Straw, Sticks or Bricks – How to Stop the Big Bad Wolf from Piggybacking

By Jessica Goulburn

Table of Contents

Introduction

In April 2011 a homeowner from Buffalo, New York was awoken to the sounds of "paedophile", "pornographer" and "creep" before being slammed to the floor by federal police officers. Police searched the man's computer, along with his wife's, and within three days, officers determined the man's innocence. Someone must have been leaching his internet connection. Approximately a week later, a 25-year-old neighbour was arrested and charged with distribution of child pornography.[1] In today's world of immediate and constant access to the internet, how important is it to protect your wireless signal? If you ask that Buffalo man, imperitive.

When it comes to wireless connectivity there are several important questions that need to be answered. Should the law prohibit access to open wireless networks? Can statute and/or common law protect the rights of wireless network owners? And furthermore, is the casual user the only person at fault?

Wireless Connections: The Technology Behind It

Closely intertwined with everyday life, the internet has changed the way individuals communicate with each other in many facets of life. The introduction of wireless capability has furthered the internet's influence on civilisation. The expectation that people be available anywhere, anytime has been greatly supported by the *ability to be* available anywhere and at anytime.

---

[1] "Innocent Man Busted for Child Pornography after Neighbour Leached Wi-Fi", *Sydney Morning Herald*, 26 April 2011. Accessed online: <http://www.smh.com.au/technology/technology-news/innocent-man-busted-for-child-porn-after-neighbour-leached-wifi-20110426-1dugz.html?from=smh_sb>

A Brief History of the Internet

From its prosaic inception as a defence mechanism against the Soviet Union, the internet has since developed into a global communications tool.[2] When Sputnik I[3] beat the United States into space, President Eisenhower introduced a new agency to develop research strategies for civilians and the military – The Advanced Research Projects Agency. A network of machines was designed that would allow researchers in different parts of the country to share results and resources – The Advanced Research Projects Agency Network.

However, what was needed was a network of networks – an internetwork. The Transmission Control Protocol/Internet Protocol (TCP/IP) involved an open-architecture network environment, allowing easier communication.

The modern internet, founded on the principles of the TCP/IP protocol is still quite different from what was originally used. This is largely due to the developments during the 1990s during which the internet slowly came to life around academic networks. Decreased regulation allowed for commercial exploitation and further development. This allowed for greater growth of the network and greater access by internet users. Since these developments, society has seen the expansion of the internet through the next generation of connectivity – Wi-Fi.

Moving into the Noughties: The Wireless Age

Wi-Fi, short for wireless fidelity, breaks through the physical boundaries of the Internet by allowing users to gain access via radio frequencies along a bandwidth.[4] As with previous internet connections, users pay internet service providers a fee and in return are provided with a certain amount of access to the bandwidth.

---

[2] Information under this heading is based on research done through various textbooks including:
Murray, Andrew D. *The Regulation of Cyberspace. Control in the Online Environment*. (UK, Routledge-Cavendish, 2007). Chapter 3.
Bowrey, Kathy. *Law and Internet Cultures.* (Australia, Cambridge University Press, 2005). Chapter 1-2.
Reed, Christopher. *Internet Law: Text and Materials*. (UK, Butterworths, 2000). Chapter 1.
As well as: Leiner, Barry M., Cerf, Vinton G., Clark, David D., Kahn, Robert E., Kleinrock, Leonard, Lynch, Daniel C., Postel, Jon, Roberts, Larry G., and Wolff, Stephen. *A Brief History of the Internet*. Internet Society Website. <http://www.isoc.org/internet/history/brief.shtml>

[3] Sputnik 1, launched by the Soviet Union, was the first artificial satellite to be put into Earth's orbit.

[4] Wi-Fi Alliance Official Website. <http://www.wi-fi.org>

With regards to security, Wi-Fi devices provide a range of options. If a connection is left unsecure, there are obviously many risks,

> "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 connection ('piggyback')."[5]

Two common encryption methodologies used are Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA/WPA2). While WEP merely protects against intruders by prompting for a password when a connection is established, WPA2 provides security (via password) and privacy – with the algorithm preventing outsiders from being able to read transmissions.[6]

There are many reasons why users leave their internet connection unsecured including an intimidation of the technology, a lack of awareness and concern of the risks, and a desire to share access with those who need it or want it.[7]

Isn't a Piggyback a Free Ride from a Friend?

In relation to the internet, piggybacking describes the process of establishing a wireless internet connection by using another subscriber's access service without permission.

Today, people have become accustomed to being constantly connected to others. This has greatly influenced the culture of piggybacking, "Users who have become accustomed to connecting to the internet using Wi-Fi in the home or at the office have increasingly searched for ways to continue using Wi-Fi access to the internet while on the road."[8]

Piggybacking allows for anonymity, which means that usually the owner of the network does not know that someone else is connected. Often, it is not the owner

---

[5] Carter, Rachel Anne and Makin, David. *Piggyback Hunting – Browsing the Internet in Australia via Unsecured Wireless Networks: Virtual Theft or Acceptable Behaviour in an Online World?* (2009, James Cook University Law Review, Vol. 16, pages 20-41). Page 24.
[6] Wi-Fi Alliance Official Website. <http://www.wi-fi.org>
[7] Bierlein, Matthew. "Policing the Wireless World: Access Liability in the Open Wi-Fi Era." (2006) *Ohio State Law Journal*, Volume 6:1123. Page 1131.
[8] Kern, Benjamin D. *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*. (December 2005, CIPerati, Volume 2, Issue 4). Accessed online: <http://apps.americanbar.org/buslaw/committees/CL320010pub/newsletter/0009/>

reporting a piggybacker but rather an outsider who has observed the piggybacker and has a suspicion of illegal activity.

In 2005, UK man Gregory Straszkiewicz was arrested by police in West London. To outsiders, who had seen him in the area time and time again, his behaviour was suspicious. The case, brought under the *Communications Act 2003*, was the first one in the UK of its kind. Straszkiewicz was found guilty of dishonestly obtaining an electronic communications service.[9]

What is important about Straszkiewicz's case and the case about the Buffalo man, is that in each example, it was not the owner bringing the prosecution. This is largely due to the fact that the owner probably did not know it was occurring. This can be linked to the idea of responsibility and whose responsibility it is to avoid piggybacking.

Is it Really Unauthorised if it is an *Open* Network?

An important question to ask is on whom the onus of fault rests when accessing an open network. If it is there for the taking, why not use it? While it is often common to compare non-secure Wi-Fi connections to an unlocked door, it is true to say that it is more like using a stranger's utilities. Piggybacking is not going into a network, peeking around and taking a document, but rather it is going into a network and using it for one's own needs. This is more like going onto someone's front lawn and using their hose to wash your hands. Furthermore, unless a door is physically open, it is often not known that it is unlocked. In comparison, most connectivity devices automatically identify an unsecure network; it is advertised as being available.

The Case For Using Unsecure Networks

Advocators for the practice of piggybacking tend to believe that it is harmless and beneficial for the casual user without creating an expense to others. Imagine you are sitting behind someone on the train, and something in their newspaper catches your eye. Is this stealing?

---

[9] Wakefield, Jane. "Wireless Hijacking Under Scrutiny". *BBC News Online*. <http://news.bbc.co.uk/2/hi/technology/4721723.stm>

An argument for the use of Wi-Fi networks is that it allows for portability. Prior to wireless internet, a user was chained to a desk in order to conduct research, chat to friends and check emails. The ability to access wireless technologies from anywhere can, add flexibility and facilitate productivity and efficiency for users.[10] This can sometimes involve piggybacking onto unsecure networks.

Another positive argument for the free use of unsecure network connections is Lawrence Lessig's observation of online marketplaces. Lessig notes that the online marketplace "benefits greatly from a network that is open and where access is free… and to the extent that individual sites begin to impose their own rules of exclusion, the value of the network as a network declines."[11]

The Case Against Using Unsecure Networks

In contrast, there are several arguments against keeping Wi-Fi free and open. While most of the time unsecure network connections are simply used to surf the web or check websites, what happens when a piggybacker uses too much? When too much data is used, high-speed access tends to slow. This is often when owners of the internet connection start to catch on.

A major concern surrounding the use of unsecure networks is security. While most piggybackers simply use an open network to stay connected and check emails, there will be some cases where access is used to intercept data and read or even modify files on the network.

Consumers need to understand that an open wireless network invites greater vulnerabilities than initially understood, "the best case is that you end up giving your neighbour a free ride… the worst case is that someone can destroy your computer, take your files and do some really nefarious things with your network that gets you dragged into court."[12] Accidently stumbling on information or actively seeking it out, if there is an unsecure network available, there is a major risk of information finding its way into the wrong hands.

---

[10] Kern, Benjamin D, *op. cit.* (2005) <http://apps.americanbar.org/buslaw/committees/CL320010pub/newsletter/0009/>
[11] *Intel Corporation v Hamidi*, 71 P.3d 296, 310-11 (Cal. 2003).
[12] Marriott, Michael. "Hey Neighbour, Stop Piggybacking on my Wireless." *The New York Times*, 5 March 2006. Accessed online: <http://www.nytimes.com/2006/03/05/technology/05wireless.html>

As well as security concerns, there is also the issue of moral and ethical matters. While many state that piggybacking is harmless, others criticise it. Terms such as ‘leaching’ and ‘freeloading’ come to mind. One of the biggest ethical problems is that the casual user is doing just that – casually *using* a network without assisting in payment. The casual user is obtaining a benefit without suffering any detriment. Instead, the detriment is upheld solely by the owner of the network.

Whose Responsibility?

When looking at the dangers of piggybacking, who is actually at fault? Does the responsibility fall solely on the casual user or should the owner of the network share the blame?

Nowadays it is simple to set up an internet connection. You just plug in the modem and the router to allow for wireless capabilities and off you go. Right? Wrong! Most connectivity devices are accompanied by manuals or prompt users via pop-ups and questions during the installation process. It is the owner’s responsibility to read these and secure their network. If the owner chooses to install the device without protection, then surely the owner has accepted responsibility. While the onus could lie with the owner in relation to setting up security measures, this does not apply with regards to the ethical and moral issues.

In terms of security and responsibility, it is imperitive to look at the intention of the owner of the network. While a WEP password may be easy to crack, the mere fact that a password has been set implies that the owner does not want people gaining access to it. This is similar to a ‘no trespassing’ sign. While easy to bypass and enter the property, the intention of the owner is clear.

Wi-Fi networks are everywhere, easily located on a connectivity device. As such, if the network is not secure, how does a user determine whether the network is intended to be public or private? The assumption would clearly be that it is open and available to be used.

Another reason why the owner must bear some responsibility is that many devices connect to a nearby network automatically. The user may not know that they are not authorised to use the network that their device has connected to. But should connection to a Wi-Fi network, whether innocently or deliberately, be illegal?

Issues of Legality

Prosecution in Australia for piggybacking has not occurred as yet. In order to determine how this issue might be dealt with under Australian law the, application of the *Crimes Act 1900* (NSW)[13] and the *Criminal Code Act 1995* (Cth) will be analysed.

Criminality Under New South Wales Law

A possible crime with relation to piggybacking would be theft. Part 4 of the *Crimes Act 1900* (NSW) (The Act) deals with stealing and similar offences. Thus it would need to be determined that property is being dishonestly acquired. However, can the bandwidth that is used by the piggybacker be considered property?

"Property" is defined under The Act as "every description of real and personal property"[14] which can suggest that the definition encompasses both tangible and intangible objects. It has been suggested that a bandwidth is a tradable commodity.[15] This has been compared to the action of making a telephone call, "property cannot be appropriated unless it is in existence," and the making of a telephone call does not actually deprive anyone of anything, although the maker of the telephone call will have to pay for the usage.[16] When looking at this statement with relation to wireless networks, it can be argued that a bandwidth cannot constitute property as the owner of the open network does not actually suffer any consequences so long as the casual user does not alter anything on the network, especially the owner's ability to make use of it.

Therefore, perhaps the crime is better suited to be prosecuted under the offences relation to fraud, found in Part 4AA of The Act. Section 192E(1) outlines the offence of fraud, stating:

> *(1) A person who, by any deception, dishonestly:*

---

[13] Although the *Crimes Act 1900* (NSW) will primarily be used, please note that there are equivalent or juxtaposed provisions in the other Australian states and territories. See, *Criminal Code Act 2002* (ACT); *Crimes Act 1958* (Vic); *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).

[14] *Crimes Act 1900* (NSW) Section 4

[15] 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.

[16] Carter, Rachel Anne and Makin, David. *Op. Cit.* (2009) Page 32.

(a) obtains property belonging to another, or
(b) obtains any financial advantage or causes any financial disadvantage, is guilty of the offence of fraud.

In order to prosecute under Section 192E, it must be shown that a person obtained property, by deception or dishonesty, and the property belonged to someone else. If bandwidth can be classified as property, a piggybacker could be charged under Section 192E(1)(a). However, even if bandwidth is not understood as property, a piggybacker may still be charged under Section 192E(1)(b). By using the bandwidth, without the owner's knowledge, a piggybacker may cause financial disadvantage. As with any other product, when you run out of bandwidth, it is necessary to buy more. This is usually billed to the owner.

In order to fully understand this provision it is necessary to discuss Division One.

Section 192B defines deception as,

(1) …any deception, by words or other conduct, as to fact or as to law, including:
(a) a deception as to the intentions of the person using the deception or any other person, or
(b) conduct by a person that causes a computer, a machine or any electronic device to make a response that the person is not authorised to cause it to make.
(2) A person does not commit an offence under this Part by a deception unless the deception was intentional or reckless.

By connecting to an unsecure network, a casual user is causing an electronic device, the router, to respond to his or her requests, a response that the piggybacker is not authorised to make. In accordance with subsection (2), it would be necessary to prove that the casual user intended to cause the router to act in such a way. While the piggybacker may not intend for deception to take place, by wirelessly connecting to the network the piggybacker is showing his or her intent to use the unsecure network. By typing in a web address or checking emails, the piggybacker is showing his or her intent to request a response from the router.

Section 192C[17](1) states,

"For the purposes of this Part, a person "obtains property" if:
(a) the person obtains ownership, possession or control of the property for himself or herself or for another person, or
(b) the person enables ownership, possession or control of the property to be retained by himself or herself or by another person…"

By piggybacking, the casual user effectively gains control, albeit not complete

[17] There are similar offences for obtaining property by deception under s326 of the *Criminal Law Consolidation Act 1935* (ACT) and under s81 of the *Crimes Act 1958* (Vic).

control, of the bandwidth for himself. Looking at the definitions of retained and obtained, piggybacking would fit subsection (1)(b). According to the Oxford Dictionary, retain means to "keep in one's possession."[18] In contrast, obtain is defined as "come into possession of."[19] "Keep in one's possession" implies the idea of 'forever'. On the other hand, obtaining something is coming into possession of it. The definition says nothing about holding onto it.

However, subsection (2) states *"A person does not commit an offence under this Part by obtaining or intending to obtain property belonging to another unless the person intends to permanently deprive the other of the property."* The key words in this part are intention and permanently.

Most casual users do not intend to permanently deprive the owner of the use of the bandwidth. Most do not intend to deprive the owner *at all*. The amount of bandwidth used by the casual user is usually so insignificant that the network owner does not notice, and is not affected by, the loss. Furthermore, it would be necessary for authorities to prove intention to *permanently* deprive. To determine this, it is necessary to look at subsection (4), which states that whether or not permanency is a factor in the use of the property, if the person's intention is to treat the property as his own, intention to permanently deprive can be inferred.[20]

A casual user effectively obtains use of property, for a specific amount of time, before disconnecting, at the piggybacker's own request. This is without the knowledge or input of the owner. However, it is questionable whether this borrowing is for a significant amount of time. Of course, this would be determined on a case-by-case basis and the key would be proving that the piggybacker had knowledge that they were not entitled to use the bandwidth, but connected anyway,

> "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."[21]

This can be linked directly back to Section 192B.

As with most crime and intention, the standard of mens rea must be determined in

---

[18] *The Australian Combined Dictionary and Thesaurus*. (Australia, Oxford University Press, 1999). Page 92.
[19] Ibid. Page 94.
[20] *Crimes Act 1900* (NSWA) Section 192C(4).
[21] Carter, Rachel Anne and Makin, David. *Op. Cit.* (2009) Page 33.

order to prosecute a piggybacker. It is imperitive to understand that some wireless enabled devices connect automatically to an unsecure network without the user knowing. In these circumstances, there would be no contravention of The Act as intent is absent. It is also important to note that it is not necessary for the owner of the bandwidth to know that the network has been tampered with. It is enough that the act of deception leads the owner of the network to part with his or her property, that is, the bandwidth.[22]

Criminality Under Commonwealth Law

Bringing action under Commonwealth law is an alternative path for prosecution. In 2001, the *Cybercrime Act 2001* (Cth) amended the *Criminal Code Act 1995* (Cth) (The Criminal Code) to include chapter ten, which focuses on national infrastructure, including computer-related offences.[23] When analysing The Criminal Code it becomes clear that piggybacking might fall within two serious offences – section 477.1 which deals with the unauthorised access, modification or impairment with intent to commit a serious offence and section 477.3 which deals with the unauthorised impairment of electronic communication.

Section 477.1 states that a conviction would be granted if a person causes unauthorised access to, or modification or impairment of, data held in a computer. Subsection (1) also notes that the unauthorised access, modification or impairment has to be caused by means of a carriage service and the person must know that such behaviour is unauthorised. However, in order to satisfy this provision, the person must have the intention to commit a serious offence[24] of the Commonwealth or a State or Territory. Thus, a piggybacker could only be prosecuted under this offence if he or she is involved in an additional offence, and the act of piggybacking acted as assistance in the commission.

Section 477.3 outlines the offence of unauthorised impairment of electronic communication. It is unlikely that a conviction could be sought under this provision. A

---

[22] Ibid. Page 34.
[23] *Cybercrime Bill 2001* and *Explanatory Memorandum* as accessed via ComLaw <http://www.comlaw.gov.au/Details/C2004B00915/Explanatory%20Memorandum/Text>
[24] 'Serious offence' is defined in the *Criminal Code Act 1995* (Cth) as an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for life or for a period of 5 or more years (Section 473.1).

conviction would mean that a piggybacker caused some kind of damage to the bandwidth used. Section 476.1 defines impairment of electronic communication as "the prevention of any such communication or the impairment of any such communication on an electronic link or network used by the computer." The definition does not contain the words 'interception', 'interrupt' or 'disrupt' which are often classified as characteristics of piggybacking. This is especially true when the piggybacker is merely using the network to browse the internet or check emails. However, what happens when the browsing of the piggybacker causes the internet connection to slow so significantly that the owner is unable to use the network effectively? Surely this is grounds for a conviction as it has impaired the electronic communication usually enjoyed by the owner.

A problem with such a conviction is that there is a blurred line between innocently using a network without impairment, and when that use starts to damage the owner's ability to use their internet.

> "This is problematic for the application of this Act… not only is the action of piggybacking necessary, but also the consequence occasioned by the piggybacking conduct must result in detriment… In particular it will create uncertainty as to when piggybacking will create a detriment sufficient to establish guilt under the Act."[25]

Piggybacking may also fall within the realms of section 478.1 (unauthorised access to, or modification of, restricted data) and section 478.3 (possession or control of data with intent to commit a computer offence). However, it may be difficult to satisfy the requirement of access to *restricted data*. The act of piggybacking will certainly satisfy the criteria of access, yet because there are no security measures in place to protect the data, it is likely that it cannot be classified as restricted.

The Possibility of Civil Liability

A third option for the prosecution of piggybacking is through civil law. Owners of affected networks may bring a civil action against piggybackers using the tort of conversion. This has not yet occurred in Australia and courts in the United States or the United Kingdom have not allowed this course of action.[26] However, that is not to

---

[25] Carter, Rachel Anne and Makin, David. *Op. Cit.* (2009) Page 37.
[26] Carter, Rachel Anne and Makin, David. *Op. Cit.* (2009) Page 38.

say that it may not be effective. The tort of conversion has been discussed in relation to technology,

> "Due to the current and ever growing technology boom many wrongs go undetected and unpunished… 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."[27]

Essentially, the tort of conversion involves dealing with goods in such a way that is inconsistent with the owner's rights. The interference must seriously obstruct the owner's use and enjoyment of the good. Lord Nicholls outlined the key elements of the tort of conversion stating,

> "First, the defendant's conduct was inconsistent with the rights of the owner… Second, the conduct was deliberate, not accidental. Third, the conduct was so extensive an encroachment on the rights of the owner as to exclude him from use and possession of the goods…"[28]

In order to be prosecuted, the piggybacker must knowingly and substantially impede the owner's right to use his or her internet connection. Substantial interference can occur when piggybacking has caused the computer and the network to slow so significantly, that the owner is unable to fully use or enjoy the facility. In this context, it is imperitive that the term 'goods' is given a wide enough definition in which bandwidth can fall.

Extending the tort of conversion to include interference with bandwidth will raise public awareness of the consequences of piggybacking. The threat of being sued will provide deterrence to those who seek to leach off other people's unsecure networks. Similarly, it may also emphasise the need for owners to secure their network.

---

[27] 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

[28] *Kuwait Airlines Corp v Iraqi Airlines Co (Nos 4&5)* [2002] 2 AC 883 (HL) at [39].

International Influences

International governments have sought ways to prohibit the use of open networks by casual users.

Britons could face legal action for leaving their Wi-Fi connection unsecure.[29] This was largely influenced by a German case where the top criminal court ruled that internet users must secure their wireless connection to prevent others from accessing the network and illegally downloading data. This puts the onus on the owner to protect their network from piggybackers.[30]

In the German case, a musician sued an internet user whose wireless connection was used to illegally download his music, which was subsequently posted online. Despite the owner being out of the country when the crime took place, the court found that the man was responsible, in part, for the download, as he had not taken any measures to prevent it.[31]

There are some practical aspects of this decision. Unless caught in the act, piggybackers are generally hard to find. However, the network owner is not doing anything *wrong* per se. It is not the network owner that is depriving someone of his or her ability to use their internet connection. It is not the network owner that is deliberately using someone else's "property". Why should the network owner be at fault?

In 2010, the United Kingdom introduced the *Digital Economy Act 2010* regulating digital media. While dealing more with the fact that open internet connection allows for illegal downloading, the introduction of the *Digital Economy Act 2010*, is still a step towards legislating against actions such as piggybacking. Under this Act, a subscriber may be sent notifications and eventually be disconnected from the internet by allowing someone else to use the connection to illegally download

---

[29] Mitchell, Stewart. "Brits Could Face Legal Action for Leaving Wi-Fi Unsecured", *PC Pro Magazine*, 18 May 2010. Accessed online: <http://www.pcpro.co.uk/news/security/358033/brits-could-face-legal-action-for-leaving-wi-fi-unsecured>

[30] "Innocent Man Busted for Child Pornography after Neighbour Leached Wi-Fi", *Sydney Morning Herald*, 26 April 2011. Accessed online: <http://www.smh.com.au/technology/technology-news/innocent-man-busted-for-child-porn-after-neighbour-leached-wifi-20110426-1dugz.html?from=smh_sb>

[31] "Germans Face Fines for Leaving Wi-Fi Unsecured", *TG Daily*, 13 May 2010. Accessed online: <http://www.tgdaily.com/business-and-law-features/49753-germans-face-fines-for-leaving-wifi-unsecured>

content.[32] While it is not defined what "allow" means, it may encompass the fact that the owner has not set a password and is therefore not taking appropriate measures to prevent illegal downloading by third parties.[33]

The idea of placing the onus on the owner of the wireless connectivity device to secure the network may assist in limiting piggybacking.

Conclusion

In today's paranoid word of terrorism, identify theft and cybercrime, it is imperitive that internet connections are secure. Whilst society has become accustomed to being constantly connected and available, that does not mean that it is right to exploit people's trust or ignorance of the dangers of leaving an internet connection unsecure. While the act of piggybacking is not yet illegal, the ethical and moral ramifications of the practice are questionable. Not only is a casual user exploiting the owner's rights to a private connection, but a piggybacker is also taking advantage of the fact that he or she is obtaining a service for free, while the owner bears the costs.

Although not the full responsibility of the owner, the onus needs to be shared (albeit not equally) between piggybacker and network owner. It is the piggybacker's responsibility to understand that it is morally wrong to use an open internet connection, no matter how little one uses the bandwidth. Similarly, it is the owner's responsibility to ensure that a casual user does not have the opportunity to use his or her internet connection by securing the network.

With many crimes assisted by computers and the internet, it is imperitive that owners secure their network. It is also imperitive that Australia legislates for practices such as piggybacking. It is wrong for individuals to dishonestly use the property of another. But just as wrong is for the rightful owner not to have an outlet to charge the offender.

Word Count: 4925

---

[32] See sections 124A, 124G and 124H of the *Digital Economy Act 2010*.
[33] Mitchell, Stewart. *Op. Cit.* (2010) <http://www.pcpro.co.uk/news/security/358033/brits-could-face-legal-action-for-leaving-wi-fi-unsecured>

Bibliography

Legislation

Crimes Act 1900 (NSW)

Criminal Code Act 1995 (CTH)

Cybercrime Bill 2001 and *Explanatory Memorandum* as accessed via ComLaw <http://www.comlaw.gov.au/Details/C2004B00915/Explanatory%20Memorandum/Text>

Digital Economy Act 2010 (CTH)

Cases

Intel Corporation v Hamidi, 71 P.3d 296, 310-11 (Cal. 2003).

Kuwait Airlines Corp v Iraqi Airlines Co (Nos 4&5) [2002] 2 AC 883 (HL).

Textbooks

The Australian Combined Dictionary and Thesaurus. (Australia, Oxford University Press, 1999).

Bowrey, Kathy. *Law and Internet Cultures.* (Australia, Cambridge University Press, 2005).

Murray, Andrew D. *The Regulation of Cyberspace. Control in the Online Environment*. (UK, Routledge-Cavendish, 2007).

Reed, Christopher. *Internet Law: Text and Materials*. (UK, Butterworths, 2000).

Newspaper Articles

"Germans Face Fines for Leaving Wi-Fi Unsecured", *TG Daily*, 13 May 2010. Accessed online: <http://www.tgdaily.com/business-and-law-features/49753-germans-face-fines-for-leaving-wifi-unsecured>

"Innocent Man Busted for Child Pornography after Neighbour Leached Wi-Fi", *Sydney Morning Herald*, 26 April 2011. Accessed online: <http://www.smh.com.au/technology/technology-news/innocent-man-busted-for-child-porn-after-neighbour-leached-wifi-20110426-1dugz.html?from=smh_sb>

Marriott, Michael. "Hey Neighbour, Stop Piggybacking on my Wireless." *The New York Times*, 5 March 2006. Accessed online: <http://www.nytimes.com/2006/03/05/technology/05wireless.html>

Mitchell, Stewart. “Brits Could Face Legal Action for Leaving Wi-Fi Unsecured”, *PC Pro Magazine*, 18 May 2010. Accessed online: <http://www.pcpro.co.uk/news/security/358033/brits-could-face-legal-action-for-leaving-wi-fi-unsecured>

Wakefield, Jane. “Wireless Hijacking Under Scrutiny”. *BBC News Online*. <http://news.bbc.co.uk/2/hi/technology/4721723.stm>

Journal Articles

Bierlein, Matthew. “Policing the Wireless World: Access Liability in the Open Wi-Fi Era.” (2006) *Ohio State Law Journal*, Volume 6:1123.

Carter, Rachel Anne and Makin, David. *Piggyback Hunting – Browsing the Internet in Australia via Unsecured Wireless Networks: Virtual Theft or Acceptable Behaviour in an Online World?* (2009, James Cook University Law Review, Vol. 16, pages 20-41).

Kern, Benjamin D. *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*. (December 2005, CIPerati, Volume 2, Issue 4). Accessed online: <http://apps.americanbar.org/buslaw/committees/CL320010pub/newsletter/0009/>

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

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.

Websites

Leiner, Barry M., Cerf, Vinton G., Clark, David D., Kahn, Robert E., Kleinrock, Leonard, Lynch, Daniel C., Postel, Jon, Roberts, Larry G., and Wolff, Stephen. *A Brief History of the Internet*. Internet Society Website. <http://www.isoc.org/internet/history/brief.shtml>

Wi-Fi Alliance Official Website. <http://www.wi-fi.org>