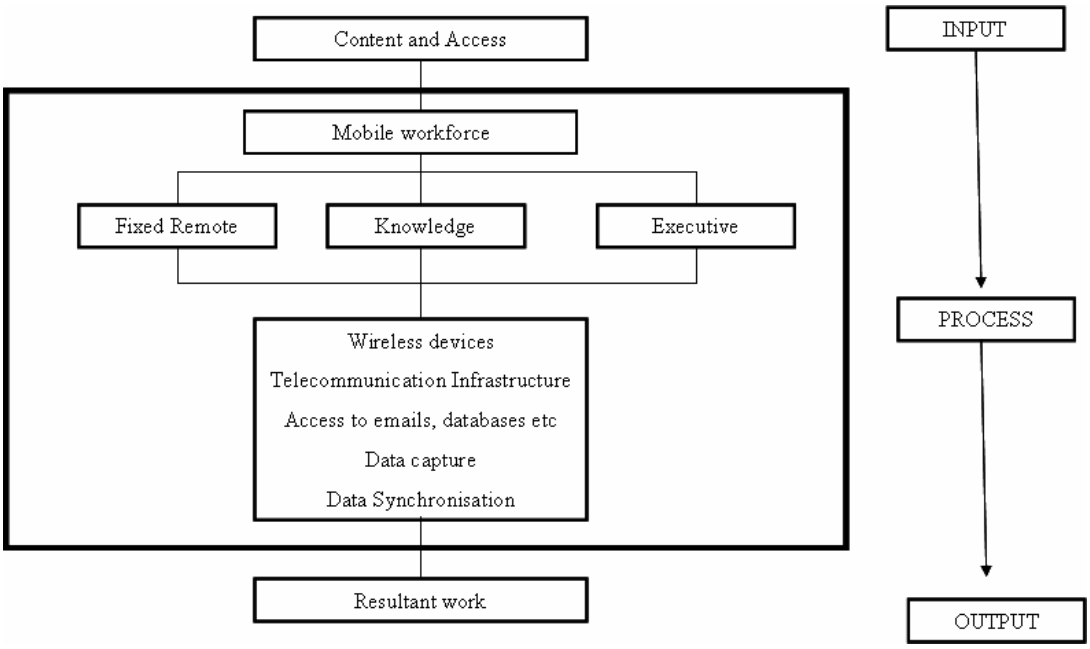


**Figure 2: The process of content and access using mobile devices by mobile workforce**

The mobile device set is the facilitating platform as these devices operate on a telecommunication network operated by the service provider. Competition for the role of primary client device has come predominantly from the mobile phone sector, but remains limited to voice and short-message service (SMS) messaging (Dyer, 2003). According to Gartner Research, data access is one of the major promises of Wireless Applications. While data access is restricted to limited services in the current climate, issues arising from these data accesses by the three work groups need urgent consideration.

## Organizational Challenges

Recent development in the area of wireless protocols has seen the emergence of wireless capabilities in the office. Wireless networks in the office are currently being driven by the emergence of the Institute of Electrical and Electronics Engineers' (IEEE's) 802.11b wireless LAN (WLAN) specifications as an initial standard. This technology allows knowledge workers to access corporate data from any location within their normal work environment. The impact of this access is the capability of enterprises to have a workforce that is connected always. For example, a number of studies in the past have singled out the email application as the most used Internet 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 wireless devices using emails with corporate databases and this will provide the most needed data access (Leung, 2002). This has prompted enterprises to invest in WLAN to reap the benefits of productivity gains.

Further, costs have now declined, interoperability is much better and access is faster - ensuring that WLAN can easily give enterprises a competitive advantage (Stevenson, 2001).

While the mobility offers flexibility, organisations find it difficult to justify the total cost as ownership is very expensive (Redman, 2002). For example, due to rapidly changing wireless technology, devices and telecommunication network protocols may become obsolete quickly. Organisations need to maintain this infrastructure in order to realise high levels of output from their workforce. To achieve this, organisations need to redefine the corporate network structure to include up-to-date wireless infrastructure. The cost for such update may be beyond the traditional capabilities of an organisation as there may be considerable delays in the Return on Investment or ROI (Davis, 2002). Therefore, currently mobility has been restricted to the office because of the cost involved in providing surplus fixed-access points to facilitate additional network connections. It appears that organisations have not yet found a compelling reason to justify the investment and hence are reluctant to invest in this direction.

Despite the advantages offered by technologies such as WLAN, 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 wireless requirements carefully in order to satisfy the needs of their workforce.

## Wireless Technology Relevant to organisations

The following types of technology (grouped under the type of network required for connectivity) are currently considered the most important:

- A wireless personal area network (WPAN) for wireless transmissions such as radio or infrared instead of telephone lines or fibre optic cable to connect data devices. This is becoming popular at home office level due to the desire to avoid cumbersome wire connections. The main objective of installing a WPAN is mobility and flexibility offered to users. Further, by having such a technology, users can connect many devices to one central hub and access the Internet and share other resources.
- Bluetooth[4] is an ad hoc, wireless interface with speeds of up to 1 Mbps and a range extending to 30 feet. Its primary functions are to normalize the data sets of multiple devices through synchronization and ad hoc device networking, including access to network peripherals. This technology has improved so much in the past two years with range extended to 100 ft. This technology is now commonly found in personal devices such as video cameras and users enjoy the wireless connectivity to transfer pictures and files from one device to another.
- A WLAN is a high-speed LAN solution that supports speeds of up to 45 Mbps and a range of 300 feet. This is typically essential for 'roaming'. Organisations are keen to install WLAN as an alternative to avoid problems encountered in establishing wired networks. However, due to physical

[4] Bluetooth is a mobile communication protocol

barriers such as thick walls etc., WLAN may not reach all users with optimal signal strength, meaning that the transmission rate may not be the same to all users. Further, security becomes a key component as many implementations do not configure their WLANS with proper encryption options, leading to security loopholes.

- IEEE 802.11b: The IEEE's standard for WLAN interoperability is perhaps the most widely accepted standard at industry level and is gaining popularity due to its neutral view. In the current climate, fast data transmission of up to 11 Mbps is possible. Mobile users can get Ethernet levels of performance, throughput and availability.
- A wireless WAN (WWAN) includes multiple voice/data technologies, such as GSM[5]. This is essential as the mobile workforce integrates both data and voice. Software applications that can convert voice data into text data for transcription and analysis are emerging in the market to facilitate integration of data and voice onto one device. A WWAN typically has a range of about three miles.
- SMS: electronic messages on a wireless network. While this technology is popular among young people, due to the difficulty encountered in entering the text using 'thumb' keys, some professionals find it difficult to use. However, with provision to attach keyboards to mobile devices, SMS is an alternative to voice messages.
- General Packet Radio Service: a "second-and-a-half-generation" technology being implemented in GSM networks that may offer wireless data access speeds of up to 144 Kbps in end-user devices. Some organisations use this service to communicate with their remote workers.
- Multipoint multi-channel distribution service (MMDS): a wireless technology used for broadcasting, personal communications and interactive media services. Organisations and some community networks use this concept for broadcasting. This technology is used to provide specific services to residents or employees as an alternative to free-to-air television services.
- Satellite: a wireless device that uses a mobile satellite service to send voice and data. This is also used with some location identification devices to establish coordinates of an entity. This is becoming popular at home recreation level, including fishing.

Organisations use a combination of these technologies to match the needs of their mobile workforce. Depending upon the usage based on frequency of data access and the level of mobility, organisations choose types of these technologies suitable to their needs. The following diagram is adapted from Gartner Research to depict this. Gartner uses the term 'campus worker' for knowledge worker used in this paper and 'road warriors' for executives. While it is possible to argue on the appropriateness of the terms used in this paper, no attempt is made to justify the term 'executive' in this paper as many Australian executives use PDAs as an alternative to notebooks that they carry. The main reasons for this is the introduction of 3G networks and devices in the past 12 months in Australia, and the capabilities of these PDAs to accommodate office systems, schedulers etc.

[5] Global System for Mobile Communications

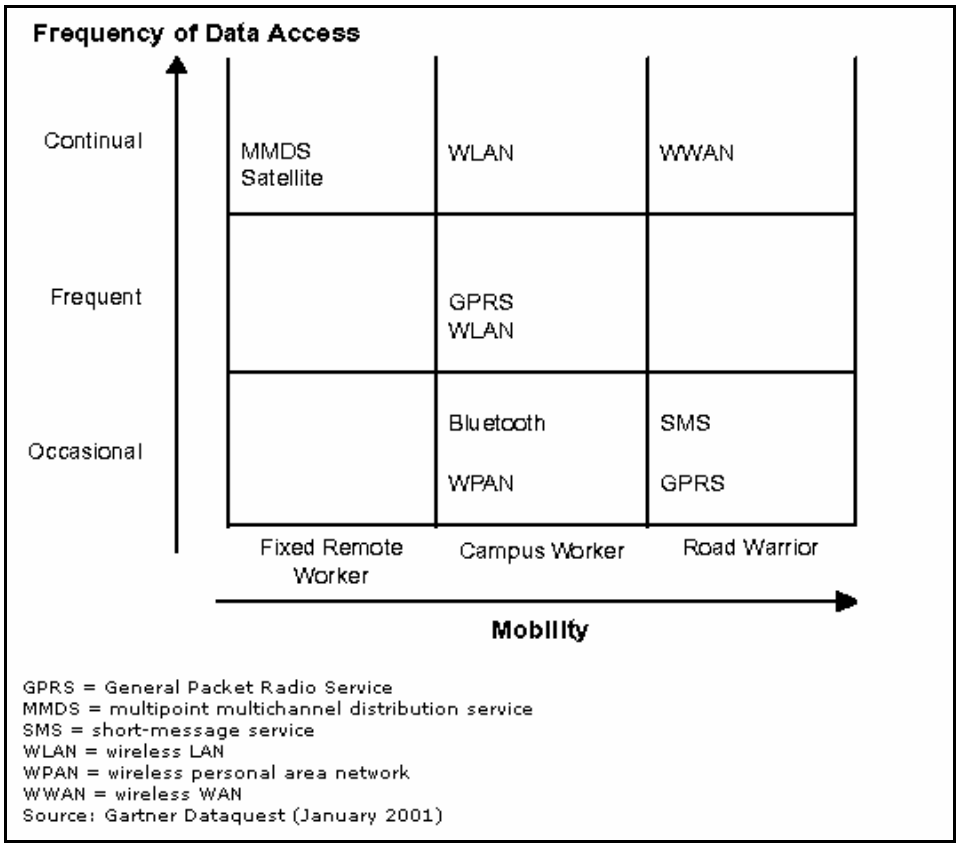


**Figure 3: Gartner's View**

From the above diagram, it can be seen that the fixed remote worker could continuously accesses data using MMDS and Satellite technologies. The mobility of this worker is low. On the other hand, the executive type uses GPRS and WWAN for data access with a high frequency and mobility. From the description of the technologies provided, it can be seen that the mixed type of technologies is essential to satisfy the needs of these three groups of workforce.

The knowledge worker could use Bluetooth for occasional mobility and frequency. As mentioned, Bluetooth is capable of addressing 'ad-hoc' needs and hence the knowledge workers might find this technology appropriate for their needs. Similarly, the use of WPAN using radio frequency or infrared by knowledge workers for occasional use indicates the selection of their choice for a particular technology.

When this concept is mapped onto the categorisation of mobile workforce provided in this paper, it is possible to predict the type of technology that would be used by the three workforce groups. Further, if we integrate the toolset used by this workforce with this mapping, it is possible to predict the wireless needs of this workforce. An initial attempt to view the hardware needs and relevant technologies is portrayed in the following picture.

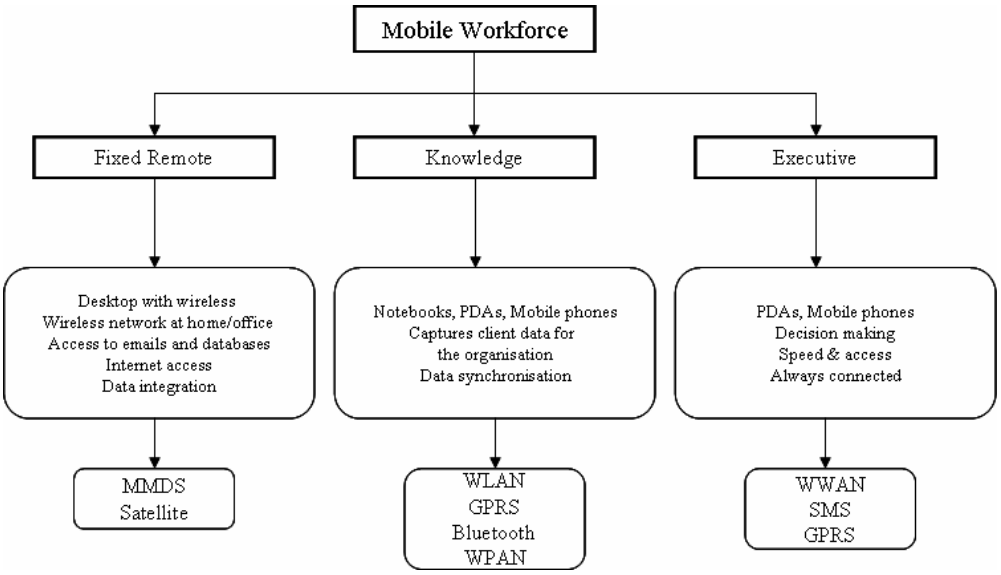


**Figure 4: Mapping of workforce, hardware and wireless technologies**

The availability of hardware devices and the flexibility offered by wireless technologies provide mobility to the workforce. However, it appears that this workforce is not fully aware of the potential legal issues and risks that can emerge due to the misuse of wireless devices. Further, organisations supporting their mobile workforce appear to either ignore potential risks that can emerge by not following requirements stipulated by governments and unions or are not aware of changing policies in this area. The following section is an attempt to highlight such potential legal issues and risks.

## Mobile Workforce Legal Issues and Risks

A key element for an organization is the ability to manage its mobile 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 mobile 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 Mobile Devices

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. 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 calibred accurately may transmit the wrong location coordinates 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. Organisations should be aware of issues associated with consumer protection and employment laws. Currently there are no uniform laws to address these issues and these are taken care of by contractual negotiations (Freeman, 2003; Kuechler & Grupe, 2003).

## Location Based Mobile Services

Location based mobile devices identify a person based on their location. Due to changes in the privacy policy, considerable privacy concerns are raised by the use of these devices. A key asset of mobile services is exploiting information about where a specific user is located when the service is requested. This asset is now exploited in the marketing segments. As far as enterprises are concerned, the data arising from the use of such location based technologies and service is less-sensitive in terms of employees' movements. However, for customers and consumers this may become very sensitive as the technology discloses the location of these people. In certain cases, these customers would like to uphold the anonymity of their locations. Therefore, legal issues associated with privacy legislation need to be understood by organisations before executing certain options for data collection using location identification technologies (Gururajan, 2001).

There is another concern for organisations in terms of employee locations. Organisations must consider that the ability to continuously monitor an employee's location may not be well received, especially for multi-use devices. Even when the location-finding function can be switched off, employees may feel compelled to disclose their location, which can create potentially contentious situations, especially in highly unionised enterprises and sectors. On the other hand, readily locating the workforce is very important for an organisation (Deise et al., 2000).

## Electronic Appraisal

The advent of wireless applications facilitates employees to move away from their fixed location and provides abundant freedom. Employees' mobility and their freedom from enterprises' physical premises suggest that employers should make greater use of technology for performance assessment. 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

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. When it comes to 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). Currently the union agreements are not addressing these issues satisfactorily.

## Content and Communication Liability

One of the greatest advantages of 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[6] 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

Today, most organisations rely on computers for their daily operations. Traditional risks and non-traditional security risks can interrupt a business or literally shut it down. For example, a security breach by a hacker can severely disrupt a business and those that depend on it. Most businesses using mobile devices 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 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

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

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 mobile 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, mobile commerce 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 commerce, 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, for example 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 area, 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.

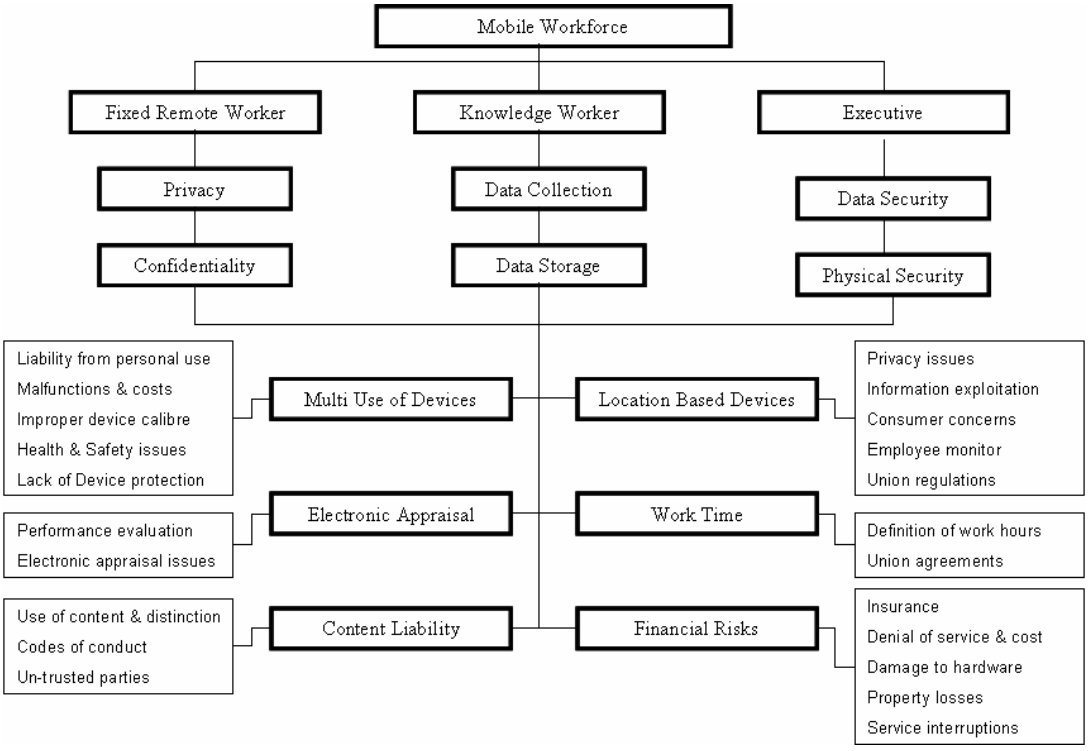


**Figure 5: Mobile Workforce Legal Issues and Risks**

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 paragraphs provide a discussion on risk mitigation strategies.

## Actions to Mitigate Risk

The first issue that is of interest to organisations 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 mobile 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 mobile 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, a mobile workforce controlled by an organisation needs to comply with these regulatory issues in Western Australia. 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, mobile workforce would use own computing equipment to conduct business from home after office hours. Organisations may need to reimburse expenses incurred by this mobile 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 mobile 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 mobile 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.

## Conclusion

Exploiting the flexibility of a mobile 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.

## References

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 Readyiness: A Customer Focused Framework*. Boston: Addison Wesley.

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

Deise, M. V., Nowikow, C., King, P., & Wright, A. (2000). *Executive's Guide to e-Business: From Tactics to Strategy*. New York: John Wiley & Sons, Inc.

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.

# Enhancing Competitiveness through Innovation: Issues and Implications for Industrial Policy-Making

**Andrew L S Goh, Department of Management, Birkbeck College University of London, United Kingdom**

## Abstract

Developing nations aspire to attain higher levels of economic prosperity and to eventually achieve developed nation status. While they have enacted industrial policies with the objective of stimulating and sustaining the economic progress of their countries, the burning question remains: do these industrial policies enhance the competitiveness of industries and firms? It appeared that policy critics, industrial economists and public policy researchers are in support of pro-innovation industrial policy; and that it will enhance economic competitiveness and hence foster industrial growth. Yet, as to whether developing nations such as Singapore have succeeded in promoting innovation through industrial policy-making or not, some lessons can be learnt from the developed world. This paper provides evolutionary perspectives of industrial policy-making in relation to how it had helped build Singapore to its current state of development. It also sheds light, with a study based on ex post facto information collected from 104 Singaporean firms, to put in the right perspective the importance of pro-innovation industry policy. Finally, it discusses the implications for Singapore's industrial policy-making and the future challenges of industry policy.

## Keywords

*Industrial policy, innovation, policy-making, innovation-driven economy, industry growth, pro-innovation industrial policy and economic competitiveness.*

## Introduction

Insofar as industrial policy-making is concerned, all nations of the world are now undergoing a trying time. No countries are spared from the new challenges of economic development arising from the changes in labour productivity, industry structuring and international trade. These new challenges have placed unprecedented strain on industries to remain fiercely competitive. With the global gloom in the last five years considered to be one of the most dismaying economic downturns ever encountered in recent history, it has prompted a re-think of industrial policy-making. Even though political leaders, economic analysts and businessmen share the same