# WarDriving Dilemmas

Hira Sathu

Unitec

hsathu@unitec.ac.nz

## Abstract

This paper, relates to computing practice in an area where ethical norms and provisions in law are either absent or inadequate. WarDriving is a popular term used to describe the activity of locating and logging the position of APs. With the integration of Global Positioning Systems (GPS) that aids in locating the wireless APs, their position is marked for future use. WarChalking is commonly used to describe this activity. Critical examination of the ethical and legal dilemmas associated with WarDriving and WarChalking are discussed in this paper. The Wi-Fi LAN technology that makes it susceptible to WarDriving is discussed first. The outcomes of WarDriving being unethical or illegal depends upon the nature of the activity and the motive of the parties. These activities could vary from passive listening to the consequent viewing of private data or use of the available computing resources including Internet connection. The paper uses analogies from day to day practices to establish correct ethical practice. The case laws and statute law on the subject in a few other countries is discussed. New Zealand could also draw from the case law of some of these countries to cover contingencies related to WarDriving that are not covered by the existing exceptions in Sec 252 of the Amendment (No 6) of the Crimes Act 1961.

*Keywords*: WarDriving, WarChalking, ethics, laws, dilemma

## 1 Introduction

An increase in the deployment of Wireless LANs (WLAN) has been a recent trend on account of the ease, speed and flexibility they offer. The manufacturers of the wireless Access Points (APs) or the wireless Routers that also have the AP features incorporated in them make the default establishment of WLANs easy. This may be a selling point for these devices but it also makes them vulnerable to unauthorised access by hackers or crackers. Lin (2003) reports that WarDriving trials to investigate the openness / insecurity of WLAN in Auckland central business district (CBD) deployment revealed that 70% of WLANs were using identifiable / no service set identifier (SSID) that included 13 % using the default SSID. As regards securing WLANs using wired equivalent privacy (WEP), 60% had no WEP enabled on them (Lin, 2003). A wider US based WarDriving activity named as the Third Worldwide WarDriving (WWWD) revealed that about 68% did not use WEP encryption and about 28% did not even change the default SSID of the WLAN (WWWD, 2006).

There are differing opinions as to the activities that are covered by the term WarDrivng. At one end are those who restrict the WarDrivng activity only to passive listening of the wireless transmitted signals with a view to logging the position of the network. On the other hand are a more elaborate set of activities that include viewing of confidential data and even use of the network resources (like Internet access) in addition to locating the wireless AP. However different the interpretation of WarDrivng maybe, it has taken up centre stage and added to the nuisance value where the activities are not authorised by the business providing the WLAN and home WLANs alike. It is not difficult to envisage that some community projects or campus wide or even city wide wireless access providers may conduct an authorised WarDriving exercise. This may be with a view to mapping for ensuring adequacy of coverage by wireless APs or locating of wireless routers vis a vis the APs. Some examples may be hot spots in an airport terminal, hotels, libraries, or a futuristic city with a community of open APs forming ubiquitous Internet accessibility. The marking, to indicate location of APs with a view to make access by users easier, where not sanctioned by the provider is termed as WarChalking.

This paper aims to describe the practice, ethical and legal issues surrounding WarDriving. The paper begins with the background to WLANs, in Section 2 to set the scene for continuum of activities that fall under WarDriving and WarChalking covered in Section 3. Section 4 discusses a few examples of WarDriving and WarChalking activities that give rise to dilemmas in the ethical and legal context. Section 5 discusses the legal position with regard to WarDriving in few other countries like US, UK and Australia. Section 6 provides recommendations for WLAN deployment and ethical practice. Section 7 concludes the findings for this study.

## 2 WLANs Background

The most common form of Wireless LANs is the Wi-Fi LANs or what are also referred to as the IEEE 802.11a,b,g based WLANs. The manufacturers of these wireless cards provide basic set of configuration settings for security purposes as covered below:

- Name for the network, called the SSID for identifying the WLAN. Most vendors have a default name that can be changed.

This quality assured paper appeared at the *19th Annual Conference of the National Advisory Committee on Computing Qualifications* (NACCQ 2006), Wellington, New Zealand. Samuel Mann and Noel Bridgeman (Eds). 

- The above SSID can be made to be broadcast (the default mode) or configured to disable broadcast of SSID.
- A basic form of encryption with 64 bit or 128 bit keys. This is termed as wired equivalent privacy (WEP). The default setting for this is no WEP.
- Filtering of the MAC address by the AP in order that no unauthorised wireless client is given an IP address for joining the wireless LAN. MAC address filtering is disabled by default.

Changing of the default SSID name of WLAN or disabling of the SSID broadcast may not qualify as strict security measures. However, it may be noted that they help by not placing all WLAN resources in full public view. Hence the configurations changes to the first two are good practice. As for WEP the actual encryption is only of 40 or 104 bit long keys. The initialising vectors for the encryption process take up 24 bits. These remain static for a period of time that is sufficient for their capture, identification and later breaking of the encryption mechanism. As for the MAC address filtering this involves the inputting of the data link addresses (also called the wireless card hardware address) of authorised clients into the AP database. Unauthorised hackers and crackers can spoof MAC addresses of genuine wireless clients and use these to break into the network.

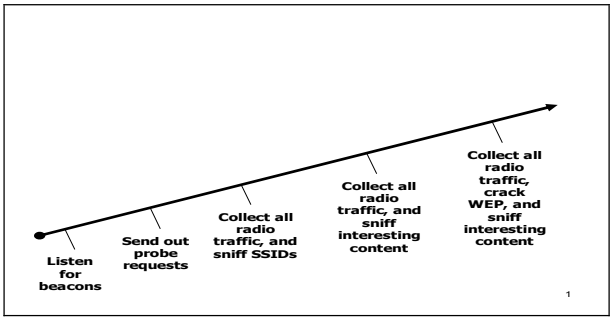
The above shortcoming has been addressed in the later WLANs to varying degrees. These are Wireless Protected Access (WPA) standard and the more recently announced IEEE802.11i (also referred to as WPA 2) standard. In brief these standards provide extended authentication mechanisms, with better encryption (Advanced Encryption Standard - AES) and dynamic key settings (Temporal Key Integrity Protocol - TKIP) (Planet3 Wireless, 2003). The next section examines how users could locate, view or even use network resources.

## 3. WarDriving and WarChalking

WarDriving as discussed above is the activity of detecting and may be logging the position of a wireless network. Another definition posted by Brian Krebs on Washington post.com is "… it is the practice of driving around with a laptop and a powerful antenna (and a global positioning system device) and eavesdropping on or merely using wireless networks that don't belong to you." (Krebs, 2006). Whether the activity of WarDriving is sanctioned or not; restricted to only locating and logging the position, or use of resources, the WarDriving activities are possible since WLANs operate on the principle of Radio Frequency (RF) energy being transmitted over free space. This RF energy can be picked up by any suitable device with a receiving antenna and converted to a viewable form. Once the connection to the network is obtained the other activities are possible as in case of a wired LAN. Once the location of an AP or wireless router is logged this may be marked for future use by oneself or others. WarChalking was the term used to indicate open AP locations since these were indicated by a chalk mark on the sidewalk, wall or any suitable landmark to identify the location of the open AP (Vandevelde, 2003). This activity has been further perfected by indicating additional information through symbols to indicate the features of the WLAN detected and mapped. These cover a range of features like: open, closed, SSID name, secured and even the quality of Internet connection like broadband access speeds etc. Where the signal received is poor, one can return with a higher gain antenna for better reception.

The range of activities that are covered under WarDriving where it is not just restricted to passive listening is covered in Figure 1 below from a presentation by Hoar (2006) who in turn used material from Josh Goldfoot, US department of Justice. Where WarDriving activity is given its broadest interpretation it would cover sniffing of network traffic, viewing private information like credit card numbers, passwords login names etc. Private data may even be modified where the files are sharable.

**Figure 1: WarDriving Continuum**




(Source: Josh Goldfoot, US department of Justice)

The WarDriving activity involved a car equipped with a wireless capable laptop computer driving with a view to pick up a wireless network connection. The laptops/computers may be equipped with software utilities like NetStumbler for windows clients (www.netstumbler.com/), Kismac for Macintosh clients and Kismet for Linux clients (Anderson, 2004). Utilities like "Kismet (http://www. Kismetwieless.net/) also identify workstations that are talking to the AP and their MAC addresses" (Maiwald, 2003). Higher gain antenna can be used where the signal received is poor.

## 4. WarDriving and WarChalking Dilemma Examples

This section discusses various examples that would arise from WarDriving and / or WarChalking and thereby raise questions as to the activities mentioned in the WarDriving continuum being unethical and / or illegal.

Passive scanning of the airwaves by itself would neither be unethical nor illegal since it is the transmitting AP (open) that is promiscuous by advertising**.** The comparison here can be made to listening of commercial radio, which is neither unethical nor illegal. However, it may be worth noting that listening on to certain radio frequencies used by police and the defence services in some countries is not permitted by law.

Active scanning of APs in a public area like an airport or other community areas (libraries, hospitals etc) that might be expected to provide free wireless Internet access

(hotspots) would be ethical. Common operating systems like Window XP are customised to scan and list open WLANs by default.

Activity involving a campus wide organisation that has multiple APs authorising the mapping and marking (WarChalking) of APs for access from these locations for the benefit of its users would be a legitimate activity. However, where an unauthorised person intends to mark this very area for own or other persons use, it would be unethical both in marking (untidy) as well as possibly against the intention of the owner to identify the APs. Where the APs are not intended for public use and a user intentionally uses such a service, classifying such an act as unlawful may be difficult to prove for various reasons. Firstly, the WLAN provider may not have clearly indicated the WLAN was not intended for public use. Secondly, adequate provisions in law may not exist to cover the activity as illegal. Consider a casual user (non computer savvy person) using an unsecured WLAN (APs with no WEP), it may be hard to prove unauthorised access. Since inability to disable TCP/IP stack to ensure inadvertent use of services by such persons could also be used as a possible defence.

There are instances where ISPs may have contracts with their users that forbid Internet connection sharing. An open and / or unsecured WLAN may be held to be in breach of such a contract.

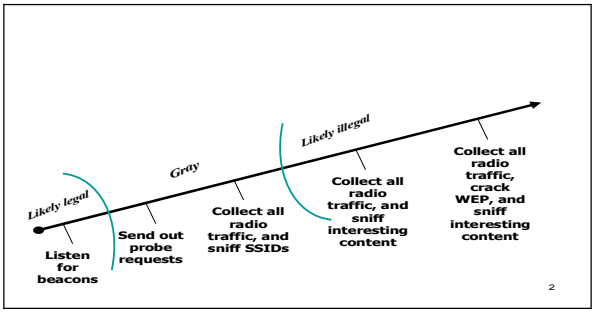
Another dilemma could be by way of classifying as to what extent is the provider of open/ insecure WLAN liable for use of their services for illegal activities by another party. Consider a person downloading child porn who may be booked for a criminal offence since violating an existing law, what about the abetment of this offence by the WLAN provider? Similar issues may arise where the IP and MAC addresses are spoofed from such open APs and used for criminal activities. This makes identification of the criminal activities difficult by law enforcement agencies.

Consider the issues associated with outcomes from authorised as well as unauthorised WarChalking activities. Where a criminal act is committed through use of a previously warchalked wireless resource, would the WarChalking constitute as an abetment for the offence? Issues like theft of computer resources, where this involves use of Internet access, CPU power, memory etc by persons where the resources are open to public would also need consideration under abetment to theft. The dilemma here could be still greater where the mapping of APs was undertaken for reasons other than for abetting a criminal offence. An analogy is that of information available from a marketing person mapping houses that do not have security alarms or say dead bolts for marketing security alarms/dead bolts being used by criminals.

Publishing of the location of APs with MAC addresses and their WEP/No WEP status on say a web site for pecuniary or other advantages may classify not just unethical but criminal. The acts here are not inadvertent use of a service but clearly intended for a monetary or other gain. Even where the intention may be to gain popularity, peer status or just for the joy of it, may still classify as a criminal act though intention may be difficult to prove in such cases.

Summarising of the possible legal, grey and illegal activities are covered in figure 2 below. The area of possible legal activities is obvious since most modern computing equipment that come equipped with wireless features would listen for beacons as a prerequisite to establish wireless connectivity. Likewise, the area of sniffing private / interesting content and cracking WEP and viewing or modifying private data that is not authorised would classify as illegal. The dilemma pertains to the activities like sending out probe requests and sniffing SSIDs. These activities could be argued either way. A case in point is that of a casual wireless client looking out for a hot spot and therefore may actively scan for a hotspot using a probe request.

**Figure 2: Is WarDriving Legal?**




(Source: Josh Goldfoot, US department of Justice)

An instance of a grey area would be where a person accesses an unsecured WLAN not knowing it be a private WLAN. Then goes on to use this to surf the net or view emails. Another example of a similar kind is where a person equipped with a Wi-Fi enabled phone automatically switches to the lowest cost connection, which may pick up an open WLAN as the desirable connection. If are charged for all WarDriving activities across the board this may render many innocent people liable to criminal conviction.

Though there are possible grey areas covered by the activities of WarDriving, the emerging legal position may be evidenced from the case laws as legal precedence. The next section discusses some examples of the case laws in other countries.

## 5. Legal Position in Other Countries

Few states in US have prosecuted persons for WarDriving. In one case a person in Florida was charged with felony for accessing an open WLAN from his SUV (Arstechnica.com). Another case relates to person in Michigan as far back as 2003: A wireless network was used for siphoning credit card numbers from the Lowes, hardware store (Poulsen, 2003). The criminal act was in the siphoning of the credit card numbers. In New Hampshire (US) a bill was proposed to protect people who accidentally tap into insecure WLANs (Lin, 2003). The objective was to make the WLAN providers responsible for securing their WLANs. However, this bill has yet to be to be enacted as law.

In the UK, Sections 125 and 126 of the Communication Act of 2003 were used to prosecute a person (Ilett, 2005). While the first section relates to dishonest intent used for obtaining an electronic service the second relates to intent to avoid payment of a charge applicable for the provision of that service. Hence dishonest use of Internet service or storage media and like would be covered by this act.

In Australia the Federal Cybercrime Act 2001 amended the earlier Act of 1995 to cover crimes related to computers and electronic communications (Caslon Analytics, 2006). Various clauses of the act cover unauthorized access, modification, impairment, producing and supplying of data to commit a criminal act as well as related computer offences. As per Caslon Analytic there has been no definitive case law of theft covering network service by unauthorised means in Australia.

There are no specific laws covering activities related to WarDriving in NZ. Computer crimes are covered under the Amendment (No 6) of the Crimes Act 1961. This is a more generalized act covering unauthorized access. A person was charged for hacking in mid of 2003 (Wood, 2004). Section 252 of this Act relates to "Accessing computer system without authorization". The exceptions covered under Sub section (2) and (3) to persons liable under sub section (1) are limited to access by persons who are ordinarily given access to the system but for other purposes and access by law enforcement agencies.

## 6. WLAN Deployment and Practice

In section 2 above the improvements made by the more recent WLAN standards were covered briefly. However, it may not be advisable to suggest a move over to the 802.11i standard in view of the large amount of wireless LAN infrastructure that uses the earlier 802.11 a, b or g standards. In addition, the core issues would still remain. These issues relate to WLAN providers not taking even the basic steps to safeguard their existing 802.11 WLANs. Instead, if some basic configuration changes are made to the default settings a large number of the ethical dilemmas of wireless LAN usage would be taken care of. This would also help legal practitioners to a limited extent to deliver judgements, since unauthorised use would be easier to discern. This section will further endeavour to suggest ways to over come the ethical and legal dilemmas briefly.

The WLAN connectivity by unauthorised persons can be further minimised by adequate siting of APs to minimise the RF energy fallout into areas not required to be covered. There is equipment that does help in the location of Wi-Fi hot spots. Chrysallis Developments have developed "a wireless signal detecting tool small enough to fit a on a key chain, that locates Wi-Fi hot spots and determines the signal strength level" (Voice & Data, 2006). Other handy tools could also be used for siting of the wireless APs.

Duntemann (2003) suggests some ways to avoid ethical and legal dilemmas where WarDriving activities are taken up by persons. On detection of an open AP, the contents of the network should neither be examined nor modified and no network resources should be used . From these suggestions it emerges that the wardrivers should configure their equipment in order that there is no unintentional use by the equipment that may violate the above. It is also recommended that a computer should have its TCP/IP stack disabled. While the computer can view an AP(SSID) it will not be able to connect to the network.

The providers of WLAN should secure their WLAN. This would obviate a wardriver seeking the defence of accidental access. The second reason for this would also ensure that the WLAN provider is not seen to be abetting the criminal activity by providing an open WLAN. PC Magazine columnist John Dvorak mentions that "once a signal leaves ones property it's fair game" (Dvorak, 2004). Some measures to preclude such a defence are:

- SSID broadcast should be disabled. This could still be guessed by various utilities. Therefore the default SSID should also be changed.
- Enable the WEP encryption of the wireless AP/ router.
- A banner should be configured for display to warn unauthorised users of the WLAN.
- The default password of the AP should be changed.
- MAC address filtering should be enabled.

The first three security practices are essential for reasons suggested earlier. A range of advanced level protections can also be adopted by WLAN providers that deal with highly confidential data.

## 7. Conclusion

The findings of this study briefly emphasize that numerous ethical and legal issues need to be addressed in the area of WLANs. Therefore current wireless computing practices of both WLAN providers as well as wardrivers needs attention. As for the New Zealand WLAN environment, over 60% of WLANs have no WEP enabled and at least 54% use identifiable SSIDs as of end 2003 (Lin, 2003). It is likely that with greater uptake of WLANs these figures may only rise. The futuristic WLAN environment should provide for laws that cover different contingencies of accidental as well as dishonest access of wireless resources.

Common WLAN users who may or may not be wardrivers or hackers need to be educated about associated risks of unethical and illegal practices by way of dos and don'ts.

On account of the fast rate of change of future wireless technologies continued awareness of possible wireless infringements by law enforcement agencies is also important.

The next phase of this study is intended to look into the specific changes that need to be incorporated in NZ laws to cover additional exceptions in the existing Amendment (No 6) of the Crimes Act 1961. Where required the option for new laws that need to be legislated to cover

contingencies related to wardrivers, wireless clients and WLAN providers should also be kept open.

## 8. References


Anderson, Z., (2004): What Is WarDriving And How Can You Prevent It? Accessed March 07, 2006 (http://www.networknewz.com/)

Arstechnica.com: accessed on March16, 2006 (http://arstechnica.com/newsars/post/)

Caslon Analytics: Caslon Analytics note WarChalking and WarDriving. Accessed March 07, 2006 (http://www.caslon.com.au/warchalknote.htm)

Dvorak, J., (2004): PC Magazine, May 4.

Duntemann, J., Jeff Duntemann's WarDriving FAQ. Accessed October 13, 2003, (http://www.duntemann.com/wifi/WarDrivingfaq.htm)

Hoar, S. B. (2006): 802.11 – Wi-Fi Technology, Trends and Legal Issues. Accessed March 6, 2006 (http://www.law.uoregon.edu)

Ilett, D. (2005): Silicon.com: Wireless network hijacker found guilty. Accesed March 06, 2006 (http://mangement.silicon.com/government/)

Lin, C-T. (2003) *8IEEE 802.11b-based Wireless Network Security,* Master of Computing Dissertation, Unitec, pp51-62 and p139

Maiwald, E. (2003): Network Security: A Beginner's Guide, Mc Graw Hill, Osborne, pp435-438

Planet3 Wireless. (2003): Certified Wireless Network Administrator, Vendor-neutral wireless network training and certification, Mc Graw Hill, Osborne, pp404-409

Poulsen, K.(2003): Wireless Hacking bust in Michigan, Security focus, The Register. Accessed on March 07, 2006. (http://www.theregister.co.uk/)

Krebs, B. (2006): Security Fix Is Heading to Vegas, Washingtonpost.com. Acessed March 16, 2006. (http://blog.washingtonpost.com/securityfix/2005/07/)

Vandevelde, E. (2003): The Orogin and Legality of Warchalking, UCLA Journal of Law and Technology, Notes 19. Accessed June 01, 2006. (http://www.lawtechjournal.com/notes/2003/19_030731_Vandevelde.php)

Voice and Data (2006): Building Blocks, Products and Services driving convergence, Voice and Data , Vol.5, No.2, April , pp65

Wood, R. (2004): NZ Police lay first charge for hacking, The dominion Post- IT Business, 15 March.

Worldwide WarDriving Results. Accessed March 06, 2006. (http://www.worldwidedrive.org/wwwstats.html)