PIGGYBACK HUNTING — BROWSING THE INTERNET IN AUSTRALIA VIA UNSECURED WIRELESS NETWORKS: VIRTUAL THEFT OR ACCEPTABLE BEHAVIOUR IN AN ONLINE WORLD?

Rachel Anne Carter and David Makin[1]

Abstract

In a world that is increasingly dominated by the Internet, there is a growing demand for low cost access at the user's convenience. The expansion of wireless Internet networks, in particular unsecured wireless Internet networks, gives rise to novel challenges for the regulation of Internet access. The ability to access unsecured wireless Internet networks with ease and with very little impact upon the owner of the network suggests that such 'piggybacking' may be criminal behaviour or may amount to an actionable civil wrong. This paper will explore the legal ramifications of piggybacking an unsecured wireless network with knowledge that there is no entitlement to the use of the network and will consider what Australian authorities should do about this situation. This paper will look at the position in Australia and juxtapose this with that of the United Kingdom and the United States of America. In both the United Kingdom and the United States of America prosecutions have taken place of individuals who knowingly accessed unsecured wireless networks for their own personal use.

[1] Rachel Anne Carter, BA, LLB (Hons), Associate Lecturer at La Trobe University, Bundoora, Victoria (this research was conducted during tenure of a Research Assistantship / Associate Lecturer at Deakin University, Burwood, Victoria) and David Makin (IT Program Manager, Aker Solutions Australia). The authors thank Luke Neal, Lecturer Deakin University Law School, for the advice provided on criminal law and would also like to thank Dr John Morss, Associate Head of School (Research), Deakin University Law School for his assistance editing the article.

I Introduction

This article will examine the legalities and potential legal pitfalls associated with connecting to unsecured third party wireless networks (Wi-Fi) in Australia and subsequently using them to browse the Internet. The practice of connecting to unsecured wireless networks in order to browse the Internet is often referred to as 'piggybacking'.[2]

The primary question being posed by this article is whether piggybacking and connecting to unsecured third party wireless networks is a criminal activity. Alternatively, even if no criminal activity has occurred, the question then becomes whether the individual using an unsecured wireless network with knowledge they have no permission to do so can be liable for a civil wrong under the tort of conversion? It is therefore essential to consider the exact nature of the wrongful act and the consequence of engaging in piggybacking. In determining civil and criminal liability, it will be essential to work out if an individual or organisation has been disadvantaged by the activity and, if so, in what manner they have suffered harm.

Several recent rulings in both the United States of America (Michigan)[3] and the United Kingdom[4] have highlighted that courts and law-makers within those jurisdictions believe connecting to unsecured third party wireless networks (Wi-Fi) in order to browse the Internet is an actionable criminal activity.[5] Piggybackers have indeed become the target of

---

2 R Rai and J Terpenny, 'Principles for Managing Technological Product Obsolescence' (2008) 31 *IEEE Transactions on Components & Packaging Technologies* 880; T. Kah Leng, 'Wireless Internet Regulation: Wireless Internet Access and Potential Liabilities' (2007) 23 *Computer Law and Security Report* 550.

3 Sara Bonisteel, *Michigan Man Fined For Using Coffee Shops Wi-Fi Network* (2007) Fox News <http://www.foxnews.com/story/0,2933,276720,00.html> at 22 March 2010; Stacy Norwicki, 'No Free Lunch (or Wi Fi): Michigan's Unconstitutional Computer Crime Statute' (2009) *University of California, Los Angeles Journal of Law and Technology* 1.

4 At the time of writing this article there is no appeal or appeal decision, although this event obtained media attention. See, Jane Wakefield, *Wireless Hijacking Under Scrutiny* (2005) BBC International News <http://news.bbc.co.uk/2/hi/technology/4721723.stm> at 20 March 2010.

5 Matthew Bierlein, 'Policing the Wireless World: Access Liability in the Open Wi-Fi Era' (2006) 67 *Ohio State Law Journal* 1123.

zealous law enforcement officials in countries which pride themselves on having excellent reputations for superior technological advances.[6]

Recent incidents from both the United States of America and United Kingdom will be examined in an effort to understand how the individuals involved in piggybacking were found guilty of committing a criminal offence. In particular, specific attention is paid to how the case law and legislation is used as the basis for these prosecutions.

In addition to looking at these recent overseas incidents, parallels will be drawn by reviewing and analysing specific Australian case law and legislation, including basic criminal law found in the *Criminal Code Act 2002* (ACT); *Crimes Act 1900* (NSW); *Criminal Code Act 1983* (NT); *Criminal Code Act 1899* (Qld); *Criminal Law Consolidation Act 1935* (SA); *Criminal Code Act 1924* (Tas); *Crimes Act 1958* (Vic); *Criminal Code 1913* (WA) and the Commonwealth legislation, which more specifically targeted crimes that involve technology and telecommunications. The Commonwealth legislation to be examined includes the *Telecommunications Act;*[7] the *Telecommunications (Interception and Access) Act*[8] and the *Cybercrime Act*,[9] which have all been incorporated into the *Criminal Code* 1995 (Cth).

Furthermore, a discussion will be made about the possibility of making those who engage in piggybacking liable for committing the tort of conversion. Although this is yet to be tested in Australia or elsewhere, this paper examines whether it will be appropriate to extend the tort of conversion to include the action of piggybacking. In particular the justification for such an expansion of the tort of conversion would be a formal recognition of the importance of the Internet in the modern world.

Finally, as a result of our review and analysis, we will gain an insight into what specific laws or guidelines exist within Australia and ascertain whether browsing the Internet in Australia via unsecured wireless

---

6 The countries where individuals who have accessed unsecured wireless networks without permission are the United Kingdom, Ireland and the USA. See, Daithi Mac Sithigh, 'Law in the Last Mile: Sharing Internet Access Through Wi-Fi' (2009) 6 *Scripted* 355.

7 1997 (Cth).

8 1979 (Cth).

9 2001 (Cth).

networks may be virtual theft, a civil wrong, or whether it is acceptable behaviour in an online world.

II Background

From its inception over 40 years ago as a secretive defence project,[10] the Internet has grown today into a seemingly ubiquitous communications medium that has become intertwined with our daily lives.[11] What is in reality a public network of networks and computers,[12] the Internet today delivers communications, social interaction, commerce, learning and entertainment to over 1.6 billion people across the world on a daily basis.[13] It is estimated in Australia that approximately five million households have Internet which is approximately 72% of all Australian households.[14] Due in part to its ubiquitous nature and our expectations as consumers, the Internet has become mobile and as such will be accessible almost anywhere from a wide variety of devices, ranging from portable computers through to cellular telephones.[15]

Whilst connection to the Internet once relied upon the use of a tethered network cable or telephone line between the point of connection and the device being used,[16] this has changed over recent years with a trend towards the use of wireless services to support mobility and ease of use when it comes to Internet browsing. One such technology that has

---

10 Patrick D Reagan, *History and the Internet: A Guide* (2002) 1–3.

11 See, B Fitzgerald et al, *Internet and E-Commerce Law — Technology and the Law* (2007) 486–487.

12 Kenneth J Baldauf and Ralph M Stair, *Succeeding with Technology* (2007) 18.

13 *Internet Usage Statistics — The Internet Big Picture: World Internet Users and Population Statistics* (2009) Internet World Statistics (Usage and Population Statistics) <http://www.internetworldstats.com/stats.htm> at 18 March 2010.

14 Australian Bureau of Statistics, '8146.0 — Household Use of Information Technology, Australia, 2008–2009' as accessed at <http://abs.gov.au/ausstats/abs@.nsf/mf/8146.0/> on 2 April 2010.

15 Shambhu Upadhyaya, Abhijit Chaudhury and Kevin Kwiat, *Mobile Computing Implementing Pervasive Information and Communications Technologies* (2002) 168.

16 Benjamin D Kern, 'Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law' (2004) 21 *Santa Clara Computer and High Technology Law Journal* 101, 103.

seen rapid growth in its recent popularity and usage is that of 802.11 Wireless Networking,[17] or what it has now become known as 'Wireless' or 'Wi-Fi'.[18] In the case of 802.11,[19] radio signals are broadcast on the 2.4 GHz frequency band and act as the communication medium, effectively replacing cables.[20] The 802.11 standard is maintained by the IEEE (Institute of Electrical and Electronics Engineers).[21]

The majority of wireless Internet Access Points advertised in hotels, airports, cafes and other public places are based on the 802.11 Wi-Fi technologies.[22] This proliferation of Wi-Fi networks has extended in recent times to the home with consumers installing 802.11 wireless networks at home using a wireless router.

As with many forms of technology, security is often a concern.[23] If the 802.11 Wi-Fi, technology is employed, certain security measures can easily be taken to protect a wireless network.[24] Failure to implement security features within a wireless network could result in the network being compromised ('hacked'), or data and information being damaged or compromised, or allowing others to connect without permission to a network and access the Internet via the network owner's Internet

---

17 Nikita Borisov, Ian Goldberg and David Wagner, 'Intercepting Mobile Communications: The Insecurity of 802.11' (Paper presented at Proceedings of the Annual International Conference on Mobile Computing and Networking, Rome, Italy, 2001) 180–189.

18 Vic Hayes and Wolter Lemstra, 'Unlicensed: The case of Wi-Fi' (Paper presented at the GMU 2008: Policy evolution with respect to unlicensed use of the radio frequency spectrum, George Mason University School of Law, Arlington, Virginia, 4 April 2008) 4.

19 See, Bob O'Hara and Al Petrick, *IEEE 802.11 Handbook: A Designers Companion* (2nd ed, 2005) 5–15, and see also Frank Ohrtman and Konrad Roeder, *Wi-Fi Handbook: Building 802.11b Wireless Networks* (2003) 7–20.

20 Baldauf and Stair, above n 12, 19.

21 Institute of Electrical and Electronics Engineers <http://standards.ieee.org/>.

22 Anurag Kumar, D Manjunath and Joy Kuri, *Wireless Networking* (2008) 8.

23 Matthew Gast, 'Seven Security Problems of 802.11 Wireless', (2002), *O'Reilly Media* as accessed at <http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html> on 2 April 2010.

24 Borisov, Goldberg and Wagner, above n 17, 180–183.

connection (piggyback).[25] Furthermore, the failure to put into place security measures is problematic because piggybacking allows anonymity, which may place the owner of an unsecured wireless network up for investigation in criminal matters if the piggybacking results in the commission of criminal activity. Although security is an issue, the majority (if not all) wireless network routers that are sold today have inbuilt technology that allows the consumer setting up the device to implement the necessary security measures to prevent unauthenticated intruders from connecting to the network,[26] thus offering the opportunity for the administrator of the network to eliminate or certainly reduce the practice of piggybacking. Furthermore, a possible solution may also be in having a secure captive portal with the conditions of access and the ability to restrict access to a network as compulsory aspects for home routers which are sold in the future.[27]

The IEEE itself maintains a variety of standards specific to securing wireless networks.[28] Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA/WPA2) are both standard encryption algorithms used to secure wireless devices and networks, with WPA and subsequently WPA2 superseding WEP and offering more robust security features. These security technologies rely on establishing a

---

25 Although there are potential security risks of an unsecured wireless network, some organisations have decided to have a totally unsecured wireless network by design so that anyone on the network can see the Internet traffic on the network, including the ability of law enforcement officials to see the Internet traffic. Although the wireless network is unsecured it employs the use of OSPF and BGP technology to mitigate the potential for criminal activities and to increase the ability to detect criminal activity should it occur on the network. Individual members can, however, protect their own nodes through creating a captive portal which outlines the terms of conditions and enables the owners to restrict or allow open access to their node and thus their Internet connection. One such example of an unsecured 802.11 wireless network that was designed to be open and thus transparent can be seen in the Melbourne Wireless Network. See, www.melbournewireless.org.

26 Michael E Whitman and Herbert J Mattord, *Principals of Information Security* (2nd Ed, 2005).

27 Austin Godber and Partha Dasgupta, 'Workshop on Wireless Security' (Presented at the Proceedings on the 1st ACM Workshop on Wireless Security, Atlanta, 2002) 41–46.

28 Joon S Park and Derrick Dicoi, 'WLan Security: Current and Future' (2003) *IEEE Internet Computing* 60, 62.

secure 'key' and controlling access by requiring a user or client of a network to have this key (for example a hexadecimal password or code) that is presented when requested to do so.[29]

Whilst WEP and WPA have critics who question the strength of these security measures, by implementing these simple embedded security measures the owner or manager of a wireless (Wi-Fi) network has the basic means available to limit and restrict unauthorised access.[30]

III Recent (and Notable) Incidents

Numerous incidents have taken place in recent years resulting in individuals being prosecuted for piggybacking onto Wi-Fi networks and browsing the Internet.[31] In this article we will examine two specific incidents: one that took place in the United Kingdom in 2005,[32] the other that took place in the state of Michigan in the United States of America in 2007.[33]

What is notable about both of these incidents is that the prosecutions were brought about directly by law enforcement officials, seemingly acting on behalf of the common good. Neither of these incidents or prosecutions was brought about by any individual or organisation that could have been disadvantaged or impacted by the actions of those individuals who were engaged in piggybacking. The other interesting item of note, common to both cases, was the fact that when discovered in the act of piggybacking by law enforcement officials, and upon being

---

29 802.11i IEEE Standard for Information technology: *Telecommunications and information exchange between systems, Local and metropolitan area networks Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements* (2004).

30 Robert Lipschutz, 'Protecting Wired & Wireless Networks', *PC Magazine* (USA) (February 2005).

31 Bierlein, above n 5, 1123–1127, 1185; Eric Bangeman, 'Illinois Wi Fi Freeloader Fined US $250', *Arts Technica*, 23 March 2006 <http://arstechnica.com/old/content/2006/03/6447.ars> at 25 March 2010; and John Cox, 'Michigan Man Fined for Using Free Wi-Fi', *Network World*, 23 May 2007 <http://www.networkworld.com/news/2007/052307-fine-using-free-wifi.html> at 25 March 2010.

32 Wakefield, above n 4.

33 Bonisteel, above n 3.

challenged as to what activity was taking place, in both incidents the individuals involved voluntarily admitted to being in the process of accessing unsecure Wi-Fi networks (to browse the Internet).

In spring 2005 in the United Kingdom, 24 year old Gregory Straszkiewicz was quietly sitting in his car using his laptop computer when he was arrested by police in West London. Local residents were concerned about Straszkiewicz sitting in his car as frequently as he did over a considerable period (three months) and eventually called the police.[34]

According to a variety of news sources published at the time of the incident[35], Straszkiewicz was arrested under s 1 of the *Computer Misuse Act* (unauthorised access to computer material).[36] He was subsequently charged and prosecuted under s 125 (for dishonestly obtaining an electronic communications service with the intent to avoid payment of a charge in using the service)[37] and s 126 (being in possession of an apparatus allowing him to dishonestly obtain an electronic communication service).[38] In bringing about these charges the Crown Prosecution Service felt confident that by accessing an unsecured wireless network with a Wi-Fi enabled laptop computer, Straszkiewicz was in breach of these Acts. Furthermore, their arrests were strengthened by the fact that Straszkiewicz was aware that he was accessing the unsecured Wi-Fi networks without possessing permission to do so.

In July 2005, The Isleworth Court in London agreed and subsequently found that Straszkiewicz was guilty of offences under both s 125 and s 126 of the *Communications Act 2003* (UK) and as a result was fined the sum of £500[39] and sentenced to 12 months conditional discharge as a result. He also had his laptop computer and Wi-Fi network card

---

34 Wakefield, above n 4.

35 Sam Lister, *Piggybackers are Logging into Trouble* (2005) Times Online <http://www.timesonline.co.uk/tol/news/uk/article552082.ece> at 29 March 2010.

36 *Computer Misuse Act 1990* (UK) s 1.

37 *Communications Act 2003* (UK) s 125.

38 *Communications Act 2003* (UK) s 126.

39 John Leyden, 'UK War Driver Fined £500' (2005) *The Register* <http://www.theregister.co.uk/2005/07/25/uk_war_driver_fined/> at 2 April 2010.

confiscated.[40] The main problem with Straszkiewicz's arrest and sentence is that his behaviour and punishment was based upon the need to use him as an example to prevent future piggybacking behaviour due to the potential security threats that could ensue for those who engaged in piggyback with intent to use that broadband to commit a criminal act.[41]

In what was an almost uncanny set of similar circumstances, in March 2007 Sam Peterson sat in his car browsing the Internet and checking his emails from his laptop computer whilst his car was parked in the car park of the Re-Union Street Café in Sparta, Michigan, USA.[42] Local shopkeepers had noticed Peterson on multiple occasions sitting in his car within the car park of the café and had suspected him to be a stalker or deviant of some kind. As a result, the police were eventually called and Peterson was questioned by them. When the police arrived and caught Peterson in the act of piggybacking, he freely admitted to using the nearby café's wireless service to browse the Internet. Peterson admitted to accessing the network despite the fact that he wasn't a customer of the Re- Union Street Café.[43]

Several weeks later Kent Country Prosecutors proceeded to charge Sam Peterson with a felony under Michigan State Law, in particular for breach of the *Fraudulent Access to Computers, Computer Systems, and Computer Networks Act*.[44] Although introduced back in 1979 to combat computer based crime (hacking), long before the conception of consumer orientated Wi-Fi networks, the Act itself had been revised

---

40 Lister, above n 35.

41 Helen Nugent and Michael Sims, 'Hidden Crime of "Wi-Fi Tapping" Only 11 Arrests but Most of Us are Guilty' (2007) *The Times Online* <http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2872726.ece> at 2 April 2010.

42 Bonisteel, above n 3; Steven Musil, 'Michigan Man Dodges Prison in Theft of Wi-Fi, CNet.com', (2007) CNet.com <http://news.cnet.com/8301-10784_3-9722006-7.html> at 1 April 2010; Russell Shaw, 'Michigan Man Busted for Stealing Wi-Fi Signal Could Have Received Five Years' (2007) ZDNet.com <http://blogs.zdnet.com/ip-telephony/?p=1640> at 1 April 2010.

43 Ibid.

44 *Fraudulent Access to Computers, Computer Systems, and Computer Networks Act* 53 USC (1979).

over the years to somewhat accommodate changes in technology.[45] The modern interpretation of this Act has allowed the Act to deal with unauthorised access to an unsecured wireless network by the means of piggybacking.

Under the *Fraudulent Access to Computers, Computer Systems and Computer Networks Act*,[46] Peterson was found guilty of a felony by the Court, sentenced to six months' probation, fined $400 and given 40 hours of community service.[47] The basis upon which Peterson was found guilty was that he had accessed the Wi- Fi system with knowledge that such access was unauthorised.[48]

As with the Straszkiewicz case in London, the prosecution in the instance of Peterson's arrest and charge was brought about by law enforcement officials. The owner of the Wi-Fi network in question, Donna May, the owner of the Re-Union Café, was not involved in the case brought against Peterson. May wasn't even aware that what Peterson was doing was a crime.[49] This is problematic, because the consequences for Peterson in engaging in such activities resulted in conviction for a criminal offence although it was unknown by the perpetrator that what he was doing was a criminal act. Furthermore criminalising piggybacking is complicated as the victim appeared to have suffered no real loss or disruption as a result of the action.[50]

---

45 *Fraudulent Access to Computers, Computer Systems, and Computer Networks Act* 53 USC (1979).

46 Ibid.

47 Richard Koman, '*$400 Fine for Using Wi-Fi Without Buying A Cup of Joe'* (2007) ZDNet Government <http://government.zdnet.com/?p=3175> at 22 March 2010.

48 Although Peterson was found guilty under the Act, it has been suggested that his guilt may be constitutionally invalid in the US on the basis that the legislation is too broad and thus that it gives too much discretion to the police and prosecutors as to the level of piggybacking required amounting to guilt. In particular this legislation has been accused of having no minimum standard upon which a prosecution should be assessed against. See, Norwicki, above n 3, 4.

49 Jacqui Cheng, '*Michigan man arrested for using café's free Wi-Fi from his car'* (2007) Arts Technica <http://arstechnica.com/tech-policy/news/2007/05/michigan-man-arrested-for-using-cafes-free-wifi-from-his-car.ars> at 31 March 2010.

50 It was said that, when another man was similarly engaged in piggybacking

These are by no means the only two cases of individuals being prosecuted for illegal use of unsecured Wi-Fi networks (piggybacking).[51] The investigator, Detective Constable Stephone Rothwell, who was in charge of the matter, highlighted the novelty of this case, stating that this was 'the first of its type in the United Kingdom and it sets an example to people who use increased computer technology to try and avoid paying for the Internet.'[52] Although this was the first prosecution, many people had been involved in this activity previously, but had not been prosecuted for their actions.

Subsequently, in March 2006, the then United Kingdom Secretary for Trade and Industry, Fiona MacTaggart, in an address to Parliament, highlighted that during 2004, 17 individuals were charged and 16 convicted of a criminal offence through piggybacking,[53] which was a breach of s 125 of *Communications Act*.[54]

American law enforcement remains as zealous and active as its British counterpart in the fight against illegal piggybacking, primarily because of the increased risk of a proliferating crime rate. The seriousness of wireless piggybacking stems from the anonymity that offenders can achieve due to the increased difficulty in prosecuting criminal activities carried out by those whilst accessing an unsecured wireless network.[55]

---

of the Re-Union Street Café, the owner of the Café, Donna May, told the man to say to police when questioned that he had asked permission to use the network so that he would avoid liability for a criminal offence. This evidence coupled with the fact that May never pressed charges against Peterson (rather he was charged by law enforcement officials) showed that the owner of the wireless network was not even concerned about its usage, yet a criminal conviction was given to Peterson for his activities. See: Norwicki, above n 3, 5 (Para 50).

51 Dan Ilet, *Law and Policy: Wireless Network Hijacker Found Guilty* (2005) Silicon.com <http://management.silicon.com/government/0,39024677,39150672,00.htm> at 1 April 2010.

52 Wakefield, above n 4.

53 Fiona Mactaggart, UK Secretary for Trade and Industry, *House of Commons Written Answers 23 March*, House of Commons (2006) (pt 11 column 512W).

54 *Communications Act 2003* (UK) s 125.

55 Grant J Guillot, 'Trespassing Through Cyberspace: Should Wireless Piggybacking Constitute a Crime or Tort under Louisiana Law' (2009) 69 *Louisiana Law Review* 389, 390; Bierlein, above n 5, 1123–1124.

IV Piggybacking: an Australian Perspective (Criminality of Accessing Unsecured Wireless Networks)

With regard to prosecutions in Australia specifically related to illegal use of or access to unsecured wireless (Wi-Fi) networks for the purpose of browsing the Internet (piggybacking), no precedent cases have been identified in the course of writing this article.

To explore how such an incident might be dealt with in Australia, the *Crimes Act 1958* (Vic),[56] *Telecommunications Act 1997* (Cth), the *Telecommunications (Interception and Access) Act 1979* (Cth) and the *Criminal Code 1995* (Cth) will be examined (albeit at a summary level) to ascertain how such a case could potentially be prosecuted. Whilst these may not be the only relevant laws, these are being examined to provide a general cross-section of the legislation that exists today, which could potentially be used in such a prosecution.

Looking specifically at the *Crimes Act 1958* (Vic) as an example of criminal law, the most logical place to begin one might think is that of *theft*.[57] Thus, in order to prove theft, it would be necessary to prove that property is dishonestly appropriated. The main point of contention in relation to piggybacking with unsecured wireless networks is whether the bandwidth can be classified as property. The definition of property for the purposes of theft in s 71(1)[58] encompasses intangible property,

---

[56] Although *Crimes Act 1958* (Vic) will be used primarily this will be juxtaposed with the position in the other states and territories. See, *Criminal Code Act 2002* (ACT); *Crimes Act 1900* (NSW); *Criminal Code Act 1983* (NT); *Criminal Code Act 1899* (Qld); *Criminal Law Consolidation Act 1935* (SA); *Criminal Code Act 1924* (Tas); *Criminal Code 1913* (WA).

[57] *Crimes Act 1958* (Vic) s 71 and s 72. The basic requirement of theft is that a person steals if s/he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it — s 72(1). Similarly in the Australian Capital Territory and South Australia the term theft is used in s 134 of the *Criminal Law Consolidation Act 1935* (SA) and s 308 of the *Criminal Law Consolidation Act 1935* (SA). In contrast in the Northern Territory, Queensland, Tasmania and Western Australia the term stealing is used but the offence is essentially the same as that of theft. See, s 209 of *Criminal Code Act 1983* (NT); s 391 of *Criminal Code Act 1899* (Qld); s 234 of *Criminal Code Act 1924* (Tas); s 371 of *Criminal Code 1913* (WA).

[58] *Crimes Act 1958* (Vic). In Western Australia in s 370 of *Criminal Code 1913* (WA) and in Queensland under s 390 of *Criminal Code Act 1899*

thus the ability to term piggybacking as theft will be contingent upon the classification of bandwidth.[59] In an article written by Paul U Ali, it has been suggested that bandwidth is a 'tradable commodity', thus bringing it within the realm of intangible property.[60] The better approach was propounded by Professor Mirko Bagaric and Gerard Nash, who in annotating s 71(1)[61] highlight in the context of telephone calls that 'property cannot be appropriated unless it is in existence',[62] suggesting the action of making telephone calls does not actually deprive the owner of anything, although the person upon whose account the telephone calls were made will be subsequently liable to pay for those calls. In drawing an analogy between telephone calls and bandwidth, it may be argued that bandwidth is not in fact property as the owner of the unsecured wireless network has not been deprived of anything particularly if the usage does not alter the network owner's ability to enjoy the network.[63] A further problem in classifying piggybacking as theft is establishing a loss, particularly given the fact that the amount of bandwidth used by piggybackers to browse the Internet is often negligible. Even once these have been established, there is still the problem of intent, requiring the enforcement authorities to prove that there was a deliberate intent to deprive the wireless network owner of Internet bandwidth in the form of stealing it as opposed to simply using some bandwidth.[64]

(Qld) there is a list of items which are capable of being stolen. The authors contend that bandwidth could be capable of being stolen as it is a movable object.

59 Paul U Ali, 'Bandwidth as a Tradeable Commodity: An Overview of Online Bandwidth Exchanges and Bandwidth Derivatives' (2000) 28 *Australian Business Law Review* 458, 458–459.

60 Ibid.

61 *Crimes Act 1958* (Vic).

62 Gerard Nash and Mirko Bagaric, *Annotated Criminal Legislation Victoria* (2010) 265.

63 *Akbulut v Grimshaw* [1998] 3 VR 756.

64 In particular this may be difficult to establish in some instances because Windows XP which runs on many modern computers is designed to automatically pick up any available wireless networks. Therefore the issue remains that if your computer has automatically detected an unsecured wireless network and an individual uses it, did they have the requisite intent for the purposes of criminal liability. For information on how computers are configured to detect wireless networks see, Luc Small, 'Theft in a Wireless World' (2007) 9 *Ethics & Information Technology* 179, 180.

Contingent upon the interpretation of bandwidth and whether or not it is property will determine the applicability of an individual engaged in piggybacking being charged under either s 81[65] or s 82.[66] Provided bandwidth could be termed as property[67] for the purposes of the legislation then an individual engaged in piggybacking could be found to have breached s 81 in obtaining property by deception.[68] The crucial element to convict an individual who has obtained bandwidth by deception will be to establish that the individual actually knew that they were not entitled to use the unsecured wireless network yet still, either intentionally or recklessly, continued to use it.[69]

If we look internationally to the convictions both in the United States and in the United Kingdom, the intention element has been present whereby in both instances the individual freely admitted to accessing an unsecured wireless network with knowledge that there was no permission to do so. The question which then must be asked is how to interpret the mens rea standard. It is quite clear that innocent individuals who accidentally access an unsecured wireless network such as by having a wireless enabled device[70] without specifically trying to access a network is passive, thus not possessing the requisite intention element and not amounting to a contravention of the Act. Rather, in order for there to be a contravention, it will be necessary that a deliberate

---

65 *Crimes Act 1958* (Vic) [Obtaining property by deception]. There are also similar offences for obtaining property by deception under s 326 of the *Criminal Law Consolidation Act 1935* (ACT) and under s 192C of the *Crimes Act 1900* (NSW).

66 *Crimes Act 1958* (Vic) [Obtaining a financial advantage by deception]. There are also similar offences for obtaining property by deception under s 332 of *Criminal Code Act 2002* (ACT); s 192D of the *Crimes Act 1900* (NSW); and s 252A of *Criminal Code Act 1924* (Tas).

67 Ali, above n 59.

68 *Crimes Act 1958* (Vic) s 81. There may have also been a breach of s 326 of the *Criminal Law Consolidation Act 1935* (ACT) if the action of piggybacking occurred in the Australian Capital Territory or a breach of s 192C of the *Crimes Act 1900* (NSW) if the conduct took place in New South Wales.

69 See, *Criminal Law Consolidation Act 1935* (ACT) s 326; *Crimes Act 1900* (NSW) s 192C; *Crimes Act 1958* (Vic) s 81.

70 Small, above n 64, 180.

action is undertaken either 'as to fact or as to law'[71] with the intent or recklessness[72] to access an unsecured wireless network.

In order to contravene it is not essential that the party whose wireless network has been accessed knows of this;[73] rather what is essential is that the act of deception actually leads the victim to part with their property[74] (in the form of bandwidth). Problematically, at the time of writing, this issue had not been judicially considered. Further, given the uncertainty and consequent problems in classifying bandwidth as property, it is unlikely a charge under s 81[75] for piggybacking would result in a successful prosecution.

An alternative offence, which is likely to produce more success in convicting those engaged in piggybacking unsecured wireless networks, would be under s 82 (obtaining a financial advantage by deception).[76] The advent of criminal prosecution for those who have obtained a financial advantage by deception using the aid of technology is not a new phenomenon,[77] thus the most effective means of dealing with criminal liability for piggybacking should be through s 82.[78] The main difference between obtaining a financial advantage by deception through

---

71 Nash and Bagaric, above n 62, 291.

72 Gerard Nash and Mirko Bagaric suggest that recklessness requires 'more than carelessness or negligence [rather it] must involve an indifference or disregard' as to whether the access to an unsecured wireless network is authorised. See, Nash and Bagaric, above n 62, 292.

73 Ibid.

74 *Director of Public Prosecution v Ray* [1974] AC 370.

75 *Crimes Act 1958* (Vic) s 81. For the relevant offence in New South Wales or the Australian Capital Territory see, s 326 of the *Criminal Law Consolidation Act 1935* (ACT); s 192C of the *Crimes Act 1900* (NSW).

76 *Crimes Act 1958* (Vic) s 82. For conduct which has occurred in the Australian Capital Territory, New South Wales or Tasmania see, s 332 of *Criminal Code Act 2002* (ACT); s 192D of the *Crimes Act 1900* (NSW); s 252A of *Criminal Code Act 1924* (Tas).

77 Russell G Smith, 'Crime Prevention in the Digital Age' (Paper presented at the Australian and New Zealand Society of Criminology Crime Power and Justice Conference, Brisbane, Australia, 8–11 July 1997) 1.

78 *Crimes Act 1958* (Vic) s 82. For conduct that has occurred in the Australian Capital Territory or New South Wales or Tasmania see, s 332 of *Criminal Code Act 2002* (ACT); s 192D of the *Crimes Act 1900* (NSW); s 252A of *Criminal Code Act 1924* (Tas).

piggybacking and past convictions involving technology is that the past convictions have used technology as a mechanism to obtain a separate financial advantage. Here, however, the financial advantage obtained by the piggybackers would be the actual usage of the Internet.

Currently we are faced with a situation where the access to the bandwidth itself is the financial advantage. Due to the failure of the *Crimes Act*[79] to define financial advantage, it is necessary to afford the term with its ordinary meaning. In looking at the natural meaning of the term financial advantage, it is clear that gaining access to the Internet either to use it for browsing or downloading is clearly a financial benefit whereby in obtaining such potentially unlawful access the perpetrator has the benefit of a wealth of information without having to pay a fee. In particular the benefit in using piggybacking is that it allows an individual to circumvent the requirement to pay for such access. In establishing a contravention of s 82[80] it would be necessary to show the same deception and dishonesty required under s 81,[81] which is essentially having an intentional or reckless mindset when piggybacking. In many instances this will easily be satisfied when an individual knows they are not authorised to access an unsecured wireless network or are indifferent to their access. Should the lawmakers in Australia decide to follow the international approach (in the United Kingdom and the United States), then the best option to obtain a successful conviction will be under s 82.[82] Importantly, it will be possible to obtain a conviction under s 82[83] even if the owner of the wireless network suffered no loss or no real inconvenience[84] due to the piggybacking.

---

79 1958 (Vic).

80 *Crimes Act 1958* (Vic) s 82. For conduct that has occurred in the Australian Capital Territory or New South Wales or Tasmania see, s 332 of *Criminal Code Act 2002* (ACT); s 192D of the *Crimes Act 1900* (NSW); s 252A of *Criminal Code Act 1924* (Tas).

81 *Crimes Act 1958* (Vic) s 81.

82 *Crimes Act 1958* (Vic) s 82. For conduct that has occurred in the Australian Capital Territory or New South Wales or Tasmania see, s 332 of *Criminal Code Act 2002* (ACT); s 192D of the *Crimes Act 1900* (NSW); s 252A of *Criminal Code Act 1924* (Tas).

83 Ibid.

84 *R v Kovacs* (1974) 1 WLRR 370; *Smith v Koumourou* (1979) RTR 355; *Ho and Szeto v R* (1989) 39 A Crim R 145.

An alternative option to prosecute individuals engaged in activities resulting in unauthorised access to unsecured wireless networks is for law enforcement agencies to bring an action under the *Criminal Code 1995* (Cth). Perhaps greater success will be achieved through the use of such provisions because this Act was enacted specifically to target criminal activities which use either a computer or the Internet.[85] Potentially the action of piggybacking falls within two of the more serious offences created by the Act: namely s 477.1 (unauthorised access modification or impairment with intent to commit a serious offence)[86] and s 477.3 (unauthorised impairment of electronic communications).[87] Furthermore, it would be possible also for a prosecution to proceed under s 478.1 (unauthorised access to or modification of restricted data)[88] or s 478.3 (possession or control of data with intent to commit a computer offence).[89]

In looking at s 477.1[90] a conviction would be granted if it could be shown an offender accessed an unsecured wireless network with the knowledge the access is unauthorised and the individual intended to commit a serious offence. This offence could only be committed if the individual engaged in piggybacking was also in the process of committing an ancillary offence. Essentially it would be necessary to show that the piggybacking was merely a means to assist in the commission of a different criminal offence. In most instances it would be easy to prove the actual access to the wireless network, often with intent to connect to the unsecured wireless network. The commission of a serious offence will be more problematic and is a matter beyond the scope of this paper.

Furthermore, s 477.3[91] is unlikely to result in a satisfactory claim given an actual impairment to the electronic communication (bandwidth). The reason why it would be difficult to successfully establish such

---

85 Tony Krone, *High Tech Crime Brief No. 5: Hacking Offences (2005)*, Australian Institute of Criminology <http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb005.aspx> at 1 April 2010.

86 *Criminal Code 1995* (Cth) s 477.1.

87 *Criminal Code 1995* (Cth) s 477.3.

88 *Criminal Code 1995* (Cth) s 478.1.

89 *Criminal Code 1995* (Cth) s 478.3.

90 *Criminal Code 1995* (Cth) s 477.1.

91 *Criminal Code 1995* (Cth) s 477.3.

a case is because in most instances of piggybacking there is no real loss or change to the usage or access to the Internet. The definition of impairment specifically excludes a mere interception, which is often what piggybacking would be characterised as, particularly if it is conducted by individuals who are only using it for basic browsing and checking of emails. Rather this offence is more likely to be satisfied if there is computer 'whacking' (deliberately accessing a 'Wi-Fi network for destructive, malicious, theft or espionage purposes'),[92] as opposed to someone piggybacking to browse the Internet. It is, however, possible, although unlikely, to be upheld in the courts that a reduced performance of an Internet connection or a reduction of the amount of bandwidth available may be sufficient to amount to an impairment for the purposes of this offence. This is problematic for the application of this Act and certainty in prosecuting offenders, whereby not only is the action of piggybacking necessary, but also the consequence occasioned by the piggybacking conduct must result in detriment. One of the biggest issues with this is that potentially it will create uncertainty in the prosecution of piggybacking. In particular it will create uncertainty as to when piggybacking will create a detriment sufficient to establish guilt under the Act. Thus prosecutions under this section would potentially create confusion as to the application of the law and will further complicate the issue of piggybacking and the legality of such an activity. Individuals, therefore, will be confused as to when they may lawfully be involved in piggybacking and when engaging in this conduct will result in a criminal conviction. As such it is less feasible to pursue an offender based upon either of the two potentially applicable serious offences created by the *Criminal Code*.[93]

For unsecured wireless networks it would be difficult to establish s 478.1[94] due to the requirement of access to restricted data. The unauthorised access can easily be proven simply by the action of piggybacking; however, this is unlikely to be a contravention if there are no security measures in place to protect the data and bring it within the definition of restricted data.[95] Similarly it would be difficult to prosecute under s 478.3[96] if an individual is merely accessing an unsecured wireless

---

92 Kern, above n 16, 105–106.

93 *1995 (Cth)*.

94 *Criminal Code 1995* (Cth) s 478.1.

95 *Criminal Code 1995* (Cth) s 478.1 (3).

96 *Criminal Code 1995* (Cth) s 478.3.

network for personal browsing. Rather it is essential that the purpose for which the unsecured wireless network is accessed is for the individual to obtain data or other information which can then be used to facilitate the commission of a serious computer offence under Division 477.[97]

V Civil Contravention Piggybacking: an Australian Perspective (Civil Liability — Tort of Conversion?)

A viable alternative to 'punish' those engaged in unlawfully accessing unsecured wireless networks is for the owners of the network to take a civil suit against the perpetrator using the tort of conversion. Currently there are no Australian cases which have used conversion for piggybacking. Further, no courts in either the United States[98] or the United Kingdom have allowed this course of action. There are currently, however, substantial academic writings promulgating the introduction of an actionable tort of conversion for piggybacking, particularly within the United States.

The impetus for the use of the tort of conversion can be summarised as follows:

> It is important for the law to provide remedies for every type of wrongdoing. Due to the current and ever growing technology boom many wrongs go undetected and unpunished. Although it is customary for the law to lag behind and then ride on the coattails of social progress the rapid evolution of technology threatens to make the gap between law and society increasingly wide [therefore there is a] need to recognise the need for the law to catch up or at least to chase after the emerging property rights which technology creates. Not only will wireless Internet form the basis of a claim but by broadening the application of conversion…can anticipate future forms of intangible property.[99]

---

97 *Criminal Code 1995* (Cth) s 478.3 (1)(b).

98 Guillot, above n 55, 390–391, 415; Laura D Mruk, 'Wi-Fi Signals Capable of Conversion: The Case for Comprehensive Conversion in Illinois' (2008) *Northern Illinois University Law Review* 347, 367–373; Mary W.S. Wong, 'Cyber-Trespass and "Unauthorised Access" as a Legal Mechanism of Access Control: Lessons from the US Experience' (2007) 15 *International Journal of Law and Information Technology* 90.

99 Mruk, above n 98, 373.

The tort of conversion is dealing with goods (including bandwidth)[100] in a way which is inconsistent with the lawful owner's rights.[101] For the tort of conversion to be actionable, the interference with property must be a serious interference with the owner's use and enjoyment of the bandwidth. This serious interference can be proven in piggybacking where the effect is 'causing computers to slow down [or to] take up the bandwidth of the [victim's unsecured wireless network] Internet connection.'[102] The reason why such behaviour can be classed as an act of conversion is seen through the need to ensure that the term 'goods' is given a wide definition. It is conceivable that bandwidth may be classified as goods should this term be afforded with a wide definition.[103]

In deeming bandwidth to be goods for the purpose of conversion, it is necessary to then look at the interference with the Internet connection. 'The key to identifying conversion lies in the level of interference imposed'[104] on the unsecured wireless network. Importantly, provided that the effect of piggybacking was to cause interference with the owner's right to use their network unencumbered then this would be sufficient interference to satisfy the requisite element required to prove conversion. If an action is taken for conversion, and it can be proven that the piggybacking was engaged in it, it does not matter whether this action was dishonest or there was intent to deprive[105] the unsecured wireless network owner of their rights to use the Internet.

The tort of conversion should be modernised and extended to the application of piggybacking of unsecured wireless because '[d]evelopments in electronic commerce have meant that intangible rights can be converted through manipulation of electronic data.'[106] The introduction of this tort would recognise the importance of the Internet in modern society and the need to alter our existing legal system so

---

100 Danuta Mendelson, *The New Law of Torts* (2007) 185.

101 R P Balkin and J L R Davis, *Law of Torts* (4th ed, 2009) 61– 93.

102 *CompuServe Inc v Cyber Promotions Inc* 962 F Supp 1015 (SD Ohio, 1997)1027.

103 Ali, above n 59.

104 Mruk, above n 98, 356.

105 Balkin and Davis, above n 101, 72–79.

106 Mendelson, above n 100, 198.

that it acknowledges that technological advances are essential to the functionality of a modern world.

Extending the tort of conversion to piggybacking will hopefully raise public awareness of the issue and evidence the law's distaste for such conduct. This should in turn prevent many individuals who would have otherwise engaged in piggybacking behaviour (particularly amateurs with very little knowledge of the Internet) to discontinue such behaviour. The mere threat of being sued should successfully act as a deterrent, dramatically reducing the number of individuals engaged in piggybacking unsecured wireless networks. In addition to preventing people from piggybacking, the extension of this tort should also be used to alert the owners of unsecured wireless Internet networks to put security measures into place to alleviate the problem of piggybacking, and perhaps the amount of damages available can reflect the owner's attempts to protect their own network.

VI Conclusion

It is more than likely that a combination of technological improvements in Wi-Fi hardware (and software) along with increased consumer awareness will start to rapidly reduce the number of open or unsecured wireless networks. The perpetration of piggybacking will become far more difficult, although it's unlikely that it will disappear entirely. As we discovered, in both the United States of America and the United Kingdom, zealous law enforcement officials have brought about successful prosecutions for piggybacking through a combination of long standing computer crime legislation[107] along with newer technologically savvy legislation.[108]

Australia, too, has a fertile landscape of legislation and the potential for common law developments to pursue piggybackers. From the most fundamental aspects of criminal law through to specific legislation targeting cyber criminals, and in conjunction with our existing criminal laws on obtaining a financial advantage by deception, reasonable grounds exist for prosecution to be sought with respect to individuals piggybacking. Although legally we do have the means for prosecution,

---

[107] *Fraudulent Access To Computers, Computer Systems, and Computer Networks Act* 53 USC (1979).

[108] *Communications Act 2003* (UK) s 125.

there has been a marked reluctance in Australia to prosecute and use the criminal system to curtail the unauthorised access to unsecured wireless networks.

One justification for the lack of active enforcement through the criminal system for those engaged in piggybacking may be inherent in the Australian psyche and egalitarian attitude that may be said to justify access as acceptable behaviour in an online world. In reality, however, perhaps it should not be the role of the State to police the use of unsecured wireless networks, but rather there should be a greater obligation on individuals to put security measures into place to protect their own interests.[109] Perhaps given the unique nature of the Internet and the fact that the technology is changing constantly suggests that it may be more beneficial for 'technology not the law to be a prominent regulatory institution of cyberspace'.[110] Although it is essential for technology to help in the war against piggybacking, this needs to be done in conjunction with a fair and efficient legal system prohibiting and punishing such behaviour as well as technology preventing such behaviour. If the focus on increasing security is made, then this should eliminate much of the problem of piggybacking.

In Australia, rather than exploiting the resources of the criminal system for piggybacking, there should be an emphasis on ensuring those who have a wireless network take measures to secure their own networks. Furthermore, it may be more appropriate to leave 'punishment' for accessing such networks to our civil system through an action in the tort of conversion, thus putting the enforcement on the victims who are affected by the actions of piggybackers.

---

[109] Peter N Grabosky, Russell G Smith and Gillian Dempsey, *Electronic Theft: Unlawful Acquisition in Cyberspace* (2001) 6.

[110] Ibid 7.