Reading Service Set Identifiers (SSIDs): Marking and Locating Public and Private Wireless Spaces

Matthew Wong[1], Alison Powell[2] & Andrew Clement[3]

[1] Faculty of Information Studies, University of Toronto, matt.wong@rogers.com
[2] Department of Communications, Concordia University alisonbpowell@gmail.com
[3] Faculty of Information Studies, University of Toronto, andrew.clement@utoronto.ca

ABSTRACT

The use of wireless Internet networks has increased dramatically in the last several years. From the home to municipal-scale networks, the Service Set Identifier (SSID) plays a significant role in the identity of networks – distinguishing one from another. As the primary tool for network node owners or providers to communicate with potential users, the network name also serves as an indicator of availability for use. Our paper reports on empirical findings from two large Canadian cities and an extensive North American database of network data that illuminates the ways these identifiers are used in practice. These data will be used to examine SSID naming as a way of marking wireless space as *public* or *private.* Our findings and discussion contribute to the knowledge on wireless Internet networks by providing an assessment of the use of SSIDs as a way of communicating public and private space. Furthermore, our work will be important for understanding future implications for software, hardware, standards, and policy development related to wireless network deployment.

Introduction

The widespread distribution of domestic wireless equipment using the 802.11 group of IEEE standards has led to a proliferation of wireless signals in many urban areas. These signals create an invisible topography that spreads across the city, consisting of radio signals that permit connection to the Internet. Some of these signals are encrypted, meaning that they are only accessible to those with a password or encryption key, and others are unencrypted, meaning that anyone with a compatible device within range of the radio transmitter can access the signal. Whether encrypted or unencrypted, these radio signals, like the waves that produce radio and broadcast television, are invisible to those without the equipment to identify and receive them. However, people with laptops or other portable computing devices can identify wireless networks by their Service Set Identifier (SSID), a 32-character text string, also known as the network name. In a potential sea of wireless networks, the SSID is the central, meaningful identifier that allows users to distinguish between networks, and the first clue as to their availability. When wireless Internet equipment was less common, people with laptops and specialized software began "wardriving" or "warchalking" – traveling through cities to locate and map unencrypted (and sometimes encrypted) wireless access points. Warchalking often meant leaving visible marks (for example, on a sidewalk outside a house) indicating the presence of an unencrypted ("open") wireless network. These markings, according to Sandvig (2004), were the descendents of hobo markings indicating good places to get a meal or a bed for the night, but this time indicated the presence of different types of invisible radio signals, which might be useful for roaming computer users. Since it was never designed to be of particular utility, warchalking proved to be a short-lived phenomenon as more and more wireless signals spread across cities, provided by corporations, community groups, and individuals. Now, with more devices producing wireless signals and more receiving them, the ability to identify wireless signals is becoming associated with their SSID tags.

However, the SSID plays another more subtle role in wireless networking. As the primary tool for network node owners or providers to communicate with potential users, the network name also serves as an identifier of *public* or *private space*. For the user, this is important for identifying wireless networks that might be available for public use, whether free or paid. Alternatively, it might identify residential networks that are either intentionally or unintentionally available for use. For the node owner, the SSID can signal an intention to share or restrict access. For community wireless organizations, being able to communicate the intention to share a wireless signal is a crucial capability. One of the questions that this paper will address is how SSID names are used by individuals to mark their wireless signal clouds as either public or private. It will also examine how and whether SSIDs are employed as a way of marking corporate and community wireless signals in public space. Answering this question also raises the possibility of employing SSIDs as explicit ways to "mark" wireless spaces. However, this explicitness requires a small, but arguably significant, step by the owner of a wireless network. Creating an SSID for one's wireless network requires an extra step in configuration beyond merely plugging a wireless router into a broadband connection.

According to Sandvig and Shah (2005), this extra step means that most home wireless network owners do not change the default SSIDs that are automatically programmed on to their routers. Neither do most network owners encrypt their signals. It is unclear how people who receive these unencrypted signals interpret them – do they feel as if they are sharing a resource, or pirating one? In other words, do default open wireless access points create a de facto wireless public space, and if they do, is this deliberate? Our paper reports on empirical findings of wireless networks from two large Canadian cities that illuminate the ways these identifiers are used in practice. These findings are supplemented by an analysis of SSIDs from across North America accumulated using the Wireless Geographic Locating Engine (WiGLE) database. These data will be used to examine SSID naming as a way of marking wireless space as public or private. This research also answers a number of questions. How are individuals and organizations using SSIDs to identify or describe their home networks? How might groups who wish to communicate with users impart a message to them using SSIDs? In which ways might these activities be useful for indicating public and private wireless spaces? What perceptions and understandings of wireless ownership might play a role in deciding what space is private instead of public? In turn, what systems design and policy implications might result from these perceptions and understandings?

To answer these questions our research uses three approaches. First, we consider individual negotiations of public and private wireless space. In particular we describe the use of SSIDs as labels that use *internal* and *external* criteria to define their publicness or private exclusivity. Second, we will examine the practices of wireless networking companies like FON, who try to bring private resources into the public domain. Third, we will discuss collective perceptions of public and private wireless space by examining how community wireless networks like Montreal's *Ile Sans Fil*, and Wireless Toronto create public wireless spaces. Unifying these approaches is an attempt to understand the common perception of home Internet access connections as private property, as well as transition to more public access.

Urban Spaces Extended Wirelessly

Wireless augmentation of space connects to existing ideas of public and private. Literature in urban studies suggests that people negotiate public and private spaces in complex and nuanced ways that depend on cultural values. In North America, physical spaces are marked – visually, symbolically, and through cultural practice – as being either public or private. Private spaces are not expected to be shared without invitation, whereas public spaces (which often are understood as belonging to the state rather than to "the people") can in theory be shared by everyone. In practice, of course, the purity of this distinction breaks down, and the boundary between them is contested. People are often restricted from entering nominally "public spaces," for reasons of "security" and community "morality," while private spaces, such as shopping malls, present themselves as open to the public. These issues around public versus private access, and their intermediary hybrids, arise over many kinds of space, notably those oriented to internet access. As Viseu, Clement, Aspinall and Kennedy (2006) note,

> a seldom stated premise behind most public policy initiatives and discussions is that public access sites are mainly useful for people who do not yet have private access and

> that once everyone has private access there will be little need for public facilities…public access is thus seen as a transitory phase or stepping stone to the final goal of endowing all citizens with private access...this approach overlooks the multiple roles played by different access modes, public and private, in the use of the internet...it also rests on the belief that most things – spaces, goods, services, resources, knowledge and information – are either private or public, hence allowing little or no room for mixed or hybrid access modes (635).

The same authors go on to suggest that the kinds of Internet activities performed also influence the "character and shape of a given space at a given time, hence contributing to its hybridity" (Viseu et al., 2006, pg.651). As an example, Viseu, Clement and Aspinall (2004) explain how activities like online shopping and banking are often regarded by individuals as private activities. Other authors also discuss the shaping of public space through performance (Goffman, 1971), as well different perceptions of spaces such as semi-public and domesticated spaces (Hampton & Gupta, 2007). However, distinguishing public and private spaces remains troubled, as states, individuals, and communities attempt to define their contours. Add in the "invisible" layer of radio connectivity that WiFi now provides to a city, and new negotiations over public and private space ensue.

Methods

This exploration of wireless Internet as a canvas for the negotiation between public and private spaces draws on research conducted as part of the CRACIN and CWIRP projects[1] in Toronto and Montréal. One part of this research included wireless radio surveys conducted between October 2005 and June 2007. The surveys were conducted in two residential Toronto neighbourhoods and in multi-block sections of the downtown core. Using a wireless-equipped laptop and a GPS receiver, one of the authors walked up and down the streets and across several blocks passively recording wireless signals and their point of origin. Collectively, 605 distinct SSIDs were detected in this manner, with their locations, strength, and encryption status recorded using the program Net Stumbler[2]. Our exploration of SSIDs also makes use of the WiGLE database[3]. Through the WiGLE database we have been able to access an additional 2.9 million SSIDs collected during 2001-2005 from locations across North America. Using database query techniques, we were able to scan the extensive collection of SSIDs for potential indicators of pro- and anti-sharing positions among wireless users.

This data is supplemented by interviews and observations of the practices of Wireless Nomad, a Toronto-based cooperative wireless ISP (Wong & Clement, 2007), and Île Sans Fil (ISF), a Montreal community wireless group (Powell, 2006)[4]. These

---

[1] The Canadian Research Alliance for Community Innovation and Networking, see www.cracin.ca, and Community Wireless Infrastructure Research Project, see www.cwirp.ca/

[2] See www.netstumbler.org

[3] The authors would like to thank the WiGLE organizers and administrators as well as Professor Christian Sandvig, University of Illinois at Urbana-Champaign, for access to and technical support with the database.

[4] The authors would like to thank our collaborators at Wireless Nomad and ISF for participation in producing this paper.

qualitative contributions help to provide context for and understanding of the multitudes of SSIDs collected in our research.

Marking Private Space

For many individuals, wireless space seems to be defined as an extension of private domestic space. Based on research conducted in Toronto residential neighbourhoods, people often label their networks in ways that emphasize the network's privacy or their ownership of it, either by focusing on the location of the signal, or referring to words or phrases familiar to household members. Some people use "external" labels, or labels that mean something to people outside the home – connecting the radio signal to a physical location or address. For example, some SSIDs are labeled by house number or address, such as *53Tyrell*, *17Borden* or *350 Huron*, all of which are street addresses in the areas surveyed. Corporations also use these external labels, such as *Gowlings-Toronto* or *weirfoulds*, which are the names of two law firms. The efficacy of these SSIDs as external labels can be demonstrated by the fact that an Internet search on "Gowlings" or "Weirfoulds" and "Toronto" returns the corporate homepages of both companies. Having an easily identifiable label does not necessarily speak to the opened or closed nature of the network. For example, while *Gowlings-Toronto* and *17Borden* are clearly labeled networks, both were encrypted against unauthorized use.

Other people use some form of "internal" label that probably means something only to the users of the network. Instead of labeling the network for the benefit of individuals on the outside (e.g. strangers), these private names reflect the idea that a wireless connection belongs to domestic or private space. For example, some SSIDs observed have names like *sweetpea*, *jabberwocky*, *chumpco*, or *piggy1001.* These intimate nicknames are meaningless for strangers, but suggest that for the network node owner, wireless is resolutely private and personal. Possessive network names also seem to suggest this as SSIDs like *mine*, *MyNet,* and *MyWirelessNetwork* were all observed. Even when a generic SSID is used, such as *wireless* or *WLAN,* presumably the node owner would recognize their own network name from a list when it came to choosing which network to connect to. However, greater difficulty may be expected when multiple network exist which use such a generic name.

A blending of such internal and external identification can be seen when individuals use their own names as the SSID, which would mean something to both internal users and neighbours in the area or friends visiting. For example, *Paul & Diana Wireless*, *Michael home*, and *Todd's Net*, were all SSIDs identified on one residential street. In the downtown business district *weirfoulds_guest* was another SSID detected, suggesting a separate network available for visiting guests (e.g. clients).

Other SSID names make it very clear when the space is considered private by using the SSID in essence as a "beware of dog" or "private property" warning sign. This kind of labeling may reinforce another individual activity: encrypting or password protecting the wireless signal. An encrypted network requires a personal connection with the network owner in order to gain access to the encryption key. Some SSIDs that were observed with clearly protective, private names included *privatenet*, *Get Lost!*, and

getyourownlan. These names are all very clearly used to delineate space that the wireless node owner considers private as well as an admonishment that anyone looking for a free and open wireless network should probably look elsewhere. Indeed, some SSIDs included profanity, demonstrating an antagonistic attitude towards other wireless users, or at least "free loaders".

Labeling Public Space

In the two residential neighbourhoods surveyed, even with over 300 networks identified, it was difficult to find clearly labeled networks for public use. Indeed, one of problematic aspects of SSIDs as the key method for communicating withWiFi users is that it can be difficult to assess whether an unencrypted network has been intentionally left open for public or shared use or was merely left open by accident. As a result, our analysis of SSIDs looked for a number of particular key words to identify the public character of the network space. These included URLs as SSIDs (e.g. website or email addresses) and words like "free", "public", and "open." In the downtown Toronto area some SSIDs discovered with unencrypted networks were labeled *Free Public WiFi, FMC Public,* and *LAS Free Airport Access.* As with the residential neighbourhoods, the number of networks presumably for public use appeared to be very small in comparison to the total number of networks. Interestingly, upon exploring these particularly networks further, attempts to connect to any of these networks met with failure. Even with multiple attempts, neither a achieving a stable connection nor acquiring an IP address was possible. The fact that these SSIDs existed but were unavailable for connection raises the possibility that these networks may be a new form of computer attack. Piscitello (2004) suggests that presenting access points which attract would-be users could be used as a new form of "phishing" attack. In such a case, if a user connects to an artificial log-in page from the "rogue" access point which captures personal information the user supplies, then it would be very easy for such a user to become a victim of fraud or identity theft. Fortunately, since no stable connection was created it is less likely that these networks were part of some attack, but more likely networks that simply were not available.

Scanning the WiGLE database produced a number of additional examples of apparently public networks. In these cases, we searched on the *freenet*[5] database field set to "yes" and networks where encryption (i.e. WEP) was disabled. The following table (see Table 1) represents some examples by region, as provided by the database. In the examples where further exploration of the SSID was possible, for example, looking up a URL, a comment is provided.

Table 1. Examples of Presumably Free Networks from the WiGLE Database

SSID	Region	Comment
Free Internet	California	
Free Access	California	
Free Wi-Fi by AnchorFree	California	AnchorFree appears to be a large nationwide (US) wireless provider

[5] The *freenet* flag is an optional flag in the database denoting an "Open freenet for public use" that can be set when a record is created manually, or later updated when the data is generated automatically, e.g. from radio survey logs. See: http://www.wigle.net/gps/gps/main/handadd/

Socalfreenet.org	California	Wireless Internet provider for low-income families
Free2mbpsforyou	California	
free use with no abuse	East	
atlantafreenet.org	East	A community initiative to promote WiFi in Atlanta, Georgia
manchesterwireless.org	East	A community initiative to promote WiFi in Manchester, New Hampshire
Surf 4 Free on Me	East	
free enjoy!	East	
P.F. Chang's Free HotSpot	East	A Chinese restaurant in the Mall of Georgia; listed with Ripple Wireless Hotspots[6] in Atlanta
Free to Roam	Midwest	
www.nevermind.org – free inet!	Midwest	Currently links to a personal homepage
free ipod: www.ipod4u.tk	Midwest	Advertising via SSID, although website no longer available
AG Cafe Free Internet	Midwest	
free wireless is cool	Midwest	
FREE WIRELESS www.lazerquick.com	Northwest	A commercial printing company in Oregon
Free WiFi – meta_alex@hotmail	Northwest	
www.personaltelco.net/node504w	Northwest	Personaltelco.net is a volunteer group based in Portland, Oregon (the URL actually brings up a description page of the owner of the node)
SkyTrain Free Wireless	Northwest	

When searching the "freenet" and "encryption" fields of the WiGLE database, many of the results turned up some of the key words we had hypothesized would be used to denote public networks. Some of the examples above demonstrate the frequent use of the word "free" and URLs in the SSID. However, as a proportion of the total number of networks available in the database, the number of results was rather low (less than one percent). Of course, given the extra step required to set the flag in the database denoting these networks as freenets, it is important to distinguish that these numbers may not be truly representative of the total number of presumably free networks in the regions.

Sometimes SSIDs are part of an overall strategy to identify free and open networks. In Montréal, the community group Ile Sans Fil deliberately uses their SSID to delineate the public spaces in which their partners offer free Internet access. Their SSID *www.ilesansfil.org* points to their website, which explains the group's mission. In addition, when a wireless user selects the ISF network, they are automatically directed to a login page for the organization, linked to a portal page that displays information about the group and the public location in which wireless access is offered. This is an excellent example of using the SSID to define public space. It appears that this definition is understood by users of the service: interventions with people who used the ISF services, people described that they looked at the lists of SSIDs posted on their computer to determine which SSID to use, and recognized that ISF was a free (as well as unencrypted)

[6] Ripple is an IT services company in Atlanta, Georgia. See: http://www.rippleit.com/about

signal. The explicit labeling with the group's URL reinforced the idea that users were *sharing*, not *stealing* the wireless signals.

Along with SSIDs, ISF also uses signs and stickers to identify the areas where their wireless signals are available. Like SSIDs these are ways to mark public space as wireless-equipped, and to reinforce the connection between ISF as a community organization, and the public (and community) spaces in which they provide wireless access. ISF has developed other strategies to publicly identify their locations as having wireless, and as being part of a community organization. They organized a public tour of locations where their group provided wireless access, producing a commemorative t-shirt with a map and the names of all the locations included in the tour. Like the unified SSIDs and the stickers and labels, this event reinforces the physical locations that have wireless Internet as being public, and even in a certain way makes the Internet "visible" at those locations.

Defaults as De Facto Regulation

However, despite these examples that seem to indicate an awareness of a public/private distinction among some users, it is not clear whether this awareness is shared by all users. The abundance of unnamed (blank), default (*default*), or manufacturer's names (*linksys*, *NETGEAR*, *Dlink,* etc.) attached to unencrypted networks suggest that many users are plugging in their routers, finding that they work, and then leaving them alone[7]. This should not be interpreted as the users not caring about issues such as public/private spaces, but perhaps as a lack of awareness or knowledge about what is being broadcast. Indeed, there may also be a lack of awareness as to the strength or distance that their radio signal is even being broadcast. However, we suspect that for many users, given that they pay for their Internet access, and that the radio signal originates in their dwelling, that they retain at least an implicit understanding of ownership and private space. For example, like other aspects of property, something that is within a person's home is implicitly their private property. Thus, even if a wireless network is by default left open, this is often not with the owner's knowledge or consent.

This observation suggests that Shah and Sandvig's (2005) concept of "software defaults as de facto regulation" has a powerful relevance. They argue that by facilitating default open status, software defaults in fact create a de facto regulation of signals, where people are not empowered to make the choice whether to open their signal or not. Shah and Sandvig argue that since only half of the people who own wireless networking equipment encrypt their signal, and that some evidence suggests that people living in lower income areas are less likely to change their defaults, software developers and policymakers must address the power of the technology. This argument presumes not only that the default settings on wireless equipment exert a determining influence on people (especially those with less formal education); but also that design and policy development need to make it easier for *individuals* to protect their *private property* – in this case, the broadband Internet connection that their ISP considers to be a privately purchased service, and which existing policy typically prohibits being shared. Therefore,

[7] Of the 605 SSIDs identified in the radio surveys, 98 SSIDs were blank, *default*, or one of the generic manufacturer's names, such as *linksys*, *Netgear* and the like, and did not use encryption.

Shah and Sandvig's proposed design and policy interventions are set up to reinforce the concept of wireless Internet signals as private property. Yet, individual users as well as community groups that provide wireless services often describe a willingness to share wireless signals and bandwidth. Furthermore, the activities of individual wireless users we reported reveal nuanced ways of negotiating privacy and security. Are there ways to go beyond the assumption that privately owning a router and Internet connection will necessarily mean thinking of a wireless connection as private? We consider the case of the Toronto wireless ISP Wireless Nomad as an example of a bandwidth-sharing business plan that appears to challenge existing ideas of private wireless signals. Following this, we consider the policy and design changes that would have to occur in order for software defaults to define public, as opposed to private, wireless spaces.

Mixed Public and Private Models and Wireless Nomad

Toronto's Wireless Nomad Co-operative Incorporated (WN)[8] attempts to negotiate privacy, security, and bandwidth sharing through the use of free wireless networking accounts and the experimental use of "mesh" networking technology. WN is an Internet service provider that sells Digital Subscriber Line (DSL) services, deployed through wireless networking nodes. Subscribers to WN become members of the cooperative organization and receive access to any other wireless node on the WN network. That is, they can log-in to WN nodes distributed throughout Toronto homes and businesses. Subscribers receive "full" access to these nodes, in that there are no port or access restrictions to these connections. In contrast, users who subscribe for free accounts with WN also have access to nodes throughout the network although their connection is limited to web surfing and services like email (via POP and SMTP ports) are blocked. Furthermore, bandwidth is prioritized in the network via the kind of account that is accessing it. In order to ensure a fair distribution of bandwidth, access is prioritized starting with the node owner with the highest speed and ending with free accounts limited to 64Kbps.

WN has also experimented with deployments of "mesh" networking technology which uses linked wireless network nodes to share back-end broadband connections. For example, in one test deployment, a single DSL connection was connected with three other houses via mesh nodes. These mesh nodes were simply plugged into AC power and then began to receive and transmit radio signals through the network. In theory, mesh networking technology can be extensively deployed in residential communities in order to share communal bandwidth with all users of the network. As a result of the requirement for fewer broadband connections, the cost for Internet access could effectively be reduced. This potential sharing structure would redefine WiFi access as neither public, nor private, but *shared*.

Like ISF, WN uses a common SSID for all their wireless nodes. The SSID is *wirelessnomad.com* and this is used not only to create a common account profile amongst all the nodes, but for subscribers to easily identify nodes belonging to the WN network. Similarly, the mesh nodes are labeled *mesh.wirelessnomad.com*. Furthermore, users who

[8] See www.wirelessnomad.com

are just "passing by" and can detect the WN signal can actually access the default log-in page broadcast by the wireless node. From there, these users can create a free account to begin surfing on the network. However, these free accounts, while free in a monetary sense, in effect create a form of authenticated membership which keeps WN's networks essentially private, even if it is theoretically open to the public. Since WN, as with ISF, does not in fact indicate its "free" nature in its own SSID, it appears that they both rely on the external quality of their SSIDs in order to invite users to find out more about their services.

Recently, Spanish telecom Fon has captured headlines as they float their wireless bandwidth-sharing scheme. The Fon scheme, like WN, prioritizes members of the network over non-members. There are two types of network members: "Bills" sell access to their networks to non-members (called "Aliens") but must pay to use other user's networks, while "Linuses" share their networks for free and receive free access in return. While the company claims that its networks has the largest number of freely-accessible WiFi access points in the world, critics note that even if these access points are open they may not be publicly accessible – for example, they may be located in residential neighbourhoods. Still, the attention provided to their project has raised the profile of issues of bandwidth sharing and the potential of new business models for wireless projects[9]. Important future research questions have arisen from these deployments. For example, what is the feasibility of a shared wireless network, as typified by WN, succeeding in residential neighbourhoods such as in Toronto? While WN seems to be making some in-roads in a very saturated broadband market, it is not obvious that a shared wireless neighbourhood network will work, although extremely high density locales like townhouses and apartments/condos may work very well. Preliminary anecdotal data suggests that when people are attracted by the prospect of a lower-cost wireless service, they are anticipating rates much less than half the prevailing rate (i.e. $10-15/mo) in order to be a serious contender for replacing their current broadband connections. Furthermore, it is not clear that residential users are interested in sharing their Internet connection with others (even if it is more accurately described as a "group" Internet connection), which speaks to the implicit assumption of Internet connections as private property.

Changing Conceptions of Space – Design and Policy Implications

Can Sandvig and Shah's call for changes in the design and regulation of WLAN software defaults be extended to permit people to mindfully share their wireless Internet bandwidth without presenting users with an unrealistic choice? While Sandvig and Shah (2005) argue that wireless companies need to make encryption as easy a default option for home WLAN owners to choose as non-encryption, we propose a similar development and policy initiative that could create a non-threatening way to share one's bandwidth. This could, like WN's bandwidth-sharing, provide the ability to identify either a

[9] See http://mtl3p.ilesansfil.org/blog/archives/2006/02/09/this_is_pretty_good.html for a discussion of this phenomenon.

willingness to share, or define the entry conditions to a community (like ISF's or WN's use of specific SSIDs). However, this kind of choice would need to be integrated easily and coherently into the design of the wireless device's configuration screen. Extending beyond Sandvig and Shah's call for easy-to-configure wireless devices to protect privacy, we would like to extend configuration to allow individual users and communities of users to define whether and how they would want to share their bandwidth.

In qualitative interviews conducted in Toronto (Wong and Clement, 2007), respondents report that they would be comfortable with a neighbour who wanted to use their wireless connection from time to time. In particular, one person said that she knows that Internet access is very expensive and that it did not make a lot of sense for her lower-income neighbour to pay $40 CDN/month just to check email and surf occasionally. She said that as long as her neighbour asked first, it was no problem. However, she did wish to retain control over it, particularly if that occasional use became constant Bit Torrent (peer-to-peer) downloading or other high bandwidth activities. It is important to note here that while control is retained, there is a willingness to share, also assuming that the other party asks first. It is less clear how people would feel about sharing if it was done anonymously. It is reasonable to assume that owners would find it unsettling to have other people using their network, maliciously or not, without any sort of consent or knowledge first. The key seems to be knowledge about whether or not one's signal is being shared. Therefore, as much as individuals need to be made aware of their ability to encrypt their signals to make them private, they may also need to be made aware of ways to share those signals. At the same time, considering that questionnaire responses from a generally tech-savvy sample of informants indicate overwhelmingly that they protect their own networks, it seems unlikely that a majority would take advantage of such knowledge in order to share them. Less than ten percent of respondents intentionally left their network open for others outside the house to use. A community-focused design and policy (perhaps beginning from the idea of the WiFi Thank You explained at http://www.wifithankyou.com/) would make it easy for people to choose to share, and perhaps also allow them to indicate their knowledge of their networks open status, perhaps even as part of their SSID. As important as Sandvig and Shah's (2005) reflection on software defaults may be, it continues to presume that wireless signals must only be private property. It might also be possible to imagine WiFi signals as being able to be public or community property as well, and to configure software so as to permit people to consciously make choices, as well as to share the choices they have made.

Further research on the regulatory and policy dimensions of signal sharing is also required here. WLAN owners who share Internet signals they have purchased from a commercial ISP are in danger of violating their end user agreements or terms of service contracts, most of which proscribe such sharing, and may even be liable to criminal prosecution for "theft of telecommunications." While the authors are unaware of any such prosecutions of WLAN owners, there have been several high profile prosecutions of those who have "poached" signals from open networks. We are also not aware of any instances of ISPs enforcing the prohibition against signal sharing in relation to customers who are also WLAN owners. Doing so raises obvious issues of the necessary resources required for enforcement. More broadly, due consideration needs to be given to refining

the regulatory and criminal law dimensions of signal sharing in order to create a space for signal sharing practices and communities.

Conclusion

Software needs to be designed and regulated in ways that not only protect individuals, but permit the creation of self-definition by communities. At the same time, it is not clear to what extent merely providing people with the opportunity to share their networks would motivate them to do so. While developing software to promote sharing of bandwidth would provide some people with the ability to willingly share their Internet connections, bandwidth is still expensive and many people (especially those who can not tolerate interruptions to their connection) would still not necessarily choose to share their bandwidth. This might make neighbourhood mesh networks impractical by creating significant pockets of isolation, or gaps in the network. But then again, perhaps in high density, low-income housing projects, this situation would be ideal.

Current hotspot-sharing schemes such as Fon and WN provide a potential alternative to wireless "walled gardens," but their business models may not prove to be sustainable in the long term. Thus far, community groups such as ISF are making the most concerted attempts to create the wireless equivalent of urban public space. It remains to be seen exactly what the result of these efforts will be, since ISF's hotspot model depends upon a business or organization purchasing the bandwidth and sharing it with clients or passers-by. Some municipalities have invested in WiFi clouds or corridors, but these solutions also define WiFi access as a private service, much like telephony in a deregulated policy environment. Future research will have to determine the extent to which WiFi (and Internet access in general) might be defined as a public good.

BIBLIOGRAPHY

Goffman, E. (1971). *Relations in Public*. New York: Basic Books..

Hampton, K. & Gupta, N. (in press). Community and Social Interaction in the Wireless City: Wi-Fi use in Public and Semi-Public Spaces. *New Media & Society,* 9(6).

Pischitello, D. (2004). *Hot Spot or Hot Zone? Understanding the Hazards of Public WiFi LANs.* Retrieved July 26, 2007 from Core Competence Inc. web site: http://www.corecom.com/external/livesecurity/hotspot.htm

Powell, A. (2006). *"Last Mile" or Local Innovation? Canadian Perspectives on Community Wireless Networking as Civic Participation.* Paper presented at The 34th Research Conference on Communication, Information, and Internet Policy, Arlington, Virginia, USA.

Sandvig, Christian. (2004). An Initial Assessment of Cooperative Action in Wi-Fi Networking. *Telecommunications Policy,* 28 (7/8), 579-602.

Sandvig, Christian, and Rajiv Shah. (2005). *Software Defaults as De Facto Regulation: The Case of Wireless Aps*. Paper presented at The 33rd Research Conference on Communication, Information, and Internet Policy, Arlington, Virginia, USA.

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating Privacy Online. *Information, Communication & Society,* 7(1), 92-114.

Viseu, A., Clement, A., Aspinall, J. & Kennedy, T.L.M. (2006). The Interplay of Public and Private Spaces in Internet Access. *Information, Communication & Society,* 9(5), 633-656.

Wong, M. & Clement, A. (2007). Sharing Wireless Internet in Urban Neighbourhoods. In Steinfield, C., Pentland, B., Ackerman, M. & Contractor, N. (Eds.), Proceedings of the Third Community and Technologies Conference, Michigan State University. New York: Springer.