This is a reprint from a paper published in the Proceedings of the IADIS International Conferences
IADIS,http://www.iadis.org

LEGAL REMEDIES FOR SECURING THE MOBILE ENTERPRISE

Elaine Lawrence
University of Technology Sydney
PO Box 123 Broadway NSW 2007 Australia

John Lawrence
(Barrister-at-law)
King Street Chambers Sydney NSW 2000 Australia

ABSTRACT

The Mobile Enterprise must be alert to the potential threats posed by hackers, virus and worm writers as well as warchalkers and wardrivers and take steps to secure itself. This paper reviews the impact of attacks on the wireless and networked communication systems in a legal and security context with a view to formulating technical and legal policy suggestions for technologists, scientists, managers and government policy makers. To assist in addressing these problems, the researchers present a modified Mobile Enterprise Security and Legal (MELS) Framework, which has been revised for this paper. It is adapted from the Network Security Wheel, the Confidentiality, Integrity and Availability (CIA) Security model and sets out four legal questions that must be addressed if the enterprise is under attack. This paper outlines the types of threats that impact on the mobile enterprise and illustrates the reactions from international and national legal communities.

KEY WORDS

mobile, enterprise, legal, security

1. INTRODUCTION

The impending explosion of disruptive technologies, particularly Wireless LAN (WLAN) options (including the availability of Wireless Broadband in an unregulated spectrum), and ubiquitous mobile technologies, justifies consideration of the likely effectiveness of current legal remedies, given the global harmonization initiatives in progress. The exponential growth of wireless technologies has meant increased security risks, such as hacking and the improper uses of network resources (Cisco Academy Connection, 2004). These attacks could exploit the 802.11 family (802.11x) Wireless Local Area Network (WLAN) security technology standards. The 802.11g protocol suffers from the same security risks as 802.11b and even though the 802.11i standard promises to minimize these risks, it is too early to tell. Companies may not implement all the security features of the WLAN. For example, the network administrator may not change the default administrator passwords on all the equipment during setup, thereby allowing hackers easy ingress to the WLAN. In April 2004, Cisco issued an advisory alerting customers that a hard coded, non-removable user names and passwords in some versions of its Wireless LAN Solution Engine and Hosting Solution Engine software could give attackers complete control of the devices (Roberts, 2004). Cisco warned that malicious attackers using the default username and password could:

- hide insecure wireless access points (called Rogue Access Points) on wireless LANs to gather confidential information from the WLAN;
- create and modify user privileges;
- change configuration settings;

- cause system wide outages by change the radio frequency used to send data over the WLAN;
- redirect traffic from a Web site hosting e-business or m-business services (Roberts, 2004).

If companies do not put in place adequate usage policies and employees set up their own insecure Access Points to the network (Cisco Academy Connection, 2004), the company would have no basis to discipline the offending employees. The security of Wi-Fi and other wireless networks is an area of coming litigation (LexisNexis, 2003) and the risks and the concomitant legal issues are the subjects of this paper.

This paper investigates, by examining cases, international and national government legislation and rulings, the interaction between mobile and/or networked enterprises and the law with reference to security issues. It firstly provides an overview of what is happening in the wireless and networked space, such as virus and worm attacks including cryptoviruses, metamorphic worms, snarfing, warchalking, wardriving (set out in Section 2), and the response of the law. The next section outlines the research methodology and the amended Mobile Enterprise Legal and Security (MELS) Framework as set out originally by Lawrence and Lawrence, (2004) while the final sections discuss the jurisprudence analysis of the legal issues. Finally the paper concludes by pointing the way to future research.

2. DEFINITIONS AND ISSUES

In a mobile environment it is necessary to establish communication among mobile, spontaneously networked peers such as PDAs, mobile phones and laptops without any centralized coordinating authority. Schoder and Fischback (2003) believe that peer-to-peer (P2P) could gain importance with the development of mobile business and ubiquitous computing. Many enterprises, whether they suffered as a result of the dot.com crash of the year 2000 or not, are now taking tentative steps towards transforming themselves into mobile and/or networked enterprises. However these enterprises find themselves being attacked by people who are attracted to the possibility of being able to hack into a wireless enterprise. In fact many pundits claim it will not be long before mobile phone viruses appear (Thompson, 2004). Definitions of the potential problems are now presented.

A cryptovirus is malware that encrypts files on a user's device, making them unreadable. The virus uses a public key generated by the virus author to encrypt data that resides on the host system and is survivable as the virus can only be removed by the virus author who has the private key. Such an attack could:

- extort information
- be used as a tool for espionage or information warfare
- encrypt electronic money
- be used to demand a ransom from businesses for decrypting the files by supplying the private key (Young and Yung, 2003).

The user would be a victim of extortion – the user may pay ransom and retrieve the data, refuse to pay the ransom and lose the data or ignore the ransom demand if a backup exists (Young and Yung, 2003).

Metamorphic worms are able to alter their appearance so radically that antivirus companies are not able to recognize that they are malware (Thompson, 2004). These worms use strong encryption and change their pattern every time they run so researchers may take days or weeks to examine the worms and write cures (Donovan, 2003). The self-styled elite virus and worm writers are aware of the consequences of being caught by cybercrime experts so they have adopted the technique of 'publishing' their code and descriptions of how the programs work on websites. When the so-called script-kiddies (or aspiring hackers) release the code, the actual authors admit writing the code but deny setting it free on the networks. Security professionals and police consider the above as 'legally precise but morally corrupt' (Thompson, 2004). Snarfing attacks enable intruders with Bluetooth devices to capture documents, contacts and other information from other Bluetooth enabled phones by exploiting a security flaw in the wireless protocol (Wright,2004). The snarfer is able to:

- send text messages
- initiate calls
- obtain personal phone book entries without requiring user interaction

Austrian researchers at the 2004 Hanover CeBIT fair were able to sniff out 1296 Bluetooth devices using a notebook and 2 Bluetooth dongles (Wright, 2004). The legal jurisprudence analysis is set out in Section 5.

Wardriving is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. Wardrivers require a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources. Some people have made a sport out of Wardriving, in part to demonstrate the ease with which wireless LANs can be compromised. With an omnidirectional antenna and a geophysical positioning system (GPS), the war driver can systematically map the locations of 802.11b wireless access points (www.whatis.com). Warchalking is the practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access. That way, other computer users can pop open their laptops and connect to the Internet wirelessly. It was inspired by the practice of hobos during the Great Depression to use chalk marks to indicate which homes were friendly (www.warchalking.org). Because chalk markings are temporary, warchalkers hope to avoid legal fines for defacing public or private property (www.whatis.com).

Wardrivers and warchalkers are accused of stealing bandwidth from the legitimate users and corporations (who provide and pay for the bandwidth) and compromising the security of a company's secrets. The mobile phone company Nokia labels it 'theft, plain and simple' (Standage, 2003) and warns that such hackers are reducing the amount of the valuable network resources available to the workers in that organization. Groups of warchalkers logging on together could slow down a company's whole network. Unprincipled spammers (war spammers) could use a network as a proxy to dispatch millions of unwanted e-mail messages anonymously, with no danger of being traced (Wearden, 2002). This ability would allow the spammer to avoid bandwidth costs, which can be substantial for huge quantities of spam e-mails. The anonymity is a useful tactic for those who (a) send spam as a service for other companies and/or (b) may have been in trouble with the law (Deakins, 2002). The Australian law firm Deakins (2002) reported that many of the hundreds of Wi-FI networks in Melbourne were insecure and only nominally protected by factory default passwords (Montcalm, 2003).

The National High Tech Crime Unit in Britain state that distributed denial of service attacks by organized crime groups are a favourite way of attacking online betting sites for example. Individuals sell or hire out their bot armies (compromised networks of systems for denial of service attacks) for specific attacks. Non-exclusive access to compromised PCs have been sold for $ US 500 for 10,000 hosts (Deats, 2004)

The following table illustrates sample business views on the issues discussed above.

Table 1. Sample views on virus, worms and warchalking

Phil Reitinger, Senior Security Strategist for Microsoft commenting on why virus and worm writers target Microsoft.	*To me, it's online arson (Thompson, 2004).* Company has set up $US5 million fund to reward people for supplying information that leads to the capture of writers who target Windows machines *(Thompson, 2004).*
Marc Rogers, former police officer who researches computer forensics, on virus and worm code writers.	*It's like taking a gun and sticking bullets in it and sitting it on the counter and saying'Hey, free gun' (Thompson, 2004).*
Peter Ferrie, Symantic's antivirus researcher	*More viruses and worms are installing some kind of back door that does things like steal passwords, log keystrokes or look for particularly sensitive files. Combine that with the fact that mass emailing is being used for replication and you get a widespread collection of compromised machines in a very short time (Braue, 2004)*
Head of e-business for Confederation of British Industry (CBI)	*The CBI condemns warchalking as an implicit incitement to irresponsible and illegal acts* (UK business, 2002).

3. METHODOLOGY

This paper follows on from previous studies on e-law and the technology of the digital economy undertaken by the researchers from 1997 –2004. The legal methodology is classical jurisprudence analysis which is the study of rules and regulations and case law to clarify these provisions which are recorded for the

communication of generalizations. The resulting synthesis is then provided as a summary of the situation (De Vuyst, 2002). Exploratory research is conducted into an issue when there are very few earlier studies that can provide information about the problem (Hussley and Hussley, 1997). The focus is on gaining insights and familiarity with the research area for more rigorous investigation at a later stage. This research was approached in two phases. First, a literature review was undertaken to understand and draw out the critical issues associated with WLANs in the Mobile Enterprise. Secondly the researchers carried out research on legal issues connected with the WLANs, Mobile Commerce and Internet Commerce (Allen, 2002), (Stanfield, 2003), (Fitzgerald and Fitzgerald, 2002), (Elliott and Phillips, 2004). The literature and law review and subsequent analysis of the issues and synergies drawn from these studies led to the proposal for the Mobile Enterprise Legal and Security (MELS) Framework which has been revised for this paper (Lawrence and Lawrence, 2004).

4. THE REVISED MELS FRAMEWORK

In all network environments the Security Wheel (BMB, 2003) is a useful visual tool to use and is particularly suited to the WLAN environment as is the Confidence, Integrity and Availability (CIA) Security model. The revised MELS framework is based on these two models and represented in Figure 1 and its relevance to legal issues is set out in Figure 2.

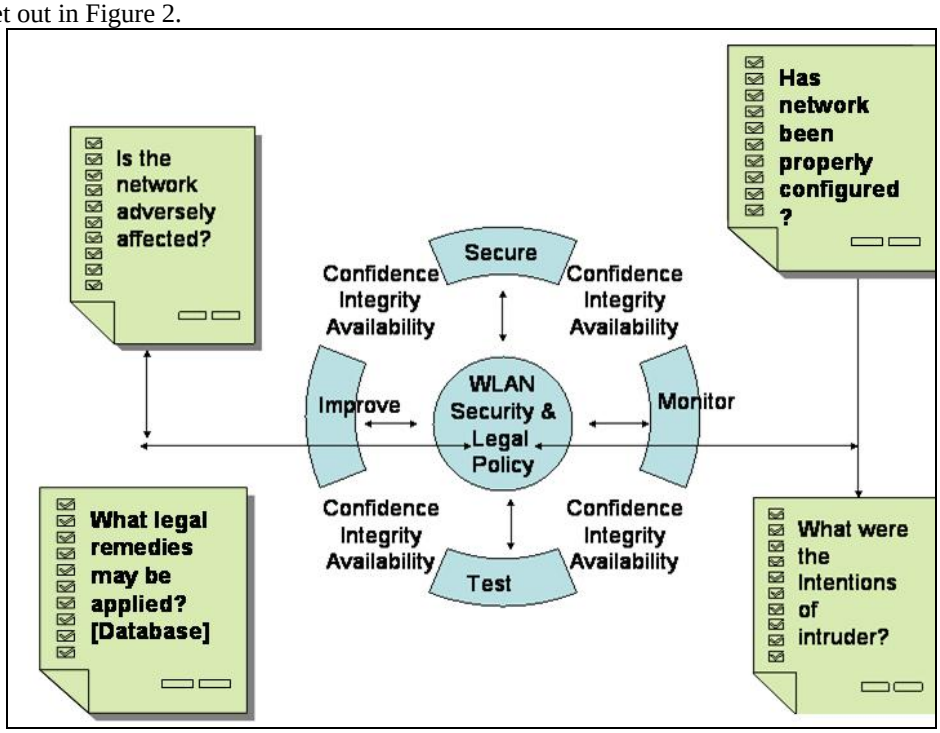

Figure 1. Revised MELS Framework (Sources: The Security Wheel (Sources: http://www.bmbgroup.com/dls/BMB_20Profile.pdf), and Montcalm, 2003))

At the core of the MELS framework is the need for a robust legal and security policy for WLAN management. This must be continually monitored, tested, improved and kept secure whilst ensuring that WLAN enjoys the users' confidence and maintains its integrity and availability. To assist the WLAN administrators' task of ensuring this strong policy is adequate, four questions concerning compromises to the WLAN must be answered when breaches occur namely:

- Has the network been adversely affected?
- Has it been properly configured?
- What were the intentions of the intruder?
- What legal remedies may be applied?

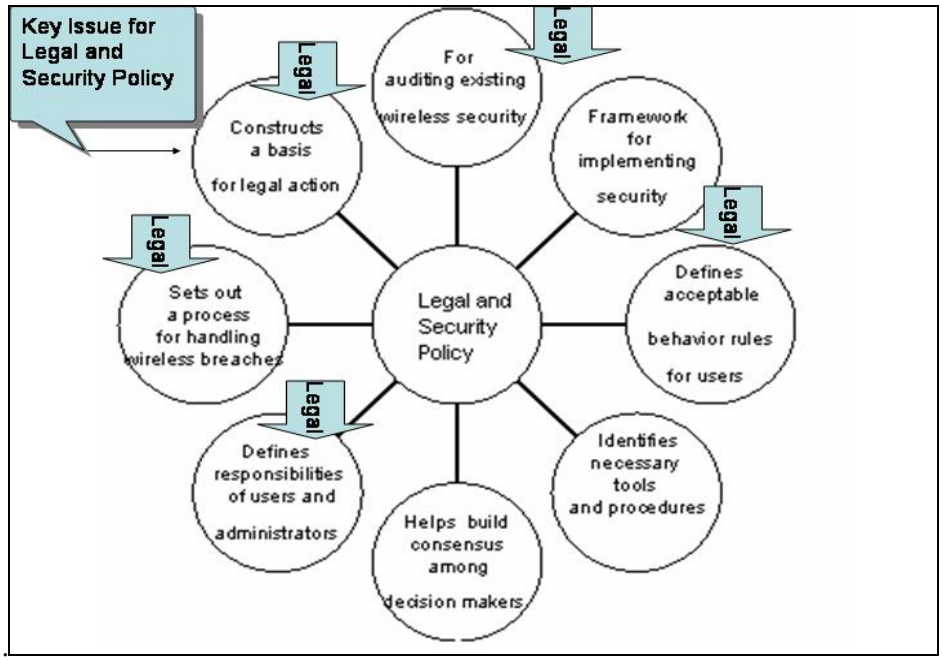

Figure 2. Reasons for WLAN security policy
adapted from Cisco Networking Academy Program: Fundamentals of WLANs v1.0

For the last question, the researchers propose a global, harmonized, legal, collaborative extranet similar to the medical fraternity's Cochrane Collaboration (www.cochrane.org). The MELS Framework emphasizes an up-to-date Security and Legal Policy for the reasons set out in Figure 2, including, most importantly, acting as a **basis for possible legal action in case of breaches.** Areas of importance to legal issues are highlighted by arrows.

In most countries writing a virus is not illegal and 'some legal scholars argue that it is protected as free speech' (Thompson, 2003). It becomes illegal once it is released, spreads and causes damage to computer systems. In order to examine the legal and business risks for an m-enterprise, it is important to consider the potential areas that may construct a basis for legal action. If a person accesses and does damage to the WLAN by, for example, introducing a worm or virus, they could put office systems at risk, cause loss of reputation and commercial advantage. Companies too must demonstrate that:

1. a reasonable level of care has been undertaken to protect their computer systems
2. they have a proactive strategy for monitoring and enforcing the security policy

or they may be in exposed to liability in negligence (Quek and McPherson, 2003).

5. LEGAL JURISPRUDENCE

Damage caused to a business by virus/worm infections may include:

1. cost of restoring the computer(s) to an operational state
2. value of any data lost
3. loss of profits for the time that business or production is incapacitated
4. loss of reputation or goodwill (New Zealand Law Commission, Report 50).

The damage available in **trespass** include cost of repairing goods, loss of profits or use of goods and in appropriate cases exemplary damages (New Zealand Law Commission, Report 50). If files that are copied are not protected by copyright, breach of confidence may be a possible remedy. The New Zealand Commission believes that a person who obtains confidential information by reprehensible means is subject to a duty of confidence.

Some academics have theorized that virus writers could perhaps be charged under conspiracy laws as creating viruses might be considered as abetting a crime by providing materials to people who release the

worms (Thompson, 2003). Singapore has recently passed laws against hackers and virus writers that enable the law enforcers to arrest suspects before they act – 'pre-emptive action' (Reuters, 2003). Convicted hackers may be jailed for up to three years or fined up to $US5800 and in the first half of 2003 there were 24 cases of hackers gaining access to unauthorized sites. Table 2 below illustrates the recent arrests of worm and virus writers.

Table 2. Recent arrests for Virus/Worm infringements

2003	Virus/Worm
Minor arrested	RpcSpybot – worm
Jeffrey Lee Parson	Blaster-B worm
Romanian man	Blaster-F worm
2 British adults	TKBot-A Trojan Horse
Simon Vallor	For writing Gokar, Redesi and Admirer Viruses

In a mobile enterprise where workers use Bluetooth enabled devices there is the danger that 'snarfers' who capture documents, contacts and other information may obtain company secrets. The copyright owner has the right to use the material in a variety of ways and the rights may be assigned or leased with or without limitations or conditions. Use of copyright material, usually by copying without the permission of the owner, will ordinarily be an infringement of copyright, except in certain circumstances, for example copying of a limited portion of a book by a student (the 'reasonable portion' test). Australia protects ISPs from legal action if they are only used as a conduit for copyright material. The United States protects ISPs only if they sign up for a regime of ' takedown notices'.

In August 2000, the Federal Government of Australia passed amendments to the Copyright Act that came into effect in March 2001. The right of communication will apply to 'active communication, such as broadcast or cable transmission and to 'passive communication, such as making material available to be viewed or downloaded (e.g. a website). There will be criminal penalties and civil remedies for making, importing or commercially dealing in devices and services that circumvent technological copyright protection measures such as decryption software. (there are however permitted purpose exceptions - such as for governments and decompilers of software). Liability of carriers and Internet Service providers for infringing copyright is also dealt with as they are persons who provide the broadcast or determine the content of the communication. There are factors to be taken into account to determine whether a person is liable for authorizing or infringing and these factors are based on existing case law.

5.1 National and International Legislative Controls

The European Convention on Cybercrime has as its objective "to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. It is the first international treaty on crimes committed via the internet and other computer networks, dealing with infringements of copyright, computer related fraud, child pornography and violations of network security. This treaty is the result of the work of the European Union and other countries including the United States, Japan and Canada. The European Union has a website, Cybertools On-Line Search for Evidence (www.ctose.org) to help people investigate computer crimes and gather evidence that can later be used in court.

In the USA, there are a several agencies, including the FBI, working in the area of cyber crime, often with overlapping jurisdictions. The National Information Infrastructure Act, 1996 provides a framework for dealing with computer crimes at the federal level. The Electronic Communications Privacy Act (ECPA) 1986 is also relevant. In particular, s2511 prohibits "interception and disclosure of wire, oral or electronic communication. However, s2511 (2) g (i) provides that it shall not be unlawful for any person "to intercept or access an electronic communication made through an electronic communication system that is configured so that electronic communication is accessible to the general public". In Texas, the Penal Code Section 33a.04 would appear to prohibit Wardriving as set out in Sec. 33A.04. Theft of Telecommunications Service. (a) A person commits an offense if the person knowingly obtains or attempts to obtain telecommunications service

to avoid or cause another person to avoid a lawful charge for that service by using: (1) a telecommunications access device without the authority or consent of the subscriber or lawful holder of the device or pursuant to an agreement for an exchange of value with the subscriber or lawful holder of the device to allow another person to use the device (www.bakers-legal-pages.com).

However, in Bill 495 being considered by the New Hampshire legislature, the onus will be placed on operators of wireless networks to secure them or lose some of their ability to prosecute anyone who gains access to the networks. (www.wired.com), (Koman, 2001).

The Digital Millennium Copyright Act's anti-circumvention clause makes it a crime to try to crack digital rights management software. This is a massive expansion of copyright protection, a change that shifts the entire purpose of copyright from supporting creativity to granting total and absolute property rights not to artists but to middlemen (Security, 2003).

In Australia, under the Cybercrime Act 2001 "Serious Computer Offences", punishable by lengthy jail sentences are established for unauthorised access to, or modification of, data held in a computer or impairment of electronic communication to or from a computer. It also makes it a crime to possess one of the many virus writing toolkits available online – this provides legal backing to authorities to treat malware authors as criminals in Australia (Braue, 2004).Also in Australia, under the Telecommunications (Interception Act) 1979, criminal penalties apply to a person who "authorizes, suffers or permits another person to intercept a communication passing over a telecommunication system"

5.2 Cases

One celebrated virus case concerns the arrest of David Smith who was responsible for the transmitting the Melissa Virus. He was arrested in 1999 but within weeks of his arrest he was helping authorities to investigate and arrest other virus writers. The judge reduced his possible 10 year sentence to 20 months (www.securityfocus.com).

At the time of writing no cases involving snarfing, warchalking or wardriving had reached federal or appellate courts where decisions can set precedents for criminal proceedings by law enforcement agencies or for civil actions. At the District Court level in USA a few cases of interest have appeared before the courts.

In the District Court in Georgia, Judge Thomas Thrash found that "port scanning" of a network without gaining access to that network does no damage and therefore does not constitute a crime under anti-hacking laws (www.theregister.com). In the WLAN environment this could be likened to using the products such as AirMagnet or Wireless Security Auditor, as mentioned in section 2. In Texas, Stefan Puffer was charged on "two counts of unauthorized access into a protected computer system and unauthorized access of a computer system used in justice administration" but was acquitted because had not intentionally caused any damage. Puffer had claimed that he broke into the computer system to prove how easy it was. In North Carolina, Clayton Dillard was accused of breaking into Wake Internal Medicine Consultant's computer system and illegally accessing information on hundreds of patients. Dillard pleaded guilty, claiming that he was an "ethical hacker", but was sentenced to 18 months probation and ordered to pay $10000 (US) in fines (www.channel3000.com). In each of the three cases the MELs framework questions: Is the network adversely affected, has the network been properly configured and what were the intentions of the intruder? feature prominently. In Case 3, the police noted: 'No matter what your intentions are, there is a point that experiment and research stops and criminal activities start' (Phillips Business Information, 2002).

6. CONCLUSION

There are few precedents to follow in the area of wireless wardriving, warchalking and snarfing but the paper has provided an overview of the current situation as well as the revised MELs framework as a way for mobile enterprises to ensure that they are setting in place legal and security polices to protect their networks. Legal remedies are being put in place try to criminalize virus and worm activities. Network companies such as Cisco are working on developing new security strategies and technologies in what is know as Self Defending Networking which rely on firewalls, intrusion detection software and behavioral anomaly software. Promising work on 'stealth' wallpaper (based on secret stealth technology that is used to hide military radar)

can block WiFi at 2.4, 5 and 6 gigahertz while allowing through GSM and 3G cellphones. (Fox, 2004). This technology could stop outsiders gaining access to a secure network by utilizing rogue access points set up by office workers.

REFERENCES

Allen, M. 2002. *E-Business, The Law And You.* Prentice Hall, 2002 Australia.

BMB Profile And Services, 2003. Security Wheel Definition, *BMB Profile And Services*http://www.Bmbgroup.Com/Dls/BMB_20Profile.Pdf, Page 8.

Braue, D. 2004. Virus wars: Fighting back, *Australian Personal Computer*, apcmag>need to know> pp 24 -5

Cisco Networking Academy Program ,2003. *Fundamentals Of Wireless Lans* V.1.0

Deakins Bits And Bytes, 2002. *Wi Fi: Wireless Networks*, Page 2

Deats, M. 2004. Next Plus Security. *Sydney Morning Herald*, 25 May 2004, Next page 1.

De Vuyst, B. 2002. Dispute Resolution of gTLD conflicts: *Proceedings of the 35th Hawaii International Conference on System Sciences*, Hawaii, USA. 0-7695-1435-9/02 IEEE (CDROM

Donovan, J. 2003. Symantec Australia; Submission to the Parliamentary Committee Public Accounts and Audit Inquiry into Management and Integrity of Electronic Information in the Commonwealth,http://www.aph.gov.au/house/committee/jpaa/electronic_info/submissions/sub63.pdf

Elliott, G. & Phillips, N. 2004. *Mobile Commerce And Wireless Computing Systems*, Pearson Addison Wesley, 2004.

European Convention on Cybercrime http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185

Fitzgerald B. & Fitzgerald, A. 2002. *Cyberlaw Cases And Materials On The Internet, Digital Intellectual Property And Electronic Commerce*, LexisNexis Butterworth, 2002 Sydney

Fox , B. 2004. Stealth wallpaper keeps company secrets safe, *New Scientist* page 19 12 August 2004.

Hussley J. and Hussley R. 1997. *Business Research*. MacMillan Press Ltd.

Koman, R.. 2001. Lessig: The Future of Ideas, 21 December 2001, http://www.openp2p.com/pub/a/p2p/2001/12/21/lessig.html?page=1

Lawrence, E. and Lawrence, J. 2004. Threats to the Mobile Enterprise: Jurisprudence Analysis of Wardriving and Warchalking, *Proceedings of the International Conference on Information Technology*, Vol 2. Las Vegas April 2004 pp285-291.

LexisNexis, 2003. *Cyberlaw*, General News And Information, Section Wireless 2003 Warren Publishing Inc, Communications Daily November 5.

Montcalm, B. 2003. How To Avoid Legal And Ethical Issues In Wireless Discovery, *Sans Institute* http://www.sans.org/Rr/Papers/68/176.Pdf

New Zealand Law Commission, Report 50: Electronic Ccommerce – part 1, The Law of Tort; http://www.austlii.edu.au

Phillips Business Information, LLC. 2002. Is Wireless Data A Security Threat? Feb 13, 2002, *WirelessData News*, Potomac; Feb 13, 2002; Vol 10, Issue 4

Quek, J. and Mcpherson, S. 2003. IT Security – Are You Meeting Your Duty Of Care? *Minter Ellison Technology News*, October 2003 P.3

Reuters, 2003. Singapore Internet Security Laws Get Tough. *Sydney Morning Herald, Next*, 18 Nov. p 1

Roberts, P. 2004. *Cisco warns of wireless security hole*, IDG News Service, 7 April, 2004 wfusion.com/news/2004/0407cisowarns.html

Schoder, D. and Fischbach, K. 2003. Viewpoint: Peer to Peer prospects. *Communications of the ACM*, February 2003, 46 (2): 27 – 29.

Security (2003) Melissa man recruited by FBI, *The Australian* 23 September 2003, p. 5. www.securityfocus.com/news/126

Standage, T. 2003. Beyond The Bubble, A Survey Of Telecoms, *The Economist* October 11th 2003, P.7

Stanfield, A.2003. *E-Litigation*, Thompson Legal And Regulatory Ltd: Lawbook, Sydney 2003.

Thompson, C. 2004. Dangerous Minds, *Good Weekend, The Sydney Morning Herald Magazine*, April 3, 2004, pp. 20 – 26

Wearden, G. 2002. Drive-By Spam Hits Wireless LANs. *Special To CNET News.Com* September 6, 2002.

Wright, C. 2004. Tough Call for Smart phones. *Sydney Morning Herald* .Next. 6 April.

Young, A. and Yung, M. 2003. Cryptovirology: The use of cryptography in virus attacks: http:// sconce.ics.uci.edu/docs/ cryptovirology.pdf.