Ethics and Information Technology (2007) 9:179–186
DOI 10.1007/s10676-007-9139-1


# Theft in a wireless world

Luc Small
*Philosophy Program, School of Humanities, Faculty of Arts, The Australian National University, AD Hope Building (14), Canberra, ACT 0200, Australia*
*E-mail: Luc.Small@anu.edu.au*

**Abstract.** I explore philosophically the phenomenon of home wireless networks as used to share broadband Internet connections. Because such networks are frequently unsecured, third parties can use them to access the Internet. Here I consider carefully whether this kind of behaviour should be properly called theft. I begin with a brief non-technical introduction to 802.11 wireless networks. Subsequently, I present a four part argument – appealing to the unsecured nature of the networks discussed, entrenched software and hardware behaviours, trespass law, and the openness of 'public park' spectrum – suggesting that this kind of behaviour is permissible and should not be construed as theft. Substantively, I conclude that, despite the quite compelling considerations that these arguments bring to bear, this behaviour is theft. Additionally, I draw attention to significant flaws in the design and implementation of wireless technology (specifically in the out-of-the-box configuration for wireless access points and in the wireless connectivity of early versions of Windows XP) that facilitate the intentional and unintentional theft of Internet bandwidth. I suggest some simple mechanisms that could be incorporated into the technology which would serve to remove the ethical ambiguity in its usage by third parties, including adding the ability for a network owner to explicitly mark her network as not for public use, and changes to default hardware and software behaviours. I conclude by encouraging increased use of value-sensitive design practices in the development of future wireless technologies.

**Key words:** 802.11, broadband, ethics, internet, morality, network, theft, value, WEP, wireless, WPA

**Abbreviations:** ACA: Australian Communications Authority; CD: Compact Disc; IEEE: Institute of Electrical and Electronics Engineers; ISM: International Scientific and Medical; WEP: Wired Equivalent Privacy; Wi-Fi: Wireless Fidelity; WPA-PSK: Wi-Fi Protected Access Pre-Shared Key

This paper asks the question: *Can the use of a neighbour's wireless Internet access be considered theft?* In essence I seek to explore philosophically the phenomenon of home wireless networks, which are commonly used to share a broadband Internet connection amongst a number of computers. These wireless networks are frequently left unsecured and presently it is very easy for even a novice user to intentionally or unintentionally 'borrow' a neighbour's Internet connection (and consume Internet bandwidth) shared in this manner. Here I consider carefully whether this kind of behaviour should be properly called 'theft'.

The prevalence of this kind of 'borrowing' of Internet bandwidth is hard to judge given that in most instances it is likely to go, if not undetected, at least unreported. However, what motivates this paper is not so much whether the activity is prevalent (although my understanding is that it is) but rather how it should be understood when it does occur. Moreover, I am concerned to explore how the technology involved may help to facilitate such 'borrowing'.

The wireless technology that I am focusing on in this paper has come to be known informally as *Wi-Fi*. More formally it is referred to by the appellatives *802.11a*, *802.11b* and *802.11g*, which denote the Institute of Electrical and Electronics Engineers (IEEE) standards defining the technology.[1] Here I aim to provide an account of only those aspects of the technology that have bearing on the ethical issues that I shall identify later.

Wi-Fi networks are designed to provide an alternative means of networking computer systems when a wired network is deemed impractical or undesirable.

[1] Further revisions to the standards are presently under consideration. The proposed revisions, however, do not alter the basic characteristics of this technology.

Hence they have proved phenomenally popular in the home environment, which typically lacks the cabling required for a wired Ethernet network. In the United States, for instance, it is estimated that more than ten million homes are equipped with a Wi-Fi network.[2] For a technology that has only been in mass-market production for approximately 5 years, the uptake has been exceptional.

Most Wi-Fi networks are built around a wireless access point or router.[3] Any computer wishing to participate in the wireless network must be equipped with a wireless network card, which transmits outgoing network traffic to the access point, and listens for incoming traffic from the access point. In this manner all the computers on the wireless network can establish communication with each other via the access point. The access point is also typically connected to an upstream network, in most cases the Internet. In this fashion all the computers on the wireless network can gain access to the upstream network. The most common configuration in the home, naturally, has been to utilise a wireless access point as a means to share a broadband Internet connection amongst a number of computers.

Unlike traditional wired networks, Wi-Fi networks transmit their data over radio waves in the microwave portion of the electromagnetic spectrum. The set of frequencies allocated for Wi-Fi transmissions belong to the Industrial, Scientific and Medical (ISM) band.[4] The ISM has been set aside by international agreement and in Australia it is managed as licensed spectrum operating on a 'public park' concept.[5] Briefly, this means that the ISM can be used by anyone to broadcast any data, within limits. Under the 'public park' ethos, it is up to the various users of the band to limit interference between transmissions, and to thus peacefully coexist. For this reason, wireless networks typically broadcast at minute power levels, constraining the reach of their transmissions within a radius of thirty to three hundred metres or so. In this manner, the same broadcast frequency can be re-used by another network only a short distance away, without causing appreciable interference. It should be noted, however, that despite the limited range of the transmissions, they often reach significantly beyond the physical boundaries of the network owner's property.

In order to handle the fact that a wireless network is, by its very nature, subject to eavesdropping, wireless networking standards include mechanisms for encrypting data traffic before it is broadcast as a radio wave. Interception of the radio waves is of course still possible; however eavesdropping is rendered pointless if the appropriate key to decrypt the encrypted data payload is unknown. Unfortunately Wired Equivalent Privacy (WEP), the name given to an early version this kind of encryption mechanism in the IEEE standards, has proved ineffective in reality. It has been demonstrated that with reasonable levels of computer power, the required key can be reverse engineered from a reasonable sample of encrypted data (obtained via interception).[6] Wi-Fi Protected Access Pre-Shared Key (WPA-PSK),[7] a newer security implementation designed to address the shortcomings of WEP, has also been found to be susceptible to attack, although to a significantly lesser extent.[8]

Whilst the mechanisms for securing a home wireless network have, to varying degrees, been found to have their shortcomings, perhaps of more concern is the fact that, in the real world, such protections are often not used at all. By default most access point manufacturers leave the security options on their devices turned off. Not only does this render the wireless network susceptible to eavesdropping, but worse, it allows anyone with a computer in range of the network to join it. Hence the user's computer network becomes the playground of any interested third party with a computer and a wireless network card. The panacea to such an undesirable state of affairs, naturally, is to turn on the security settings of the access point. Unfortunately, however, many users

[2] Seth Schiesel, "Growth of Wireless Internet Opens New Path for Thieves," *The New York Times*, 19 March 2005.

[3] It is also possible for a wireless network to operate in 'ad-hoc' mode, in which computers communicate directly without an access point as intermediary.

[4] Australian Communications Authority, *Wireless Local Area Networks: Frequently Asked Questions* (2004 [cited 22 June 2005]); available from https://www.aca.gov.au/consumer_info/frequently_asked_questions/WLANs_FAQ.pdf.

[5] Ibid.

[6] See, for instance, Nikita Borisov, Ian Goldberg, and David Wagner, *Security of the Wep Algorithm* ([cited 7 February 2007]); available from http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[7] In addition to WPA-PSK, which is targeted at home and small business consumers, the WPA standard defines another security scheme targeted at enterprise users and not susceptible to the attacks mentioned. WPA-PSK is exclusively discussed here as the focus of this paper is on Wi-Fi usage in the home.

[8] See, for instance the following two-part discussion: Seth Fogie, Cracking Wi-Fi Protected Access (WPA), Part 1 (4 March 2005 [cited 7 February 2007]); available from http://www.informit.com/articles/printerfriendly.asp?p=369221&rl=1 and Seth Fogie, Cracking Wi-Fi Protected Access (WPA), Part 2 (11 March 2005 [cited 7 February 2007]); available from http://www.informit.com/articles/printerfriendly.asp?p=370636&rl=1.

are "just happy to make their access point work at all" and are reluctant to change their settings if their network is functioning correctly, as is.[9] Meanwhile the access point manufacturers are reluctant to change their defaults because it adds a degree of complexity to the installation of the network that might alienate potential users.

For these reasons a great many wireless networks are fair game for unauthorised access, creating the opportunity for the stealing of broadband Internet access. But is it really stealing when the attitudes of the manufacturers and users are so obviously problematic? Can anyone truly be blamed for *borrowing* a little Internet access under such circumstances?

To get some clarity on the matter, I will firstly supply a definition of theft for the purposes of this paper. Subsequently, I will offer a quite compelling four part argument suggesting that this kind of behaviour is permissible and should not be construed as theft. This argument firstly considers the unsecured nature of the networks discussed, which could be construed as giving the green light to utilising the Internet bandwidth. Secondly, it considers the behaviour of wireless networking in early versions of Windows XP, which would appear to assist in such activities. Thirdly, it considers whether property law might grant the use of Internet access as a compensatory measure for the incursion of wireless network signals onto the borrower's property, which might be understood as an act of trespass. Fourthly and finally, it argues that the openness of the 'public park' spectrum in which wireless networks broadcast implies an open access policy to unsecured networks. Despite the merits of this argument, I ultimately conclude that each proposal can be countered, and that the unauthorised use of a wireless network should be considered as theft.

In the concluding portion of the paper I suggest a number of improvements to the technology that would render it less ethically problematic by serving to clearly delineate an instance of theft from authorised access. Ultimately, I argue that when designing wireless network technology, greater priority needs to be given to assessing the ethical implications attendant to the technology.

## A definition of 'theft'

For the purposes of this paper, I will follow the definition of theft given in the Australian *Criminal Code Act 1995*, which follows closely the definition of theft given in the United Kingdom *Theft Act* of 1968.[10] Under this definition, an act of theft occurs when a "person dishonestly appropriates property belonging to another with the intention of permanently depriving the other of the property."[11] Thus, I take it that there are three central tenets to theft properly understood. Firstly, the perpetrator must deprive an owner of what is rightfully the owner's property. Secondly, the perpetrator, in depriving the owner of their property, must have acted with the intent to do so. And thirdly, following from the second point and as noted in the definition, the perpetrator must have acted dishonestly and is thus open to moral sanction. If any of these three conditions are not met then, arguably, a theft has not occurred.

## Four arguments for 'freeloading'

Having defined theft, I will now turn to four arguments that suggest that utilising a neighbour's wireless Internet bandwidth should not be considered theft. Each argument is proposed by a hypothetical figure I have termed 'the freeloader'. This character utilises any unsecured network, quite intentionally and without regard for the network owner. We might incline to call her a thief, but this is not how the freeloader sees it.

In the first instance, the freeloader argues that the network owner, in leaving his network unsecured, is signalling that it is acceptable for the freeloader (and anyone else) to use it. It is the case after all – as the freeloader will promptly remind us – that wireless networks have security mechanisms designed to restrict access to only authorised users. Whilst the most widespread of these security mechanisms, WEP (as noted above) is seriously flawed and easily compromised, its use by the neighbour would have signalled that the network is restricted to authorised users. Now the freeloader is prepared to admit that if she were to crack the WEP encryption so as to gain access to the network, she would be committing theft, by deliberately thwarting the barriers erected by the neighbour against unauthorised use. In the case of the unsecured wireless network, however, the

[9] Schiesel, "Growth of Wireless Internet Opens New Path for Thieves".

[10] See Ministry of Justice, *Theft Act 1968 (C. 60)* (Ministry of Justice, 1 February 1991 [cited 30 July 2007]); available from http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1204238.

[11] See 'part 7.2, Division 131 – Theft' of Attorney General's Department, *Criminal Code Act 1995* (Office of Legislative Drafting and Publishing, 30 December 2006 [cited 7 February 2007]); available from http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/2088CEAEEE78C48BCA25725C00838526.

freeloader is quick to insist that the neighbour has placed no explicit restrictions on its use, indicating that access is freely granted to all comers.

The second argument that the freeloader invokes closely relates to the first and is based entirely on precedent. The Microsoft Windows XP[12] operating system originally shipped with a wireless configuration utility that contained a simple algorithm for selecting between available wireless networks. Essentially Windows XP selected the 'first available wireless network', meaning that without user intervention Windows XP would connect to the first network for which it has the necessary security credentials (e.g., WEP keys) or, alternatively, the first available unsecured network. Because of its network selection algorithm, Windows XP would thus automatically connect to the neighbour's network, assuming it is the only available network. Knowing these facts, the freeloader argues that the wireless behaviour of Windows XP tends to suggest that it is generally accepted (at least by the programmers at Microsoft) that if a network is unsecured then it is free to be used. The implementation of wireless networking in the original Windows XP appears to carry the assumption – the freeloader stresses – that if a computer system is unsecured then access to it is implicitly granted to all users. The freeloader thus presents empirical evidence, namely the behaviour of wireless networking under Windows XP, in her second argument to strengthen the conclusion drawn in the first.

In waging her third argument the freeloader turns the table on the situation, suggesting that she, and not the network owner, suffers the greater harm from the networking arrangement. Far from thieving, the freeloader argues that she is actually tolerating what is, in reality, an act of trespass or encroachment by the neighbour onto her property. As partial recompense for damages thus done to her, the freeloader argues that she is entitled to utilise the neighbour's Internet bandwidth to whatever extent she desires. On the face of it, it seems that the freeloader can make a strong case for adopting such a perspective. The neighbour's radio transmissions do, after all, spill onto the freeloader's property, and the freeloader sees this as an invasion or violation of her space. The freeloader would not be alone in making such a conjecture, either; John Dvorak has run this precise line in a column in *PC Magazine*:

> Here's what I propose: Once a wireless signal leaves private property, it becomes public domain. ... If someone beams an Internet connection into my home and I happen to lock onto the signal, he is trespassing on me, not the other way around. ... Keep it out of my house if you don't want me using it. Keep it out of my car. Keep it away from me in public places.[13]

Trespass and encroachment inhabit an area of law that is both complex and fascinating. In the legal tradition the cases that most closely resemble the present one have typically involved instances in which a building or structure on a neighbouring property has occupied the airspace of an adjacent property. Overwhelmingly, it has been concluded that airspace constitutes part of the property, and hence, that it is an act of trespass to make an incursion into neighbouring airspace that would interfere with "the ordinary use and enjoyment of the land".[14] Consider, for instance, the case of *Kelsen v Imperial Tobacco Co (of Great Britain and Ireland) Ltd* (1957).[15] The plaintiff in this case issued a writ alleging trespass into the airspace above his shop after the owners of an adjoining building erected a sign above his shop. The sign was fixed to the adjoining building and protruded some eight inches over the airspace of the plaintiff's shop. In this case the judge ruled in favour of the plaintiff, upholding the allegation of trespass. By extension, the freeloader, in her third argument, argues that the incursion of the neighbour's radio transmissions into her airspace is an act of trespass, entitling her to some form of recompense, specifically Internet access. She would, of course, have to convincingly argue that the neighbour's wireless transmissions interfered with the "ordinary use and enjoyment" of her land. Perhaps she might argue that the neighbour's transmission effectively prevented her from setting up a wireless network at the same frequency on her land, without the risk of appreciable interference between the networks.

[12] I preface my comments by saying that it is not my intention to single out Microsoft Windows XP, because there are no doubt other software systems that exhibit similar behaviour. Additionally, it should be noted that the connection algorithm can be overridden by changing the operating system's configuration settings; however, the default in (most) original builds of the operating system is to have it operating as described. Subsequent Windows XP service packs have changed the default behaviour to not connect to non-preferred networks without first prompting the user.

[13] John C. Dvorak, *The Looming Legal Threat to Wi-Fi* (16 April 2004 [cited 22 June 2005]); available from http://www.pcmag.com/article2/0,1759,1565274,00.asp?kc=PCRSS03079TX1K0000584.

[14] Adrian Bradbrook, S MacCallum, and A Moore, *Australian Property Law: Cases and Materials*, 2nd ed. (Sydney: Thomson Lawbook Co., 2003), 1031.

[15] Ibid., 1026.

Despite maintaining the cogency of her last argument, the freeloader is willing to admit that it may perhaps be less than conclusive. Radio waves – the freeloader will grant – are intangible, of no mass and no extension, and as such they perhaps cannot be understood to trespass real property per se. But whilst such an intuition may or may not be defensible it is not clear, the freeloader insists, that it threatens the acceptability of her actions. To illustrate this, the freeloader volunteers a fourth argument. If we understand wireless network radio waves to inhabit a different property-space entirely to real property, then the most likely space they do inhabit is a kind of commons, described by the Australian Communications Authority (as I noted above) as being analogous to a 'public park' – a shared space in which,

> ... the planning objective is for all users to be able to access a small portion of the total resource (in this case a frequency band) and to share that resource in a way that requires minimal regulatory interventions.[16]

Under this schema the typical boundary lines of real property carry no sway, and hence the possibilities of trespass and encroachment are ruled out – annulling the freeloader's third argument. That said, the notion of a 'public park' suggests a very loose kind of participation in which once a participant *throws* something onto the 'public park' in the form of a radio wave, it becomes a kind of communal commodity. As a communal commodity it becomes everybody's property – the neighbour and the freeloader alike. This kind of sentiment is invoked in the Dvorak quotation above: "Once a wireless signal leaves private property, it becomes public domain".[17] Armed with this knowledge, the freeloader argues once more that her actions are permissible because she is utilising Internet bandwidth that has been given up freely, or at least implicitly (given the neighbour's participation in the wireless public park), by the neighbour to the public.

## Revisiting the arguments

The four preceding arguments suggest that the freeloader's unrestricted use of a neighbour's unsecured wireless network is completely permissible. The freeloader, it would seem, has successfully vindicated herself of all charges of theft. In essence she has established that it presents no moral dilemma to utilise any unsecured wireless network to the satisfaction of one's Internet needs. However, phrased this way, and despite the arguments waged above, this activity still sounds patently dishonest and very much like theft. Does this mean that our standard moral intuitions do not apply when it comes to cyberspace; that conventional notions of stealing do not apply? Or does it suggest that the freeloader's foregoing arguments contain a string of fallacies? I believe that the latter is the case, and I will presently dismantle the arguments, from last to first, to demonstrate why.

Turning first to the argument that anything broadcast on the 'public park' is implicitly public property I suggest that, pressed harder, it is completely indefensible. If a family takes a picnic hamper to a real public park it does not follow that that picnic hamper can be raided by any would be park attendee. The hamper remains the property of the family despite the fact that it occupies a proportion of the commons. By analogy it seems clear that a wireless network should not be considered public property simply because it inhabits the wireless public park. It still belongs to the network owner, just as the hamper and its contents belong to picnicking family. Hence to take from the hamper is to steal, and likewise, to consume Internet bandwidth is to steal. As such, the freeloader finds no vindication in invoking the notion that wireless networks inhabit a public park.[18]

The freeloader may rejoinder, however, that the picnic hamper example functions as a poor analogy to the case of wireless networks. Instead she proposes the following alternative. Imagine a family picnicking with a radio tuned in to a sporting broadcast. Meanwhile, another family, keen to follow the broadcast (but without a radio of their own), settles down to picnic within earshot of the first family's radio.[19] The freeloader argues that such an example bears closer analogy to her use of a neighbour's wireless network. In both cases, after all, one party

[16] Australian Communications Authority, *Wireless Local Area Networks: Frequently Asked Questions* (cited).

[17] Dvorak, *The Looming Legal Threat to Wi-Fi* (cited).

[18] That said the comments by Dvorak raise an interesting question at the intersection of philosophy, the law and broadcasting. Dvorak maintains a network owner can claim ownership of a signal within the bounds of their private property. This posits an essential relation between physical property and the radio wave broadcasts of the wireless network. The ACA's 'public park' model, by contrast, suggests that the wireless public park and real property inhabit different, unrelated and disparate property spaces. I believe there is much to be explored in the relationship between these different yet co-located property spaces, but so as not to depart from the core theme of the paper, I must flag it as an issue and move on.

[19] I am indebted to John Weckert for devising this thought experiment and putting it to me.

utilises a resource broadcast wirelessly on a public commons by another party.

Testing our ethical intuitions, the freeloader asks: is there anything wrong with the second family listening to the first's radio? The freeloader maintains that, intuitively, there is absolutely nothing objectionable about this behaviour. For this reason, she concludes it would be completely inappropriate to label the second family's conduct as theft. Given the close analogy between the case of the second family and her use of the neighbour's wireless network, the freeloader contends that her behaviour should, by extension, not be considered theft.

The freeloader's defence fails, however. It fails not because the freeloader's assertion that the second family has done nothing wrong is faulty. I happily accept that, in listening to the first family's radio, the second family commits no crime. It fails because the freeloader's example doesn't model an essential dimension of the use she makes of the wireless network. The freeloader (to recapitulate) consumes Internet bandwidth quite intentionally and without regard for the network owner. As a result the network owner is deprived of a resource that is rightfully his. The second family, by contrast does not deprive the first family of anything. By failing to model this element of deprivation the freeloader's alternative analogy fails to properly capture the dynamics at play in the case of wireless networks. The picnic hamper example, meanwhile, properly captures the fact that one party is deprived of what is rightfully theirs by another party and it is therefore the better, and telling, analogy.

Considering, secondly, the argument based on the claim of trespass, I argue that there is no relationship of entailment between an act of trespass and the receipt of some kind of recompense. Furthermore, I resist the notion that the freeloader can freely choose the form of recompense that she desires, namely unbridled use of the neighbour's wireless network. Consider, for instance, another case not far removed from *Kelsen* (1957) but somewhat closer to home. Frequently it is the case that one neighbour's tree will grow such that branches, leaves and fruit will encroach into the airspace above another neighbour's property. Here the law holds that an owner has "the right to lop the branches of trees that may overhang his boundary".[20] However, the owner can in no sense claim ownership of these branches, lopped or un-lopped. New South Wales law, for instance states: "Should any branches, roots and even fruit be removed they must be returned to the owner of the tree".[21] Hence the law is firm in insisting that the landowner has no rights to the spoils – the fruit, flowers, etc. – of the offending tree. By analogy it would seem that the freeloader has no right to the spoils – i.e., Internet access – of the intruding radio waves. The argument from trespass thus fails to give the freeloader legitimate grounds for using the neighbour's wireless network.

Lastly I turn to the first two arguments, the first of which suggested that if a network is unsecured then it implicitly invites public access and the second of which drew support for the first argument from the wireless networking behaviour of Windows XP. Clearly the first argument is highly questionable. If I were to find the front door of my neighbour's house wide open, I would not take this to mean that I could gain entry to the house. Furthermore, I would not feel it my right to take the odd item of furniture home with me. Therefore if the freeloader views her actions as defensible, she must additionally reject our strongest intuitions that walking into an unlocked house, which is analogous to connecting to an unsecured wireless network, and taking whatever we please, which is analogous to utilising the Internet connection, is morally prohibited. If this example feels too far removed from the computer environment, then consider our natural reaction if a computer system possesses a security flaw that allows a hacker to connect to a system and enjoy unrestricted use of its functions. Under such a set of circumstances we do not excuse the hacker on the basis that the system was poorly secured. Instead we hold him accountable for exploiting the system, and indeed for simply connecting to it. Yet such actions are entirely analogous to connecting to an unsecured network and siphoning off the Internet bandwidth. Additionally, the fact that the original Windows XP implements the kind of logic the freeloader invokes does not support the freeloader; it only suggests that the wireless behaviour of Windows XP is aberrant.

From these counter-arguments it is clear, I believe, that despite what looked like quite an impressive case assembled by the freeloader, her actions still can be understood under the conventional banner of theft. Despite all the arguments the freeloader can muster to the contrary, her actions, clearly, are tantamount to theft.

[20] Bradbrook, MacCallum, and Moore, *Australian Property Law: Cases and Materials*, 1029.

[21] Law Reform Commission, *Discussion Paper 22 (1991) – Community Law Reform Program: Neighbour and Neighbour Relations* (2002 [cited 22 June 2005]); available from http://www.lawlink.nsw.gov.au/lrc.nsf/pages/DP22CHP3Section 3.12.

## Conclusion

In this paper I have thus far demonstrated that despite a number of seemingly strong arguments that would have us see things differently, utilising a neighbour's wireless network to access the Internet is nothing more or less than a case of theft. Despite the ephemeral nature of Internet traffic, the vagaries of radio waves, and the intangibility of cyberspace, standard moral considerations still apply, and theft is theft. However, I believe that the nature of wireless technology in its current incarnation – which has seen much thought applied to developing the technology itself, and little on its ethical implications – has lead to an ethical ambiguity that promotes the kinds of defences the freeloader presents. Therefore, in concluding this paper, I shall catalogue the flaws in the technology that I feel have lead to the ethical confusion I have described in detail above.

Firstly, I hold that the technology has conflated two separate ideas in equating 'unsecured' and 'free for anyone to access'. As noted earlier, this assumption was clearly at play in the minds of the programmers developing the early version of the wireless component of Windows XP, which (to re-iterate) will connect to any available unsecured network. The conflation of these two ideas bears no analogue in either real-world circumstances (such as the unlocked house example I described earlier) or within computing circles. If wireless networks were instead to broadcast a message to the effect that they are 'for public use' or 'not for public use' then no ambiguity would exist, whether or not the network was secured. Whilst the existence and setting of such a message would not make the network any more secure, it would at least allow a decisive judgement to be made on the actions of the freeloader. Such a system is not without precedent either. Since their inception, Compact Discs (CDs) have carried a 'copyright bit', a Boolean value that signals if the recorded material is subject to copyright restrictions. In the absence of any capacity to protect the material on a CD by encryption, the copyright bit at least allowed the manufacturer to signal that the CD was not to be duplicated. This rendered legal and ethical questions surrounding duplication unambiguous, as indeed a 'not for public use' message would on a wireless network.

Secondly, I hold that in the absence of such a message, it has been remiss of the manufacturers of access points not to enable security on their products by default. As noted earlier, the reason manufacturers have resisted such a move is because security typically adds another layer of complexity to setting up a wireless network that might serve to alienate potential customers. However, defaulting access points to having the security features turned off has resulted in a proliferation of unsecured wireless networks as users have not appreciated the need to press further and enable proper security, once their network is working.

Thirdly, I contend that Microsoft was remiss, in the first version of Windows XP, in automating their wireless networking implementation to the extent of connecting to any available unsecured network without user intervention. I have argued earlier, that even simply connecting to a wireless network (i.e., not even utilising the wireless network) without proper authorisation is ethically problematic and roughly tantamount to entering a person's unlocked house. Whilst somewhat less convenient it would seem more ethically responsible to default the behaviour of Windows XP wireless networking to always prompt for confirmation before connecting to an available unsecured network. Fortunately, this is the behaviour that newer versions of Windows XP now follow.

At base, I feel that more needs to be done in terms of assessing the ethical implications of new technologies, particularly new wireless technologies. The wireless technologies of today, it must be acknowledged, have ushered in an era of unprecedented convenience in terms of the interchange of information. But this has been to the detriment of security, because radio waves, unlike wires, cannot be constrained and secured within the bounds of private property. As I have endeavoured to show, new avenues for theft have, in this manner, been created. The ethical vagaries of the present wireless networking technologies have resulted in the twin undesirable outcomes that, firstly, well-intentioned users can unintentionally commit theft, and that, secondly, malicious thieves can defend their actions by appealing to aspects of the technology that may appear to pardon or facilitate theft. The cure to such an undesirable state of affairs is a more focused analysis of the ethical implications of any new wireless technology before it reaches the mass-market.

As Helen Nissenbaum and Batya Friedman have repeatedly demonstrated, computer systems embody values and, for this reason, proper attention must be paid to these values in designing and implementing such systems.[22] They have tirelessly advocated 'value-sensitive design' practices in which social, ethical and political considerations figure as prominently in the design of a system as technical considerations.[23] Technology cannot be thought to exist in isolation;

[22] See Helen Nissenbaum, "How Computer Systems Embody Values," *Computer* March 2001 (2001) and Batya Friedman, "Value-Sensitive Design," *Interactions* 3, no. 6 (1996) for brief but engaging introductions to the field of value-sensitive design.

[23] Nissenbaum, "How Computer Systems Embody Values," 118.

the set of features and conveniences that it introduces must be evaluated against the likely usage patterns of the target market to establish more clearly the ethical complications that its introduction might entail. If the wireless technologies discussed here are representative, then it would appear that Nissenbaum and Friedman's call is yet to be heeded. This is unfortunate, for whilst theft of Internet access might seem like quite a benign consequence when weighed against the benefits of wireless networks, the spin-off consequences are much more sinister. Already we are seeing Internet access thieved over unsecured wireless networks providing a means for criminals to disseminate child pornography and commit credit card fraud with close to complete anonymity.[24]

**Acknowledgements**

I would like to extend my thanks to Jeremy Shearmur for his valuable comments on this paper. I am also indebted to John Weckert for his most helpful suggestions and for taking the time to discuss the paper with me. Finally, I would like to thank Bonnie Allen for lending her expertise in the legal matters of encroachment and trespass, and to Thom van Dooren and Matthew Cox for their comments and suggestions.

**References**

Attorney General's Department. Criminal Code Act 1995. In Office of Legislative Drafting and Publishing, http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/2088CEAEEE78C48BCA25725C00838526 (accessed 7 February, 2007), 2006.

Australian Communications Authority. Wireless Local Area Networks: Frequently Asked Questions. In https://www.aca.gov.au/consumer_info/frequently_asked_questions/WLANs_FAQ.pdf (accessed 22 June, 2005), 2004.

N. Borisov, I. Goldberg and D. Wagner. Security of the Wep Algorithm. In http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (accessed 7 February, 2007).

A. Bradbrook, S. MacCallum and A. Moore, *Australian Property Law: Cases and Materials*. 2 ed. Thomson Lawbook Co, Sydney, 2003.

J.C. Dvorak. The Looming Legal Threat to Wi-Fi. In http://www.pcmag.com/article2/0,1759,1565274,00.asp?kc=PCRSS03079TX1K0000584 (accessed 22 June, 2005), 2004.

S. Fogie, Cracking Wi-Fi Protected Access (WPA), Part 1. In http://www.informit.com/articles/printerfriendly.asp?p=369221&rl=1 (accessed 7 February, 2007), 2005.

S. Fogie, Cracking Wi-Fi Protected Access (WPA), Part 2. In http://www.informit.com/articles/printerfriendly.asp?p=370636&rl=1 (accessed 7 February, 2007), 2005.

B. Friedman. Value-Sensitive Design. *Interactions*, 3(6): 16–23, 1996.

Law Reform Commission. Discussion Paper 22 (1991) – Community Law Reform Program: Neighbour and Neighbour Relations. In http://www.lawlink.nsw.gov.au/lrc.nsf/pages/DP22CHP3 (accessed 22 June, 2005), 2002.

Ministry of Justice. Theft Act 1968 (C. 60). In Ministry of Justice, http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1204238 (accessed 30 July, 2007), 1991.

H. Nissenbaum. How Computer Systems Embody Values. *Computer*, 118–120, March 2001.

S. Schiesel. Growth of Wireless Internet Opens New Path for Thieves. *The New York Times*, 19 March 2005.

[24] Schiesel, "Growth of Wireless Internet Opens New Path for Thieves".

# Ethics and Information Technology

BACK TO RESULTS

SEARCH MY LIBRARY'S CATALOG

Basic Description | Other Editions/ Formats | Abstracting/ Indexing & Article Access | Publisher & Ordering Information | Advertising, Rights, Demographics

Click highlighted text for a new search on that item.

| | |
|---|---|
| **Table of Contents:** | Click here to view |
| **ISSN:** | 1388-1957 |
| **Title:** | Ethics and Information Technology |
| **Publishing Body:** | Springer Netherlands |
| **Country:** | Netherlands |
| **Status:** | Active |
| **Start Year:** | 1999 |
| **Frequency:** | Quarterly |
| **Document Type:** | Journal; Academic/Scholarly |
| **Refereed:** | Yes |
| **Abstracted/Indexed:** | Yes |
| **Media:** | Print |
| **Alternate Edition ISSN:** | 1572-8439 |
| **RSS Availability:** | Click here to view |
| **Language:** | Text in Dutch |
| **Price:** | EUR 335, USD 345 combined subscription per year to institutions Print & Online Eds. (effective 2008) |
| **Subject:** | LIBRARY AND INFORMATION SCIENCES<br>PHILOSOPHY |
| **Dewey #:** | 020 |
| **LC#:** | QA76.9.M65 |
| **CODEN:** | EITHFJ |
| **Special Features:** | Includes Advertising, Book Reviews |
| **Editor(s):** | Jeroen van den Hoven (Editor-in-Chief) |
| **URL:** | http://springerlink.metapress.com/openurl.asp?genre=journal&issn=1388-1957 |
| **Description:** | Fosters and promotes reflection and analysis intended to make a constructive contribution to answering the ethical, social, and political questions associated with the adoption, use, and development of information and communication technology. |

Back to Top

**Add this item to:**
(select a list) + ADD

**Request this title:**
I'd like to request this title. GO

**Corrections:**
Submit corrections to Ulrich's about this title. GO

**Publisher of this title?**
If yes, click GO! to contact Ulrich's about updating your title listings in the Ulrich's database. GO

• Print • Download • E-mail

Back to Top

HOME | MY ACCOUNT | LISTS | HELP | LOG OUT
SEARCH | BROWSE | SERIALS ANALYSIS SYSTEM

SUPPORT CENTER | CONTACT US