A Desiderata for Wireless Broadband Networks in the Public Interest

Community Wireless Infrastructure Research Project

Amelia Bryne Potter, ameliabpotter-at-gmail.com
Andrew Clement, andrew.clement-at-utoronto.ca

Paper to be presented at the 35th Research Conference on Communication, Information and Internet Policy, 2007

Submitted August 17, 2007

D R A F T

Abstract

There is currently an expanding range of initiatives in North America, and world-wide, attempting in various ways to develop public internet infrastructures. Discussion about them so far has concentrated on the benefits they espouse (bridge the digital divide, promote commerce,..), what technological configuration is best (e.g. WiFi, fiber, hybrids of these,..) and who should own (and perhaps build) them (e.g. private sector, public sector, or a partnership of these,…). What has been relatively absent to date is systematic analysis of the functional and performance characteristics of the infrastructure itself. Such an analysis would be invaluable in assessing the competing claims about such benefits, technologies and ownership models.

This paper offers an analytic framework for assessing public internet infrastructures. Drawing initially on familiar criteria for communications infrastructures (e.g. 'public interest, convenience and necessity' from longstanding US public utility law, 'universal and affordable' from telecommunications legislation in the US, Canada, and elsewhere), it refines and expands these in light of contemporary internet initiatives. It thus presents a list of "desiderata" for public broadband infrastructure – a checklist of principles for building and operating them in the public interest.

We examine each of these infrastructural characteristics in turn, describing what is meant by the term, and how it has been used in policy development as well as the relevant scholarly literature. These desiderata are illustrated using case studies of community/municipal wireless initiatives in North America. The paper also discusses how the desiderata can be used as a tool for assessing proposed and operational broadband networks.

A Desiderata for Wireless Broadband Networks in the Public Interest

PART I – PREAMBLE

INTRODUCTION

High-speed internet service is rapidly acquiring the status of public amenity, but what sort of infrastructure is necessary to provide it? And, how can we effectively assess proposed models for such broadband initiatives? This paper explores **broadband as a public utility** and provides a **tool for assessing the design and effectiveness of proposed or operational broadband networks** in terms of their relevance and benefit to members of the public.

Much of the discourse surrounding municipal Wi-Fi developments thus far has been framed in terms of whether wireless internet should be provided by public or private entities. Largely absent from the debate, however, has been a meaningful discussion of what a properly constituted public wireless internet service ought to look like. We hope that this paper will help to shift the debate from who should operate broadband infrastructure, to what types of networks best benefit an inclusive range of broadband users.

Based on a review of relevant literature, and our knowledge of municipal and community broadband networks, we have drawn up a list of ideal network characteristics, that is: a desiderata for broadband networks in the public interest (Middleton, Longford et al. 2006). This checklist includes points that have been widely discussed in the municipal broadband movement, such as the importance of ubiquitous and affordable networks, as well as crucial characteristics that have received less attention than they should. While we believe that networks in the best public interest will meet all of these criteria, we recognize that some communities will choose to prioritize some of them over others, due to local contexts and constraints.

This paper is divided into three parts. The first part sets the context for a discussion of broadband in the public interest, and for the desiderata. It includes a brief introduction to the municipal and community wireless movements and the debate about the public and private roles in the provision of internet infrastructure; a discussion of technology, and why we have chosen to focus our discussion on internet infrastructure with an emphasis on Wi-Fi, rather than on a wider range of technologies and applications; a definition of the difference between "public broadband" and "broadband in the public interest; a discussion of how the desiderata principles relate to general principles of good infrastructure; and, some notes about how to apply the desiderata principles to planned or operational projects.

The second part of the paper presents the desiderata itself. Here, we argue that broadband networks should be: Ubiquitous & Universal, Widely Useful, Usable, Accessible, Affordable, Reliable, High Quality, Healthy, Cost-Effective, Accountable & Responsive, Secure, Privacy Enabling, Open, and Neutral & Non-Discriminatory. We define each of these topics and discuss them drawing on the research literature, and examples from the municipal broadband movement.

The third part presents a set of resources relevant to the desiderata, including references for further reading, and a summary table of the desiderata points.

Readers may want to begin by reviewing the **Desiderata Summary Table** (p. 59), which gives an overview of the desiderata, including definitions of each point, as well as notes on wireless technology, key debates, and methods of assessment.

The Larger Context Surrounding the Desiderata

A discussion of what broadband networks in the public interest should look like lies in the context of a number of larger issues, including:

- Ideological trends in policy towards deregulation and privatization
- Principles of good infrastructure
- The concept of Ubiquitous Network Societies (Intel 2005; International Telecommunication Union 2006)
- Debates over the impact of ICTs and telecom on the economy and on work
- Debates over the impact of ICTs on civic engagement and everyday life
- Digital divide debate
- Network neutrality debate
- Open Infrastructure/Access movement
- Spectrum policy
- Developments in broadband technologies, such as Wi-Fi, Fiber, and Wi-Max
- Municipal and community wireless movements

The municipal and community wireless movements provide a particularly vital window onto this larger set of issues. These movements have directed the attention of policy makers, researchers, and communities to the importance of broadband infrastructure. In particular, community wireless projects have both inspired larger-scale municipal projects, and raised key broadband policy issues (Fleishman 2006). In turn, municipalities' actions have highlighted the lack of, and the need for, North American federal and state/provincial policies to promote universal broadband access and competition in the broadband industry.

These community and municipal projects are important because, in the absence of policy for universal high-speed Internet service, and lack of clear spectrum policy, local level decisions on how to approach broadband infrastructure become crucial: "Some of the [broadband] access models being adopted may allow communities to use broadband as a resource to overcome existing social hurdles, while other models can further reinforce social and economic barriers delaying the adoption of high-speed services for all," (Fuentes-Bautista and Inagaki 2005: 5). These local initiatives represent a reversal of historical communications regulation policy, which, in the U.S., has largely come from the federal level and restricted how states and municipalities could be involved in telecommunications: "In the context of municipal wireless broadband deployments, this "top-down" model of policymaking has been flipped on its head, with the power shifting away from the FCC to city halls and state legislatures throughout America," (Stone, Maitland et al. 2006: 11).

It is yet to be determined what the role of municipalities should be in the provision of broadband networks. The answer is likely that they have many roles -- ranging from aggregators of demand, to coordinators of different players in the local broadband environment, to making prudent decisions about how to share municipal infrastructure assets that can support broadband infrastructure in a way that promotes a competitive local broadband market (Gillett, Lehr et al. 2003; Bakowski 2005; Gillett 2006; Lehr, Sirbu et al. 2006). Until larger policy changes are made that affect the social mandate of the high-speed Internet sector as a whole, it may not be fair to expect municipal projects to operate under unusually high standards, of digital inclusion, privacy, etc.(Richardson 2007). In any case, municipal broadband projects would both benefit from, and help to push for, a higher-level policy shift towards universal broadband, and a competitive broadband industry.

In summary, even if municipal broadband projects are only a temporary development, they may make a significant contribution to broadband networks that are in the best public interest, by shifting attention to this question, and putting pressure on regulators and providers to measure up to higher standards. That is, "even if municipal broadband networks [as initially envisioned] are not deployed to the public, there may yet be positive outcomes. With broadband serving as a disruptive technology and municipalities playing the role of entrepreneur, the actions of these entrepreneurs may spur private sector innovation, or at least wider broadband deployment," (Stone, Maitland et al. 2006: 34). As such, municipal broadband projects are an important subject of study and point of action.

A Desiderata is Needed!

At a time when communities across North America, and throughout the world, are moving to develop broadband networks, a tool for the critical evaluation of broadband networks can be invaluable. Amid the push for rapid development, communities must guard against creating broadband networks haphazardly. As key infrastructure for citizen economic, social, and civic participation it matters how these networks are designed, built, and managed. The desiderata developed in this paper offers guidance to this process.

This tool both draws from and is useful for municipal broadband projects. The desiderata provides an overview of qualities that, together, constitute a broadband network that is arguably in the public interest, and notes how these qualities have been addressed (or overlooked) in the public broadband debate. In the context of municipal projects this is important because, although it is clear why municipalities believe wireless broadband networks are important, including to provide more efficient city services, promote economic development, and to bridge the digital divide (Bar and Park 2005; Gillett 2006), it is less clear if and how these goals can be achieved. While early projects seem to suggest that municipally directed wireless projects can indeed make city services more efficient, promote economic development, and help close the digital divide (Bar and Park 2005; Bar and Park 2006; Gillett 2006; Gillett, Lehr et al. 2006), the path between these ideals and the results is often unclear. The desiderata both sharpens the focus of these goals, and provides a clearer way to evaluate networks.

While no comprehensive desiderata yet exists for broadband in the public interest, pieces of one do. These include municipalities' own lists of desired network characteristics (The Wireless Philadelphia Executive Committee 2005; Boston Wireless Task Force 2006), declarations like the INEC declaration on Open Networks (International Network of e-Communities (INEC) 2006), standards like the EPIC/ALCU/EFF Model Minimum Standards for Electronic Privacy (ACLU of Northern California, Electronic Frontier Foundation (EFF) et al. 2006), best practices guides for municipal technology projects (Federal Communications Commission (FCC) 2000; Bakowski 2005; Intel 2005; Richardson 2005; Excelsio Communications 2007), and municipal RFPs that define core network features and standards. Our desiderata builds on these declarations, standards, and best practices.

Strong public broadband networks are significant because they can go beyond ensuring basic connectivity, to fostering civic and community participation. As envisioned by Schaefer (1995), while the premier features of a public information infrastructure "would be its accessibility and its accountability to publicly determined goals. Such a publicly controlled system would not be judged merely on its ability to stimulate commerce and profits but on its ability to stimulate open dialog and citizen participation in a broad range of political, work and management issues," (4). While explicit civic goals (such as higher participation in local community issues) may not be accomplishable through network design, the desiderata encourages networks that are in the best public interest, and therefore, civic. In other words, the best networks – those that meet the criteria of the desiderata – are most likely to enable communicative commons and civic participation, encouraging communication that is in the interest of communities while ensuring users access to good networks at affordable prices.

Beyond providing connectivity, a broadband service in the public interest should ideally encourage users to author and share content, accommodating a diversity of views and perspectives. It should support also a wide variety of civic-oriented information services, including community portals, news and event listings, and citizen policy discussion forums.

Broadband networks are promising in this regard. There is an extensive body of literature that shows that community networks, in general, have the potential to stimulate local civic engagement and develop social capital, both online and offline (Kavanagh & Patterson, 2001; Schuler & Day, 2004). Community networks can encourage civic participation, in that they serve as sites where community members engage in the development, management, and maintenance of the network through volunteer activities, including serving on committees, providing technical support and training, or engaging in content development. Community networks can also enable civic participation by helping people get online, through providing services and supports, such access to and training on ICT equipment and software, information and communication services like internet service provision, email/listserv/web hosting, community directories, and electronic discussion forums) (Rideout and Reddick 2005).

The extent to which Wi-Fi will play a role in enabling such interaction is yet to be determined, though researchers have begun assessing the relationship between civic participation and public Wi-Fi networks (Sandvig 2004; Cho 2006; Powell and Regan Shade 2006). To begin, it seems clear that municipal and community wireless networks can be used to better inform and engage citizens about local politics and community issues (for example, through municipal government websites), through the use of a community portal, location-based information and event alerts (facilitated by software like 'Wifidog', http://dev.wifidog.org/), online forums and online polling (Middleton, Longford et al. 2006).

A Note About Technology

This paper focuses on internet infrastructure with an emphasis on Wi-Fi, as is the focus of today's most publicly debated broadband projects. Nevertheless, we recognize that broadband includes a much wider range of technologies and has a wider range of applications. As they become ubiquitous, broadband networks (especially wireless ones) have the potential to support applications and services beyond what we think of as the internet today. In the big picture, the International Telecommunications Union (ITU) envisions what it calls *ubiquitous network societies*. In these societies "information can be accessed from anywhere, at anytime, for anything", and communication will occur not only between people and between people and things, but also between things themselves. Along with RFID (Radio Frequency Identification) and GPS (Global Positioning System) technologies, Wi-Fi enables "intelligent" devices, such as parking meters, lights, mobile phones, or even coffee makers, to interact with their environments (International Telecommunication Union 2006). Some municipal broadband projects, notably, Boston's planned project (Boston Wireless Task Force 2006), and those like Corpus Christi, TX that are working to create applications of their network other than wireless internet (Corpus Christi 2007), are taking this wider vision into account. Some of these applications are already in use such as automated-meter reading systems (Perlman 2007), and public safety systems (Perkowski 2007).

There is a range of broadband technologies, including Wi-Fi, fiber, Wi-Max, DSL, cable broadband, broadband-over-powerline, satellite, cellular networks, as well as a variety of network models that incorporate more than one of these technologies. Because it is relatively low-cost and fast to deploy, because it can be used to create ubiquitous coverage in both urban and rural environments, and because it operates on the open spectrum, Wi-Fi has been the technology of choice for many public broadband projects. In this respect it has been one of the major technological drivers of the public broadband movement (Bar and Galperin 2004),

Nevertheless, other broadband technologies likely also have a role to play in future networks. For example, DSL and cable broadband are currently the most widely used broadband internet technologies, 2G and 3G cellular networks already provide mobile devices such as mobile phones with a near-ubiquitous network connection (Third Generation Partnership Project; MobileTracker 2005) and enable cell phone users to access data (Lehr and McKnight 2003; Schwartz 2005), Wi-Max may enable much more powerful Wi-Fi-like networks (WiMax Forum; Organization for Economic Co-operation and Development 2006; Richardson and Ryan 2006; Limbach 2007), and satellite technology is bringing broadband to remote locations (Katkin 2006).

In addition wireless technology itself is not sufficient to provide high-quality, reliable broadband. Currently Wi-Fi is mainly used to extend the internet connectivity reach of wireline backhaul and backbone. Oram (Oram 2007) proposes a three-tier hybrid wireless/wireline model in terms of ensuring adequate broadband service. A typical model includes: (1) a fiber ring that brings extremely high bandwidth within a few thousand feet of most locations and goes directly to major buildings such as City Hall, hospitals, and schools. (2) A second tier that involves WiMAX, and (3) a third tier where the final hundred feet of connectivity are provided by Wi-Fi. Such a three-tier model need not be built from the first tier up – fiber, WiMAX, and Wi-Fi can be built simultaneously, balancing community needs for quick build-out with longer-term goals of reliability. For example, a wireless network could be used to achieve ubiquitous coverage quickly, while a city builds fiber – a more permanent solution, over the long term..

Fiber (optic cable), in particular, has some important complementary advantages to Wi-Fi. While fiber tends to be more expensive to deploy than wireless, fiber also tends to be more reliable and secure, to support higher bandwidth speeds, and is also likely to be a more future-proof investment (Daggett 2007). Fiber is a key technology in public broadband projects, for example, the UTOPIA cooperative wholesale fiber network (UTOPIA; Utah Telecommunication Open Infrastructure Agency 2003; Cherry 2006), but it does not receive the attention it should. In fact, many wireless projects are Wi-Fi *and* fiber projects. For instance, the Fredericton, New Brunswick wireless Fred eZone grew out of extra capacity on the city fiber network (e-Novations 2005), and Boston, in its feasibility study for a citywide wireless network, shows fiber as an integral component (Boston Wireless Task Force 2006). While Wi-Fi is the main focus of this paper, how fiber may play a role in broadband infrastructures in addition to or in place of wireless is briefly discussed under relevant points of the desiderata.

Therefore, while our discussion of the desiderata in this paper focuses on internet infrastructure with an emphasis on Wi-Fi, because of its prominence in contemporary debates, we recognize that public broadband encompasses a much wider range of technologies and applications. We encourage others to apply the desiderata to projects that make use of a wider range of technologies and applications, as we believe its core principles are relevant for many types of broadband networks.

Public Broadband vs. Broadband in the Public Interest

While exploring the ideal of public infrastructure, we do not address directly the important but controversial question of what may be the best means for achieving this. The debate about this issue so far has focused on whether this should be done with government involvement or entirely through 'market forces'. One contribution this paper can make is providing a set of criteria for judging alternative proposals that may shift the debate away from ideological grounds to ones that are relevant to the intended beneficiaries – namely members of the public. This section briefly introduces this public/private broadband debate. It then makes a key distinction, between *public broadband* – the subject of this debate, and *broadband in the public interest* – the subject of this paper.

The Public/Private Broadband Debate

The debate over public and private roles in municipal broadband projects has been fierce. It touches on ideologies about the role of the public and private sector in infrastructure development, and takes place in an environment that has been characterized by a move towards private sector provision of infrastructure in North America. While it many now be coming to be accepted that the public sector does have a role to play in broadband networks (Gillett 2006), the debate about it has shaped the public sector's position and network structures. Although, there are precedents for federal and municipal government involvement in telecommunications infrastructure, whether through policy or provision,) early municipal broadband projects faced strong criticism (Baller 2005), and opposition from the telecommunications industry (Stone, Maitland et al. 2006; Tapia and Ortiz 2006).

Partly as a result of this debate, and related legislative action (Tapia and Ortiz 2006), the emerging dominant model for municipal broadband networks seems to be a public/private partnership, where the private partner owns the network and has a dominant role (Gillett 2006; Daily Wireless 2007). In this model, sometimes called a *private consortium* model, a private company (or companies) funds the design, deployment and operation of a network, and charges fees to subscribers. In turn, the municipality provides access to city assets such as light poles, may agree to act as an anchor tenant for the network, and may negotiate with the private provider to offer affordable rates for low-income users (The Wireless Philadelphia Executive Committee 2005). This model may increase the number of local broadband providers by adding one additional player to the local market, but, on a larger scale, it does little to increase competition, and may, in fact, privilege this new provider. This is ironic, given that some of the loudest arguments against municipal involvement in the provision of broadband have been that municipalities, if given the opportunity to offer broadband service to residents, would monopolize the market. That is, municipalities could use an unfair tax and regulatory advantage, making it impossible for private sector providers to compete, therefore stifling competition (Baller 2005). In actual practice, this situation has been turned around. Many municipal projects, because of municipalities' limited opportunity – whether for legal or political reasons – to participate directly in the broadband market, have found the most feasible way to bring broadband to their community is to support what are essentially (city endorsed) local private-sector broadband monopolies.

The private consortium model has become prominent partly because it can be economically and politically attractive for communities to obtain a broadband network for local use with little or no up-front investment on the part of the municipality. Public/private models where the private sector finances the majority of the network infrastructure may indeed be in a community's interest in terms of building a network cost-effectively, with little risk to municipal finances – this is something that must be determined in each local context.

Despite the dominance of this particular public/private model, there are a wide range of public and public/private broadband models, and roles that a municipality might play in a broadband network (Gillett, Lehr et al. 2003; Bakowski 2005). For example, as it was investigating possible options for its citywide wireless network, Philadelphia defined five models: Public Community, Cooperative Wholesale, Public Utility/Authority, Non-Profit, and Private Consortium (mentioned above). The models differ in terms of who funds and has control over the network, whether this is a municipality, a private company, a non-profit, or a public utility, and who provides service to customers. Most models involve some kind of partnership between the public and private sectors – only the Public Community model does not explicitly include the private sector (The Wireless Philadelphia Executive Committee 2005). Notably, Philadelphia ultimately, choose a public/private partnership with Earthlink, reminiscent of the Private Consortium model (Vos 2006g), which did not score as highly as some other models in terms of meeting the city's priorities (The Wireless Philadelphia Executive Committee 2005).

Another facet of the public/private broadband debate is ownership, specifically the difference between public and private ownership of networks. While for financial and political reasons public-private partnerships like those of Philadelphia and San Francisco with Earthlink may seem like good investments in the short term, these projects could be unwise in the long term. These partnerships, where the private-sector partner owns the network, may mean that the public sector retains little voice in governance, which may become increasingly problematic if private and public interests diverge over time (San Francisco Budget Analyst 2007). Thus, in the long term, the public good trade-off for opting for a privately owned network may be higher than the risk and cost it takes to finance a publicly-owned one. When a network is publicly owned (but not necessarily publicly operated), a municipality maintains basic control over rates and service coverage, and can provide for its own communication and data transmission needs at-cost (San Francisco Budget Analyst 2007). While advocates of private broadband networks downplay the distinction between public and private ownership, public ownership can have important additional public benefits, including: public control of high-speed information networks – an essential public infrastructure; ensured competition; generation of significant revenue; ensured universal access; and non-discriminatory networks (Daggett 2007).

Future research should explore more closely the nature of emerging public/private partnerships: Why are public/private hybrid business models chosen? Who initiates these projects? Do these projects tend to be publicly or privately owned? If publicly owned, what is the role of the private sector? If privately owned, what is the role of the public sector? In particular, is the private company required to open its network at a wholesale rate to other private providers? What is the municipal role in relation to governance of a privately owned and/or operated network – is a role for municipal governance legally built in? And, do these networks promote competition?

What is Public Broadband?

Within the larger debate over the appropriate role for the private and public sectors in broadband, there has been a smaller discussion on the definition of public broadband (Richardson 2007; Ellison 2007a; Daggett 2007b; Ellison 2007b). While this definition is important, framing it with the term "public broadband" can be misleading. The term "public broadband" seems to imply that there are only two options: public or private broadband, when, in reality, there is a wide range of public/private models for broadband networks. While some broadband models could arguably be more appropriately called public than others, we believe that a more useful definition is of what a broadband network *in the public interest* may look like. A broadband network in the public interest may be publicly or privately owned, publicly or privately operated, or any combination of the two. Such a network could be achieved with a wide range of business models, and may be achieved differently in each community, based on local priorities and constraints. A broadband network in the public interest meets a set of criteria that are independently of public or private ownership.

Principles of Good Infrastructure

"Governments have a traditional role to fulfill – making certain that essential services such as the highway and telephone systems are available to everyone at prices that will enable citizens to partake without subsidy. Consequently, Federal, state, and local governments all play a major role in ensuring the nation's commitment to universal service and satisfying the "public interest." As more and more policy makers consider advanced telecommunications as an essential and thus, a needed universal service, a number of local governments have chosen to upgrade or create their own community's basic information systems to satisfy their commitment to the community," (Bakowski 2005: 9).

The goal of this paper is to develop a set of principles – a desiderata – for broadband infrastructures in the public interest. The paper can be contextualized within the wider field of public infrastructure, encompassing, “the large-scale public systems, services, and facilities of a country or region that are necessary for economic activity, including power and water supplies, public transportation, telecommunications, roads, and schools,” (Encarta 1999). Clear principles have been established to guide the general development of infrastructure, such as those proposed by the Ontario Ministry of Public Infrastructure Renewal (Ontario Ministry of Public Infrastructure Renewal 2004), and the role the private sector may play in its development (OECD 2007). This section discusses the desiderata in the wider context of public infrastructure principles.

Infrastructure is a complex and controversial topic, with many opinions about what structures and services should be included in the definition of basic public infrastructure. In addition, because the tools we use in our daily lives are constantly evolving, our definitions of infrastructure shift: "conceptions about infrastructure are changing and the list is expanding to include new, non-physical items that have not traditionally been thought of as infrastructure." Currently, “many economists are broadening the definition [of infrastructure] as a result of the demands of the new information economy, realizing that softer forms of infrastructure are just as important to competitiveness and attracting investment as are the physical, traditional, and hard forms of infrastructure," (Vander Ploeg 2003: 4).

Despite these changes in the definition of infrastructure, general infrastructure issues include: infrastructure spending and investment (Vander Ploeg 2003), how public infrastructure influences the economy (Harchaoui and Tarkhani 2003; Harchaoui, Tarkhani et al. 2003), the role of the private sector in public infrastructure development (Ontario Ministry of Public Infrastructure Renewal 2004; OECD 2007), and how to calculate and address infrastructure deficits (Vander Ploeg 2003). The broadband infrastructure debate is structured around similar issues, including who should fund broadband projects, the connection between broadband and the economy (Gillett, Lehr et al. 2006), the role of the public versus the private sector in broadband development (Baller 2005; Tapia, Stone et al. 2005; Ellig 2006; Daggett 2007a), and broadband deficits in the form of local, national, and global digital divides (Dutton, Gillett et al. 2004), including those between advanced broadband nations like South Korea or Japan, and the United States (Turner 2005).

Infrastructure Canada (Vander Ploeg 2003) suggests a comprehensive framework for understanding infrastructure, by defining a range of infrastructure types: "a taxonomy of infrastructure that … comprise[s] terms such as traditional and non-traditional infrastructure, core and non-core infrastructure, hard and soft, tangible versus non-tangible, and even notions of natural infrastructure and human potential and capital," (3). Under their classification (Basic Inter-Urban Infrastructure, Basic Urban Infrastructure, High-Tech Infrastructure, Amenities, Knowledge-Based Infrastructure, Health Infrastructure) broadband would be categorized as High-Tech Infrastructure:

> High-Tech Infrastructure: This category would clearly include physical systems that support a range of new and emerging technologies that are becoming more and more critical to modern society. Items would include cellular and satellite telecommunications, the Internet, and e-mail. This infrastructure is tangible and hard, but non-traditional. (3)

The definition of High-Tech infrastructure addresses the position of broadband as something that has not been traditionally thought of as infrastructure, but that is arguably becoming a basic component of it. One model of ICT infrastructure that addresses the breadth of 'hard' and 'soft' dimensions is the 'Access Rainbow', which articulates a 7-layered socio-technical architecture with the aim of promoting internet access in its multiple facets. These layers metaphorically extend the conventional telecommunications protocol stack to include Carriage, Devices, Software Tools, Content/Services, Service/Access Provision, Literacy/Social Facilitation and Governance (Clement and Shade 2000). In this paper we concentrate mainly on the carriage layer, but the other come in as well.

Because broadband internet infrastructure does not fall neatly into the category of traditional, hard infrastructure (roads, water, electricity, etc.), policymakers may have difficultly justifying spending public money on its development. Partly as a result, development of broadband infrastructure has been largely left to the private sector. This approach has left many gaps in connectivity because it has not been profitable for broadband companies to provide service everywhere. As during the development of national telephone infrastructures, communities by-passed in part, or entirely, by broadband service are taking its development into their own hands (Fischer 1988; Fischer 1992; Sawhney 1992; Sandvig 2002), as is evident in the emergence of the municipal broadband movement.

Universal service has been a key aspect of public policy, including telecommunications policy, and helped to establish nearly ubiquitous landline telephone penetration in North America, including locations where companies can make little profit providing service (Beachboard, McClure et al. 1997; Mueller 1999; Dowding 2001). Universal service legislation is not necessarily needed to ensure communications technology availability and adoption, particularly where other factors favor general affluence and market dynamism. For example, mobile phone penetration is nearing one hundred percent in Western Europe (MobileTracker 2005) and elsewhere without a universal service policy targeting this technology. Nevertheless it seems that a universal service orientation towards high-speed Internet may be necessary to ensure that it reaches all North Americans, as large areas remain underserved (Xavier 2003; Turner 2005a; Turner 2005b). Some have argued though, that just as effective and ultimately less costly, may be to wait for these developments to emerge further through the market before moving forward with universal service legislation (Dutton, Gillett et al. 2004). In the meantime, as noted above, by undertaking municipal broadband projects that aim to provide ubiquitous service, municipalities are essentially taking the gap between need for service and the lack of universal service policy for high-speed Internet into their own hands. San Francisco, for instance, stipulated that it would only accept proposals from private service partners whose plan to provide wireless for the city would include at least some level of free internet access for all (City and County of San Francisco 2005).

APPLYING THE DESIDERATA

The desiderata is a tool for assessing the design and effectiveness of proposed or operational broadband networks in terms of their relevance and benefit to members of the public. This section shows how the desiderata may be applied to particular contexts.

Diverse Projects, Diverse Contexts

While we recognize that broadband projects can be significantly different from each other, we have designed these desiderata to be applicable to projects regardless of size, business model, or governance model. We contend that for all broadband networks, these same basic factors are in the public interest. We anticipate that there are many business models that can meet the criteria of the desiderata, and that the desiderata can help communities to develop new ones. In addition, while our discussion focuses on internet infrastructure with an emphasis on Wi-Fi, these same principles apply to networks that support other applications, and make use of other broadband technologies. For all cases, the desiderata provides a basic set of criteria for judging alternative broadband network proposals in terms of their relevance and benefit to the user. Of course this intended generality comes at a cost of some specificity that may be relevant to particular circumstances, but these broad principles at least provide a starting point from which to make more nuanced adjustments.

Assessing emerging broadband network models in terms of their benefit to users is valuable, as the models that are established now may become the standard for future projects. In particular, it would be prudent to assess how the dominant public/private (private consortium) model looks from the point of view of users. If this model were to become the dominant "public" broadband model – as it seems it may – what would networks look like? From the perspective of network users – the public, is this a wise route? How do these networks measure up to the desiderata? What are their benefits and drawbacks?

Assessing Trade-Offs

The network characteristics prioritized in the desiderata are not achieved in isolation from each other. These characteristics can be mutually reinforcing, for example, a ubiquitous, open network is likely to also be widely useful. However, in many situations network designers will face trade-offs between desired characteristics. For instance, many of the desired features, notably universality, ubiquity, high quality may be costly to achieve, potentially undermining affordability. . Because public wireless networks should be cost effective, the development of viable business models for service provision is essential. Thus, when assessing business models, an understanding of the context of the network deployment, and a balance between desiderata points, is crucial. Potential trade-offs between ideal network characteristics are discussed in the desiderata itself, such as the tension between privacy and security, or the benefits and drawbacks different technologies hold for achieving ubiquity and reliability. Due to local contexts and constraints, we anticipate that projects will prioritize some desiderata points over others. This section shows how the desiderata can be used to recognize and assess potential trade-offs between desired and critical network elements.

Municipal and community broadband network designers are familiar with assessing trade-offs; this is part of the process of policymaking (Bakowski 2005). In fact, the private consortium model could be seen as a compromise between the public and private sectors. The public gains a (limited) role in network design and a network for their community. The private sector partner obtains a new contract, and may agree to public benefit contributions, such as digital inclusion rates like those in Philadelphia (Wireless Philadelphia 2007a) and San Francisco (Government Technology 2007). While such an arrangement may be the least politically and financially complicated, we are wary of the conclusion that this is the best, or the only, way. There are clear examples of alternative network configurations, such as the UTOPIA cooperative-wholesale network (http://www.utopianet.org/), the OneCommunity region-wide consortium network (http://www.onecleveland.org/), and the St. Cloud, FL public utility network (Vos 2006d), among others. Again, the most important question is, what does each of these networks look like from the perspective of users? What do users lose or gain from each network model? The desiderata can help to assess the differences between these models, and potential trade-offs between them, from a user perspective.

Different ways of applying the desiderata to make such assessments may be developed. For example, those using the desiderata in the process of network design might follow Philadelphia's example. As the city began to consider initiating a wireless network it conducted a detailed study of which model might work for them based on a set of principles (a "desiderata") they defined for themselves in the particular context of Philadelphia. The feasibility study team then prioritized the characteristics, by naming each of them as either a "must" or "want" and weighted the characteristics by importance within these categories. The team used this list to analyze different business models, ranking them based on how well they could support each of the desired attributes. While it was clear that no one business model was perfect, with some ranked higher in some areas than others, this exercise helped make clear the pros and cons of each.

A similar analysis using this (more comprehensive) desiderata might begin by considering how each of the desiderata points relates to the community in question. At this stage it may be useful to refine the points to make each one of them more concrete, and to make a clear connection to local goals. For instance, "Affordable" could be reframed as "a network with a basic level of free service, and higher speed service for under $15/month". The desiderata attributes could then be ranked in order of importance to the community. Which attributes are a must? Where could the project, if needed, compromise? Business models could then be assessed based on how they measure up to these criteria.

From Design to Assessment

The desiderata may be useful at different stages of a project, and this section describes how, providing a list of documents and other information that may be useful to collect about the project to be analyzed.

In brief, the desiderata can be useful in:

- Network Design: The desiderata can be used to identify key network attributes, and potential trade-offs between desired attributes.

- Assessing a Business Plan: The desiderata can be used to help determine which business model may be most appropriate given local priorities and constraints.

- Developing and Assessing RFPs: The desiderata can be used to both develop a RFP by using it to create a list of necessary attributes, and to assess RFP responses by analyzing how proposals measure up to the network characteristics outlined in the desiderata.

- Long-Term Planning: The desiderata can be used to identify ideal network attributes and to develop a long-term plan for network development. For example, a community might develop a plan to first deploy a wireless network as a way of achieving connectivity quickly, and plan for a later investment in fiber, to bring the community more reliable, higher quality service.

- Evaluating a Planned or Operational Network: The desiderata can be used to evaluate a planned, or operational broadband network, in terms of how the network measures in terms of its benefit to the public. This can be a way of assessing the success of a network, and also re-thinking network design.

Useful Documents and Data

The desiderata can be used by people with various relationships to a project, including those directly involved in the network design and deployment, policymakers, consulting partners, researchers, independent assessors, and community members. This section provides a list of documents and other information that may be useful to collect about the project to be analyzed, divided into two general categories – planning and evaluation.

Firstly, the desiderata can be used as a planning tool. That is, as a guide for communities initiating broadband networks, as a tool that helps to illustrate the range of issues that a community should consider as they move forward with a broadband project. The following data and documents may help communities to shape local priorities and navigate potential trade-offs between network attributes:

- Stakeholder consultation in terms of accessibility, affordability, and services desired/required.
- Evaluation of possible project champions (a municipality, a community group, non-profit organization, public/private partnership, entrepreneur, etc.) in terms of what they may be able to contribute to a broadband network, and to what extent they are likely to work in the public interest.
- Funds available for the network.
- Contextual data including number of households currently with broadband, policies and standards of networks serving similar communities, local/state/federal legislation affecting the project, price/speed/coverage area/etc. of existing broadband services in the community.

Second, the desiderata can be used as an evaluation tool. The following data may help evaluators to assess the network:

- Technical testing data on network ubiquity, reliability, quality/speed, as well as stated coverage area, reliability, and quality guarantees.
- Types of network services, who offers them, and who has access to them.
- Network business plan, customer service policy, health policy, security policy, privacy policy, neutrality/openness policy, future-preparedness policy.
- Evidence of and access to stakeholder consultation in terms of accessibility, affordability, services desired/required.
- Comments of users on network service, including how it measures from their perspective(s) in terms of ubiquity, universality, reliability, quality/speed, customer service, responsiveness, security, neutrality.

- Contextual data including number of households connected before and after network establishment, patterns of network use, policies and standards of networks serving similar communities, local/state/federal legislation affecting the project, price/speed/coverage area/etc. of existing broadband services in the community.

For elaboration on these, we turn to Part II of the paper, which describes the desiderata itself.

PART II – THE DESIDERATA

INTRODUCTION

In this section we argue that broadband networks that best meet the needs of a wide range of users should be: Ubiquitous & Universal, Widely Useful, Usable, Accessible, Affordable, Reliable, High Quality, Healthy, Cost-Effective, Accountable & Responsive, Secure, Privacy Enabling, Open, and Neutral & Non-Discriminatory. We define each of these 14 topics, which have been grouped in to 5 thematic clusters, and discuss them drawing on relevant literature, and our knowledge of the municipal broadband movement. Also included is a discussion of how a broadband project might be assessed in terms of each point. Finally, while research on broadband has addressed many of the issues discussed in the desiderata, there are some areas where more research is needed; we identify these areas.

Throughout our discussion we place a special focus on the public sector role in providing broadband networks in the public interest. We recognize that privately owned and built networks can, and should, also be considered in relation to the creation of broadband networks, including the roles the private sector has played, and may play in the future in terms of providing broadband that benefits users. In terms of this paper, a focus on public sector examples, particularly from municipal wireless projects makes sense for a number of reasons, including: the municipal wireless movement is an important window into a range of key public broadband issues; and municipal wireless projects (as "public" projects) are theoretically in the public interest. We need a tool to assess whether they really are, and to help ensure that they are. In addition, the public sector can play a unique role in ensuring that broadband networks benefit users. In cases where networks are not publicly owned or operated the public sector may still have an important role to play in terms of negotiating an accountability and oversight agreement with private sector partners, or a plan to make sure that the entire community receives at least a certain level of affordable, high quality broadband service.

UBIQUITOUS & UNIVERSAL
WIDELY USEFUL
ACCESSIBLE
USABLE
AFFORDABLE

For a broadband network to benefit a user, the user must be able to access the network with relative ease. Following some basic principles can help to ensure ease of access for users across a municipality or region. A network should be **ubiquitous**, that is, reach every place that it is needed, and **universal,** that is, it should be available to every person. Good infrastructures allow for a wide range of applications people find useful in conducting their daily affairs, likewise, a broadband network should be **widely useful.** This network should be **accessible**, that is, its design should take into account, as much as possible, different user groups and their needs, and be **usable,** that is, so straightforward that it 'disappears' in the sense that it can be taken for granted. Finally, a network should be **affordable,** charging a reasonable, accessible, price for service. This section defines each of these principles (ubiquitous & universal, widely useful, accessible, usable, affordable), shows how they have played a part in municipal wireless projects to date, how they interplay with digital divide issues, and how an existing or planned network might be evaluated in terms of its performance in these areas.

UBIQUITOUS & UNIVERSAL – service coverage should include every household, business, organization, public space, tourist destination, and public transit corridor in the network's coverage area, within the limits of what is technically feasible. Ultimately, the service should reach every person when and where they need it. Wireless contributes to enlarging service coverage to areas that are not easily reachable by wireline.

The Goal of Ubiquity: Approaches to Public Wireless Architecture

Ubiquity, "coverage of every place", has been a widespread goal of municipal wireless projects. Community and private sector broadband projects may also address the question of ubiquity, but for practical or market reasons, have been less likely to make this goal a center-point of their strategies, at least in the short-term.

Municipalities have used a number of approaches to enhance local connectivity via wireless technology. Like the community groups Île Sans Fil in Montreal (www.ilesansfil.org) and Austin Wireless (www.austinwireless.net) in Texas, or private providers like T-mobile, municipalities have used "hotzone" approaches – creating an aggregation of wireless hotspots that share a single management system but are not necessarily continuous. Municipalities, often in collaboration with a private vendor, have also followed a "citywide" approach – creating a cloud of continuous wireless coverage over a large area (Shamp 2004; Muniwireless 2007a). These networks that aim to cover significant portions, or all, of a municipality or region have generally been the subject of more interest and enthusiasm. While it may in some instances make more sense to provide connectivity neighborhood by neighborhood, as in the case of Wireless Harlem (www.wirelessharlem.org) in New York City, or to target specific locations, such as low-income apartment buildings (Zager 2007), municipal wireless projects tend to aim for as wide a range of coverage as possible – ubiquitous coverage. This is true of both large-scale projects, such as in Philadelphia, San Francisco, and Taipei, and smaller-scale projects, such as in St. Cloud, FL and Chaska, MN. We believe that this approach is, generally, in the public interest, as it helps to ensure that every place, regardless of profitability, or level of current demand, is served by a network. This is important because high-speed Internet is likely to be important basic infrastructure for many devices and applications in the future.

Ubiquity is *Not* the Same as Universality!

Universal service has been a key aspect of telecommunications policy, and helped to ensure that telephone service reached nearly every household in North America, including locations where the private sector saw little profit in providing service. The corresponding goal of ensuring broadband access for those where it is not profitable is a major issue in the broadband policy arena (Dutton, Gillett et al. 2004). Therefore, while it has been a less explicit focus of broadband projects to date it is important to also highlight **universality** ("service for every person") as a complementary to, but distinct, concept from ubiquity ("service for every place"). Achieving ubiquity is a part of achieving universality.

The Digital Divide

Public broadband projects can be contextualized in a number of debates, namely the high-profile municipal wireless debate, the digital divide debate, and the open access and network neutrality debates. Each of these debates take on similar issues from different perspectives. The points where these debates overlap are important, and municipal wireless and digital divide debates converge most directly in their mutual concern for universal, accessible broadband.

"Digital divide" is a mobile concept; its meaning has changed as technology has evolved. Generally, it refers to the gap between people who have access to and can use the popular information and communications technologies of the day (Gunkel 2004), be it a computer, dial-up Internet access, a mobile phone, or broadband internet access, and those who do not. Digital divides are found both between countries and within countries, between communities and within communities. While a number of factors, such as computer literacy, perceived usefulness of technology, education level, and cultural practices, affect digital divides (Wareham, Levy et al. 2004), making sure that a community has access to local, affordable information and communications technology, notably broadband internet, is widely viewed as essential to bridging these divides.

Government sponsored technology access programs, such as programs to provide computers in libraries and schools, have long been a part of information and communications technology policy (Jaeger, Bertot et al. 2006), but as work, social life, and entertainment become increasingly tied to the use of a personal computer and broadband internet, the focus of digital divide initiatives must be expanded beyond formal educational settings. This expanded vision of bridging the digital divide is what drives, among other municipal projects, the ambitious Wireless Philadelphia project. Although the city has a three-pronged mission it hopes to accomplish with its wireless network, to (1) bridge the digital divide, (2) strengthen the economy, and (3) make City services more efficient (The Wireless Philadelphia Executive Committee 2005), a digital divide focus characterizes the project: "Wireless Philadelphia was created to transform Philadelphia's neighborhoods by making high-speed Internet access more available and affordable through Digital Inclusion – the initiative that helps people who are not online gain access with hardware, software, tech support/information, and broadband Internet service, so they can begin to use this technology to improve their educational, employment, health, and life opportunities," (Wireless Philadelphia 2007b).

Smaller communities have also made the commitment to provide affordable high-speed Internet service to citizens by building their own networks (for instance, Chaska, MN provides residential service and Fredericton, NB built a fiber network to serve the municipal, university, school, hospital (MUSH) and business sectors), facilitating the build-out of local networks by engaging in public-private partnerships, or regional collaborations (for instance, the OneCommunity project in Northeastern Ohio). While not all communities that focus on bringing affordable broadband to those in the community that do not currently have access to it use the term digital divide to describe their projects, this focus is widespread.

A Role for the Public Sector?

Research indicates that local government involvement with local broadband networks can help bridge the digital divide in several ways. What the best role for government from a public interest perspective might be is contested and depends on a number of factors: the case for a public role is complex and that the optimal policy is likely to depend critically on the type of wireless infrastructure that is being deployed and the objectives for the system (Lehr, Sirbu et al. 2004: 31). For example, while the relative low-cost and flexibility of wireless technology may make it more feasible for municipal governments to consider offering broadband service, these same factors may make it more feasible for the private sector to offer service where it did not before. Thus, a wireless network initiated by a municipality may be something that the private sector, given more time, would have developed on its own. On the other hand, "the benefits of wireless may enhance the perception that broadband constitutes essential infrastructure that needs to be provided by government because the social benefits of ensuring adequate access to such services exceed what private carriers can expect to appropriate," (Lehr, Sirbu et al. 2004: 31). This will be the case especially where there are pre-existing income and other socio-economic disparities.

Furthermore, although it may be possible that inclusive wireless ecosystems will evolve on their own (Negroponte 2002), wireless systems seem to evolve following the existing parameters of the digital divide. In their study of the Austin, TX wireless environment Fuentes-Bautista and Inagaki (2005) found that those areas and people that were already relatively well served by information and communications technologies seemed to be most likely to receive the additional benefit of wireless access first. The community groups and private sector companies involved in building wireless hotspots in Austin, for the most part, did not see the role of their wireless initiatives as closing the digital divide, even if they aimed for their hotspots to be a public benefit. Instead, "despite the presence of talents, local technological expertise, and a dense network of collaboration among the public and private institutions, we observed an uneven growth of public Wi-Fi infrastructure. Wi-Fi initiatives are mostly serving the best-connected and technologically savvy users of the Internet population in the city. Public access of high-speed wireless services is virtually absent in the city's ethnic minority and low-income areas," (Fuentes-Bautista and Inagaki 2005). Although the Austin city government, in the 1990s, had attempted to build a citywide advanced telecommunications network serving the citizens, businesses, and institutions using installed capabilities and the fiber rings surrounding the city (Berquist and Grant 1999), a state bill prohibiting the provision of telecommunications services by municipal entities in 1995, and the opposition from incumbent telecommunications providers had effectively stopped the initiative – this is unfortunate as the municipality could have played a key role in *working with* private and community groups to make sure the city's digital divide was addressed.

Research based on the digital divide and municipal broadband cases indicate that government can help initiate networks that more comprehensively address digital inequalities than solely private sector projects, or community projects with limited resources (Fuentes-Bautista and Inagaki 2005). This is not to say that community and private players are unimportant; they also play an important role in digital inclusion strategies. But, in communities that have been successful in closing digital divides, the public sector has often been involved. Likewise, in countries with the best broadband penetration, national governments have worked in stages to provide or enable access for priority sectors, including universities, local schools and local government (Dutton, Gillett et al. 2004). In particular, local government can help to bridge the digital divide by acting as an aggregator of demand, as a coordinator between various public and private sector players (for example, the Berkshire Connect Task Force, www.bconnect.org), and by financing basic network infrastructure (Boston Wireless Task Force 2006; Cherry 2006; Daggett 2007a).

In addition, despite arguments to the contrary (Baller 2005; Baller and Lide 2006), local government action, in the absence of national legislation can be an essential part of making broadband markets more competitive, leading to better prices and better service for citizens/consumers (Boston Wireless Task Force 2006; Daggett 2006; Daggett 2007a). At a basic level, governments committed to a competitive market can help less powerful players participate in the market (Dutton, Gillett et al. 2003). For example, local governments can manage, or build, municipal infrastructure useful to wireless ISPs and other applications providers, including telephone poles, sewer systems, and wholesale broadband networks, allowing private competitors equal access to this infrastructure at a fair rate. Thus, in order to promote competition, which is likely in the public benefit, municipalities should be wary of signing contracts with private providers that allow them exclusive access to city infrastructure – something that seems to be an emerging practice (Gillett 2006).

Why is Ubiquity Important?

The ideal of ubiquity has come recently to prominence with the growth of Wi-Fi. Yet, the ultimate benefit of ubiquity may not be as it is currently envisioned by many municipal wireless projects. In fact, in terms of providing Internet access - the hot-topic for municipal broadband projects - money might be better spent targeting individual homes, offices, and select public spaces, such as libraries, cafes, and airports, rather than on creating a cloud over an entire municipality. As the city of Taipei, Taiwan found when it created a vast wireless network whose coverage included areas previously uncovered by private hotspots, such as subway stations, people will not necessarily make use of internet service in all types of public spaces (Belson 2006). There are practical reasons for this, including the difficulty and discomfort of using a laptop outdoors, especially in cold, hot, rainy or extremely sunny weather. Though, as small laptops and other Wi-Fi enabled devices, such as the Nokia's Wi-Fi tablet and the Apple iPhone become more common, it is likely that people will make more use of ubiquitous networks, rather than fixed spaces, for their communication needs (Perkowski 2007). The rationale behind the current drive of municipal wireless projects for ubiquitous coverage is an area that should be further investigated: Do municipal broadband projects tend to provide indoor coverage, outdoor coverage, or both? What reasons do they give for doing so? What do these projects envision the usefulness of ubiquitous coverage to be?

Broadband ubiquity may or may not be essential to internet-based communication now, but it is likely to be important for the internet of the future (Cisco 2006; International Telecommunication Union 2006). In a society where daily-life devices require access to a communications network to function properly, ubiquitous service becomes increasingly important, and divides between those who have access to this service and those who don't become increasingly problematic. Ensuring ubiquitous coverage will not necessarily mean that universal use will be achieved, as there are many social, economic, educational, and cultural factors that complicate the use of technology, even when it is available. For example, a study of the Computers in Homes (CIH) initiative in New Zealand in which free computers and internet access were given to selected low-income households for a very small fee, revealed that: "Internet ubiquity may not be a strategically useful social objective unless contextual limitations [such a sufficient number of technical staff to support the project and long-term guarantee of low-cost service] are recognized and addressed," (Williams, Wallace et al. 2005: 1). Yet, ensuring that every place is served by an affordable, reliable broadband network is an important first step.

Assessing Ubiquity

There are a number of measures that can be used to evaluate to what extent network coverage is ubiquitous. Testing for ubiquity can be combined with testing for network quality and reliability (see High Quality and Reliable sections). That is, not simply whether or not a signal is present, but how good the signal and connection is. Ubiquity, reliability, and quality can be measured through technical tests of the stated coverage area. Companies such as Novarum (www.novarum.com) and VeriWave (www.veriwave.com) have developed testing methods for wireless networks. For an overview of network testing methods, including functional verification, performance measurement, network capacity assessment, system testing, and stress testing see VeriWave (2007). In publicly initiated broadband projects testing can be required as a part of the proof-of-concept stage, and on an ongoing basis.

While technical testing is perhaps the most accurate way to assess network ubiquity and quality, it is not a direct indicator of network success. For example, the Toronto Hydro wireless network ranked first in an independent test of municipal wireless network speed, but ranked lower in comparison to other networks in terms of overall user satisfaction ratings (Novarum 2007). Other methods can also be used to assess network ubiquity and quality, including an assessment of whether the network has a mandate for ubiquity and target levels of reliability and quality. Over what area does the network aim to offer service? What kind of service is offered (indoor, outdoor, etc.)? Does the network aim to guarantee a certain level of reliability and quality (bandwidth speed, latency, jitter, etc.)? If not, why not? If so, why this area, and level of quality? And, finally, what do users have to say about the network? From their experience, is coverage available where it should be? Is it fast and reliable?

Assessing Universality

Determining whether universal service has been achieved is somewhat more difficult than measuring ubiquity – one component of universality. In addition to assessing ubiquity, an additional measure to assess universality may include comparing the number of potential users of the network with the number of actual users. Are all potential users using the network?[1] If not, what might account for this discrepancy? Currently, broadband service is available to more people than the number of people who actually use it (Dutton, Gillett et al. 2004), may it be for reasons of cost, perceived lack of need for the service, or other cultural and economic factors. Access to and analysis of network account and login data may be helpful in terms of determining how widely used the system is and from which locations it gets the most and least use. When this data is not available for privacy, or other, reasons, an alternative assessment might be performed through a user survey, and/or through contacting people who may provide a window into use in the wider community, such as local government representatives or community-based education and social service centers.

Measuring both ubiquity and universality may be the most direct ways to measure digital

[1]Note, we are not assuming that everyone *must* be an internet user, but rather that it be available to everyone who wants it or who could benefit from it.

divides and changes in them. As above, "the most easily quantifiable broadband divides are measured by statistics on how many people are close enough to a connection to gain access to a broadband service ('availability') and how many people with such access actually choose to take it up ('deployment', 'take-up' or 'penetration')," (Dutton, Gillett et al. 2003: 18). Thus, as the focus of municipal broadband projects is frequently to bridge local digital divides these measures are important indicators of the success or failure of such projects.

WIDELY USEFUL – Good infrastructures allow for a wide range of applications that people find useful in conducting their daily affairs. While some of the most important ones can be anticipated and designed for, others will emerge over time. Wireless brings obvious benefits of portability and mobility, but also opens up new possibilities (such as location-based services) that were not previously feasible. This expands usefulness, while serving as a platform stimulating new economic activity as suppliers enter with new service offerings.

Users currently make use of the internet in a wide range of ways, including for communication, learning, entertainment, and commerce. For example, applications and services such as e-mail, peer-to-peer file sharing, online purchasing, voice over IP, video conferencing, e-learning, and online-gaming, are commonly made use of. The internet is used for a wide range of daily tasks, often taking over these tasks from offline services, as is seen in the development of news media online.

The applications we witness and envision today for broadband are only the beginning of what broadband infrastructure may enable; as we design broadband networks we must keep this in mind. Broadband networks should be designed in such a way that they are not only useful now, but so that they remain useful in the future. For example, the way a fiber network is built can determine whether it is technically possible, either immediately, or at a later point, to run the network on an open access model (Banerjee and Sirbu 2005). We cannot predict exactly what these networks should look like, but by building networks that meet the criteria of the desiderata, we can help to make it more likely that they will be useful in the future. Attention to this is important, as many municipal wireless projects see their networks as an infrastructure that will help the community to be economically competitive in the future.

The proposed Boston wireless network (Boston Wireless Task Force 2006), in contrast to most projects, explicitly includes a wider vision of the future of broadband networks, and incorporates this vision into its network design requirements. A key feature of the Boston network is its focus on openness. Not only would internet service providers (ISPs) be able to provide any type of service – from free ad-based service, to daily or location-based subscriptions on the network, but the network aims to accommodate emergent business applications. To enable this flexibility, the network would be open to customizable service plans allowing businesses to purchase varying amounts of bandwidth. This is in recognition of the fact that companies providing some services, such as those that might use sensor and telemetry applications to track a fleet of cars, may actually require little bandwidth (Boston Wireless Task Force 2006; Ho 2006).

In summary, public broadband projects would do well to evaluate their existing or planned networks in a larger, long-term context: Is this network designed to support devices and services as they emerge? Is this network designed so that its usefulness is limited to currently available services and devices? Providers must separate hype from long-term viability. This may mean choosing to invest in a more expensive, but more future-proof technology such as fiber (Daggett 2007a), building a wireless network as *part* of a larger planned broadband infrastructure, or choosing an ownership model that may be politically and financially more difficult to initiate, but that guarantees openness and neutrality– and that therefore may ultimately foster a wider range of applications and services for users.

Assessing Network Usefulness

The extent to which a network is more or less widely useful is somewhat less straightforward to assess compared to other network qualities, because it is not possible to fully anticipate what will and will not be useful in the future. Still, the more open, flexible, and neutral a network is, the more likely it will be widely useful. Therefore, questions to assess usefulness include: According to its stated policy how open, neutral, and flexible is the network? That is, how many providers can operate on the network, and how easy or difficult is it for each one to do so? What devices can be used on the network? And, is the network designed with few or many applications in mind? Does the network anticipate change? Does it have a plan for adjustment to future developments in applications, devices, and user needs? What characteristics (for example, ubiquity, reliability, privacy) does the network anticipate will be useful to support future applications? In practice, does the network prioritize these characteristics?

We anticipate that networks that fulfill the basic criteria of the desiderata (ubiquitous, universal, usable, accessible, affordable, high quality, reliable, healthy, accountable, secure, private, open, neutral & non-discriminatory, etc.) are likely to be widely useful.

USABLE – Ideally infrastructures 'disappear' in the sense that they can be taken for granted – always ready to be used effortlessly, but never getting in the way of the immediate task at hand. Wireless internet offers a significant step towards this ideal with its potential ubiquity and growing availability of easy to use wireless-enabled devices.

A community served by a broadband network built in the public interest should be able to easily make use of the network. Using the network should be as easy as flipping on a light switch, or turning on a water tap. Both electric and water utilities have vast and complex infrastructures behind them, but they are straightforward and usable at the point where they meet users. This requirement – usability – may seem basic. But, simple, misguided assumptions in the design of a network can strongly affect how and whether users make use of it. For example, the Orlando, FL wireless network may have failed because of its inconvenient location and poor service (Vos 2005), issues that could have been prevented.

As a general rule, networks should be built to accommodate their users. A network that meets community needs should be easy to use. For example, if a network aims to provide residential service it should ensure that the process for bringing the signal inside the home is straightforward, something that has proved more difficult than expected in existing municipal wireless projects (Reardon 2006).

Assessing Network Usability

An assessment of network usability can be combined with an assessment of network accessibility (below).

ACCESSIBLE – Access to the system should be as barrier-free as possible, accommodating a wide range of cognitive and physical disabilities. The service should also accommodate a community's linguistic diversity. Conducting user needs analysis at the design stage and providing technical support can help to ensure that a network is accessible. Wireless enhancement can help make Internet services more adaptable to particular populations and individual user needs.

Accessibility is an issue of tailoring infrastructures, devices, or processes to the needs of particular users. It is often regulated by law and subject to special guidelines, for example, the Web Accessibility Initiative of the World Wide Web Consortium (www.w3.org/WAI). Factors other than access to technology can make it difficult for users to make use of a network, including cultural, linguistic and disability barriers. When networks do not take a wider range of accessibility issues into consideration they can lead to a continuation of the digital divide (Baker and Bell 2007).

The public broadband debate seems to have rarely considered such additional factors of accessibility – though, this is an area that would benefit from further investigation. Here, Baker and Bell's (2007) work on whether municipal wireless projects have taken the needs of people with disabilities into consideration is a useful model. The team analyzed the written documentation of 48 municipal wireless projects, including websites and secondary sources, for indicators that the projects were addressing accessibility for people with disabilities. They found that, despite the fact that people with disabilities face a significant "disability divide" in terms of access to broadband, none of the 48 wireless projects had any specific recognition of people with disabilities. They suggest that part of the problem may be a lack of awareness of the issues that people with disabilities face in terms of broadband connectivity, and that an action as simple as ensuring websites and other information about the wireless project for those with disabilities can significantly enhance disability inclusion.

In general, networks should meet the needs of the local community. Determining appropriate network characteristics may mean conducting research with community organizations and (government, residential, business, institutional, industry) stakeholders to better understand what types of users exist: What types of network and network services are needed? How familiar are potential users with Internet technology? What forms of assistance might they need to connect to and use the network? What portion of potential users own broadband and/or WiFi-ready computers? What languages may technical support be needed in? Do cultural or disability barriers exist that may affect how users would use a network, or, that a network could help users to overcome? While a municipality or community group may not ultimately provide service directly to users, it might still play a role by conducting, facilitating, or encouraging this research on behalf of its citizens or community.

Assessing Network Usability and Accessibility

Evaluating a network in terms of usability and accessibility is essentially an evaluation of whether the network is used and how easy it is to use. Questions include: Is the network used, and by whom? To what extent did stakeholder and community-based research inform the design of the network? What kinds, if any, of technical support are offered? Is this support offered free, or at a cost to users? Are these materials and support offered in appropriate languages? If the network is operational, it is also useful to consider what challenges the network has faced in terms of making the network accessible and useable for users: What are common user complaints, and by what strategies have they been addressed? What do users have to say about the network? These questions can be approached through a combination of methods such as municipal, service provider and user interviews or surveys, tests of the network from a user perspective (e.g. how straightforward is it to obtain the service and use the network?), reviews of city and/or service provider documents, and media analysis.

AFFORDABLE – in order to ensure universal access for all, including low income households, the service should be available at affordable rates (e.g. <$10 per month) and preferably for free. Ideally, the service should provide free access to basic broadband service (e.g. 1.5 Mbps, bi-directional as specified by (National Broadband Task Force 2001), with the possibility of fees for premium, higher speed services to support high bandwidth uses. Wireless service, because it can greatly reduce the cost for extending service into areas where wireline is relatively expensive, can help make Internet access more affordable.

The municipal and community broadband movements have sparked a number of debates around appropriate cost of user-access fees for broadband service. The most prominent debates have been over whether access should be offered for free or for a fee, and, similarly, what business model can strike the right balance between long-term network sustainability, network quality, and low user fees. This section evaluates the reasoning behind these debates, including factors that may have influenced the idea that wireless broadband ought to be low-cost. Based on this, the section presents an approach for thinking through why (or why not) networks should aim to be low cost to users, how this might affect network design, and how to evaluate a network from the perspective of affordability.

A driver for low-cost-to-the-user municipal networks likely stems from the origins of many municipal broadband projects as efforts to bridge the digital divide, either for an entire underserved community, or for underserved and/or low-income members within a larger community. In this context cost is certainly a major issue, among possible others (Rideout and Reddick 2005; Tapia, Stone et al. 2005). Thus, making sure lower-cost access is available for a community is one concrete action that can be taken to close the digital divide.

Another reason why the concept of low-cost user access to wireless broadband networks has been so widely promoted and debated is because Wi-Fi has acted as a technical enabler of municipal and community systems. Wi-Fi technologies are relatively inexpensive to deploy, which should in turn make access to Wi-Fi networks relatively cheap. Another technology-based influence on the perception that access to wireless networks should be low-cost is likely that Wi-Fi operates on the unlicensed spectrum band, which unlike licensed bands, does not require access rights or an access fee (Wi-Max.com 2007). As spectrum access for wireless providers is free, it might be argued that this cost savings should be passed on to users. Though since wireless typically does not stand alone, but is built on top of other internet technologies, usually wireline, its cost savings can only go so far.

Free Service Debate

One of the most vigorous debates in the municipal wireless movement has been over whether the service can and should be offered for free. At first this may seem surprising. How could a municipal utility, such as water or electricity, be offered for free? Wouldn't some taxpayers end up paying for more than their share of use? Yet, since broadband is a utility that is more similar to roads, offering access for free may make sense. Roads are generally supported through tax money (e.g. not completely free, someone has to pay). Roads, with the exception of toll-highways, are therefore "free" to users who pay taxes as well as to visitors to the area. Roads can accommodate greater or lesser numbers of drivers, within reasonable limits, for the same maintenance costs, meaning that the city's costs are nearly fixed regardless of the number of users. Similarly, within limits, the costs for a wireless network over a certain geographic area and for a certain amount of backhaul are fixed, no matter the number of users.

What is meant by "free" in the free municipal and community wireless debates should be clarified. Ultimately, networks are not completely free: it is a matter of who pays. In most cases "free" means free-to-the-user, with government, small businesses, or the Internet provider supporting the system with other forms of revenue. There are a number of emerging free-to-the-user business models. These include:

- Ad-supported models, such as MetroFi service that aims to provide free wireless over large service areas, such as a municipality or region (MetroFi; Kim 2006; Cohen and Golvin 2007).

- Coordinated, business sponsored hotspots, like the models of community wireless groups Austin Wireless in Texas and Île Sans Fil in Montreal.

- Ad-hoc networks that have come into being due to individual actions of many users openly broadcasting the signals of their paid hotspots (sometimes inadvertently) to other users. For example, Taipei before Q-ware launched a citywide wireless network, had a large, organic open network (Belson 2006).

- Government supported free service in libraries and other public spaces, for example Toronto public library branches (Toronto Public Library 2007), or Fredericton, New Brunswick's best effort public wireless network (e-Novations 2005).

It is unclear if any of these network models will survive in the long term – they may be temporary solutions (Settles 2006). Even since they have been established these business models have evolved, with moves by major players to tweak their business models (Reardon 2007). For example, MetroFi, a company that offers ad-supported service for free and service with no advertisements to users for $20 a month, has refined their approach, and is expanding. As of 2006, MetroFi had set up a California network that covered most of the cities of Santa Clara, Sunnyvale and Cupertino, as well as downtown San Jose – a zone that includes 250,000 people. With plans to expand to Portland, the company has required the city to act as an anchor tenant for the network, guaranteeing MetroFi up to $16 million in the first five years to give municipal workers access to the network. MetroFi also draws revenues from its ad-free paid subscriptions, and saves money by not providing customer service and not actively promoting the free network, which does not need billing or processing services either (Kim 2006).

Is lack of customer service and quality-guarantee on a network a worthwhile trade-off for free service? Maybe. From a preliminary analysis it seems that residents of Fredericton, New Brunswick are generally pleased to have the city's best-effort wireless service that is provided free to users from excess bandwidth on the city-owned fiber network. But, they also understand that the network is sometimes slow and cannot always be relied on. Most residents access the network from cafes, rather than homes, where it is rare to get a signal, and, if they are regular broadband users, purchase a paid subscription from a commercial provider (Powell 2007). Alternatively, Philadelphia through its partnership with Earthlink, offers, not free, but reduced-rate broadband service for qualifying low-income users. Philadelphia's basic Earthlink service costs $19.95/month, and the digital inclusion rate $9.95/month. To qualify for the digital inclusion rate, customers must have an income at or below 150% of the federal poverty line, and/or qualify for other social programs, such as food stamps or Medicare. This means that a household of four would need to earn less than $31,000 per year to qualify (Wireless Philadelphia 2007a).

In addition, despite the common perception that Wi-Fi is low-cost, it is not necessarily the least expensive option. For example, in San Francisco AT&T is now required to sell DSL access for $10/month under the terms imposed by its acquisition of BellSouth. The proposed free San Francisco wireless is half the speed of this DSL service, and to use the free service residentially households would need to buy a wireless bridge for $80 to $200 or get the paid Earthlink service for $21.95 per month (Ross 2006; Daggett 2007c).

Each community must evaluate whether free Wi-Fi truly offers the best option for their users, or whether a better service can be provided by existing or other means. This means evaluating how free-service-for-the-user may impact other aspects of a community's communication infrastructure, for example, who owns and controls the infrastructure, whether network business models are financially sustainable in the long term, overall network quality, or levels of privacy (see below) guaranteed to users.

What is a fair user-fee?

Charging a user-fee for service may be a way to ensure that other important network attributes, such as reliability and privacy, are met. If a fee is to be charged for network access, what is a fair price? This question is difficult to answer precisely because every broadband deployment is unique to the local context, and because of unknowns associated with broadband (especially wireless) technology and emerging business models (San Francisco Budget Analyst 2007). Nevertheless, a useful first step to recommending a fair fee is estimating the cost of setting-up, running, and maintaining the network in the location in question. The San Francisco Budget Analyst's report (San Francisco Budget Analyst 2007) on the feasibility of a city-owned network provides one possible model for making this estimate, Zhang and Wolff (2004) provide another, with a rural focus.

It may be that, generally, networks run on a not-for-profit basis, whether by a municipality, non-profit organization, or a partnership, can keep user fees lower than for the same level of service as could be offered with a for-profit model. If the city of San Francisco, for example, were to own its own wireless network, it could reasonably charge users about $10 per month for at least the same quality of service as users would pay $20 per month for with the proposed Earthlink model (San Francisco Budget Analyst 2007). Though, solely in terms of affordability to the user, a non-profit model is not necessarily better than a for-profit model, as again, broadband networks can generate significant revenues from sources other than residential users, such as from government and institutional use or cost-savings. From the perspective of a user, lower-prices for better service stimulated by competition on an open-access wholesale network could also be a good option (Boston Wireless Task Force 2006).

Assessing Affordability

One step in assessing what an appropriately affordable network access price might be is to compare network user fees with user fees for broadband service of the same quality, both inside and outside the region. Prices within the region may reflect similar constraints and opportunities of area, for example service fees may be higher because of a relatively low population density, but local fees could also be high-priced as a result of a monopoly of the market, or use of a relatively expensive broadband technology versus wireless. Thus, prices for service in other regions with similar financial and demographic characteristics may be better indicators of a fair price. To assess affordability it is also useful to have access to the business model data (e.g. profit margins, revenue structures, etc.) of other local providers, and of the network in question. This can help to assess the reasons behind the user fee and whether it is higher or lower in comparison to that of similar projects. Another important factor in assessing the affordability of a network is evidence on the part of the network of awareness of what is affordable to the community it serves. What is a reasonable rate for one community may be prohibitively expensive for another. Programs like Philadelphia's Digital Inclusion Program (Wireless Philadelphia 2007a) work to address this difference within the city itself.

RELIABLE
HIGH QUALITY

A broadband network in the public interest is one that ensures **reliable**, **high quality** service. That is, service that is consistently available, and that ensures bandwidth (e.g. speed) that is not only sufficient in capacity to support most subscribers' desired uses of the network but also to encourage the development of new applications. While most municipalities engaged in broadband projects are likely aware of the importance of network reliability and quality, these factors have not been an explicit part of the public broadband debate.

Nevertheless, reliability and quality are basic principles of good infrastructure, and ones that support networks as a whole. For example, although a community may achieve the goal of creating a ubiquitous, affordable network, if this network is unreliable and low-quality it may have limited use. Attention to issues of reliability and quality can influence key decisions on what type of network to build, including: feasible size of the network; what could be considered a reasonable level of up-front investment – a more reliable, higher quality, network may cost more to build; governance and accountability structures; and the technology used. This section illustrates how reliability and quality are important to the public broadband debate, including how these two factors come into play in decisions about network design, and how a network might be assessed in terms of them.

RELIABLE – the service should be as reliable as the other common utilities, such as water, power, and the telephone, with clear performance standards established (e.g. 99.99% availability, 4 hours mean time to repair) This likely represents the major technical challenge to wireless internet, as the unlicensed 2.4 Ghz spectrum used by 802.11b/g protocols is subject to interference by other devices (e.g. microwaves, door openers) and is highly susceptible to attenuation (e.g. by trees in residential areas).

Wireless Technology and Reliability

Reliability poses a major challenge to the public wireless movement. Wireless has been celebrated for its low-cost and flexibility, factors that can make it possible to build networks faster and less expensively. Unfortunately, while these qualities make wireless an attractive technology, in general, it is not as reliable as wireline technologies. Therefore, while wireless has helped to spark enthusiasm for public broadband networks, it also has some trade-offs. In some cases wireless may not be the technology in the public's best interest.

Reliability has been a challenge for first generation citywide wireless projects in terms of interference from the physical environment (wet leaves, buildings), a lack of 24-hour power supply to utility poles, and difficulties bringing wireless signals indoors (Reardon 2006). For example, Chaska, MN, despite its reputation as a model wireless community, has faced serious technical difficulties (Fleishman 2006). As one resident writes:

> "I am a resident of Chaska and subscribe to the Wi-Fi. We're thrilled at the low price of $17/month compared to the $45/month thru Sprint. We had some great luck with Chaska's service a while ago, but in the last 1-3 months, coverage has been spotty. We live in a stucco home next to mature trees and it's been raining a lot. Go figure...Seems like we pick up the neighbor's service (not chaska.net). I'm not technical in nature, so all I can tell you is that the solid orange light is on a lot on the router and that's not good." (Fleishman 2006).

Part of the reliability issue lies in the novelty of large-scale wireless networks. As these systems become more established, especially as an increasing number of long-standing technology companies, such as Earthlink and Cisco, join the market (Perkowski 2007), these systems are likely to become more reliable. This may include an increased integration of wireless with other broadband network technologies, such as fiber and WiMax (Oram 2007). For now, wireless has some technical challenges to overcome.

The Unlicensed Spectrum

Another challenge to the reliability of wireless networks is that the unlicensed 2.4 Ghz spectrum used by 802.11b/g protocols is subject to interference by other devices (e.g. microwaves, door openers). The opening of increased spectrum for wireless communication, and/or a new regulatory system for spectrum use could mitigate possible disruptions of service as the unlicensed spectrum is increasingly made use of by wireless devices (Meinrath 2005). The implications of various spectrum regimes in terms of creating networks in the public interest has been considered elsewhere (Noam 1995; Buck 2002; Bauer 2003; Benjamin 2003; Lehr 2004; Best 2006; Cooper 2006; Muleta 2006; Organisation for Economic Co-operation and Development (OCED) 2006; Sandvig 2006; Sicker, Grunwald et al. 2006).

Ensuring and Assessing Network Reliability

Reliability should be a major consideration in network design, and is likely to affect network architecture and technology choices. Part of determining reliability standards is a consideration of what level of reliability is necessary for the network in question, and whether a trade-off in reliability may be reasonably made to enable other network attributes, such as free wireless service.

For all networks, clear reliability standards should be set, as well as a strategy to meet these standards, and guidelines establishing who is responsible for making sure they are met. For example, Philadelphia required its private partner Earthlink to build a network featuring a 1 Mb/s average data transmission rate, 95% outdoor coverage within the coverage area, 90% indoor coverage, and 99% network availability (Wireless Philadelphia 2007c). The recent decision by BelAir Networks, a provider of mobile broadband multi-service wireless mesh network solutions, to offer Service Level Agreements (SLAs) for municipal wireless deployments may help to make practices like this more standard. Under the BelAir program, Minneapolis will be the first city to receive performance guarantees for its municipal wireless mesh network. The new program insures that the vendor, BelAir networks, will provide the necessary equipment to bring performance up to expectation if the original design does not meet this standard (BelAir Networks 2007).

To help ensure that reliability standards are met in practice, the standards and the accountability structure for them should be made transparent, and mechanisms should be made available for users to report on service reliability. Service level agreements and technical testing of the network both in the “proof-of-concept” phase and in planned system checks by an independent authority are additional ways of measuring and ensuring reliability. Assessment for reliability can be combined with an assessment of network ubiquity. See the section “Assessing Ubiquity” (p. 24).

HIGH QUALITY – the service should maintain a good standard of throughput and response time for streaming or other time sensitive transmissions requiring particular Quality of Service (QoS) standards (e.g. public emergency, telemedicine). However, these should not be discriminatory in the sense of allowing the network provider to favor arbitrarily some communicants over others or permit inspection of packet content. As with Reliability above, wireless internet is challenging in this regard because of spectrum contingencies, such as interference and variable attenuation, as well as the greater difficulty in determining device identities as the basis for assigning bandwidth priorities.

While the core focus of the public broadband movement has been on making better, faster internet services available to more people, exactly what “better and faster” means is not often given the attention it should. Part of the issue is that while it is generally clear what the maximum standard for dial-up internet service is (56 kbit/s), the definition of broadband is less clear. For example:

- The FCC defines a "high-speed" connection as that transmits data at a rate of **200 Kb/s** in one direction. This is about four times the speed of dial-up (Turner 2005b).

- The International Telecommunications Union Standardization Sector defines broadband as greater than **1.5 Mb/s** (Daggett 2007), which is similar to the definition of the Canadian National Broadband Task force (National Broadband Task Force 2001).

- Broadband service in Japan is typically available at **12**, **26**, and **40 Mb/s** (Bleha 2005); and on a per megabit basis, U.S. consumers pay 10 to 25 times more than broadband users in Japan (Turner 2005a).

- The Fiber-to-the-Home Council called on the US Congress to ensure **100 Mb/s** of symmetric broadband to most Americans by 2010 and to all Americans by 2015 (Gubbins 2007).

- And, a bill introduced in the Minnesota state legislature even called for the availability of **1 Gb/s** of symmetric bandwidth to all Minnesotans by 2015 (Gubbins 2007).

How has such a wide range of numbers for what qualifies as adequate broadband bandwidth been reached? Given this wide definition of what quality broadband is, how is it possible to determine how fast is fast enough for a given group of users' needs?[2]

The most useful definition of broadband may be that of the National Academy of Sciences. The National Academy of Sciences defines broadband not as a speed but as a service that provides sufficient capacity and access to enable today's applications and encourage the development of new ones (Daggett 2007a). While this definition, because of its flexibility, is a useful place to start, defining a more specific bandwidth goal can help projects make the necessary technical and investment choices to successfully meet users' needs.

In North America, a modest but feasible starting point for broadband networks should to guarantee a minimum bi-directional speed of 1.5 Mb/s for a basic level of service. This means building networks that are robust enough to provide this level of service withstanding flux in network capacity due the number of users using the network, or other factors. And, although, networks typically guarantee a certain speed in at least one direction, a guarantee of network speed of at least 1.5 Mb/s in *both directions* is important. The directionality of bandwidth is noteworthy because it anticipates different types of users. Networks that guarantees a higher speed in downstream bandwidth anticipate users that will be acting primarily as consumers of content, for example, downloading videos or other media. A network that guarantees a higher speed in upstream bandwidth anticipates users that will be acting as producers of content, uploading files to send or share, or using the network interactively. While today's users tend to require more downstream than upstream bandwidth, there are indications that this is changing – for example, the growing popularity of uploading user-created videos to Youtube.com, or the increasing market for interactive online gaming, which requires high upstream as well as downstream bandwidth (Fitchard 2003; Gubbins 2007).

---

[2] It should be noted here that in addition to speed, other characteristics , notably latency and jitter are important indicators of the quality of service, particularly for interactive services such as voice over IP, which may have low bandwidth requirements but are highly sensitive to delays and interruptions.

Beyond meeting this basic level of service, there are a number of ways to work towards defining an appropriate target-speed for the project at hand. One strategy, not necessarily the most attuned to local needs, but one of the most common, has been to set a goal to provide broadband at a speed that matches that of leading broadband communities. While this strategy efficiently makes use of research by others on what constitutes sufficient broadband capacity, there are some drawbacks to this approach. Firstly, North American communities should recognize that to meet Japanese, South Korean, and European standards, they have a long way to go, and may have trouble doing so without a strong federal broadband policy analogous to that of these successful broadband countries (Turner 2005a). That is, municipalities, states, and even regions may have difficulty achieving high quality broadband for affordable rates without the help of national policy makers – though efforts to achieve this locally can create pressure for wide-spread changes in both broadband policy and the broadband industry, as is evidenced by the municipal broadband movement. Secondly, every user and every location do not need the same amount of bandwidth. Users' bandwidth requirements may differ from country to country, from community to community, and even within a community itself. Target bandwidth speed should take local users' needs into consideration.

In addition, while it may seem that the-higher-(the bandwidth)-the-better, setting bandwidth requirements too high may have the unintended effect of closing off the option for technologies, that, while not as fast as others, may provide a different set of benefits. For example, Vermont's governor proposed a plan to ensure all Vermonters at least 3 Mb/s of symmetric bandwidth by 2010 and at least 20 Mb/s symmetrically by 2013 (Gubbins 2007). Three Mb/s and even 20 Mb/s, while higher than the current FCC and ITU standards, are significantly lower speeds than proposed by other agencies and localities, and not high enough to support bandwidth-heavy applications such as HDTV. Nevertheless, the governor choose these figures because higher ones might have excluded wireless from consideration, a technology that may best meet the needs of Vermont's rural communities (Gubbins 2007), and that can, in most cases, be deployed more quickly than fiber.

A second approach to determining sufficient bandwidth levels is to set a bandwidth goal that matches users' anticipated needs. This approach may be more intensive in terms of the necessary investment in stakeholder analysis and other market research, but, in the end, it can pay off. For example, a network that will support interactive gaming, HDTV, and video file sharing has higher bandwidth requirements than one used primarily for text-based data transmission. If it is learned up-front that users will require a network that will support such visual and interactive data applications, it may become clear that investment in a robust fiber network, while more expensive, would be the most cost-effective investment.

A common approach, used both by municipal and commercial broadband projects to providing lower cost or free service is to offer lower bandwidth low-cost service, and higher bandwidth service for a (higher) fee – reasoning that, those who need a higher speed, more reliable connection will pay for it. This may be a good approach, as it theoretically lets users self-select their connection speed based on their needs. But, careful attention should be paid to the quality of the lowest-cost tier of service. This may be the only level of service available to low-income users, even though they may have just as high bandwidth needs as users purchasing high bandwidth subscriptions. To avoid exacerbating social differences, the speed for basic service should be such that it meets most users expectations. For instance, concerns have been raised over the free tier of service on the proposed Google/Earthlink San Francisco wireless network (Vos 2007a). Users of the free ad-supported service would have less privacy, and a guaranteed speed only marginally faster than dial-up, at 300 Kb/s. Furthermore, to use the free service residentially users would need to buy a device to bring the wireless signal indoors, typically costing $80 to $200, meaning that, despite a limited number of lower-fee paid service subscriptions, the network as a whole may do little to effectively meet San Francisco's goal of bridging the digital divide (San Francisco Budget Analyst 2007).

Assessing Network Quality

All broadband networks should meet, at minimum, the ITU and National Broadband Task Force (National Broadband Task Force 2001) standard for broadband, of bi-directional 1.5 Mb/s, recognizing that this figure is at the low end of bandwidth. Beyond this a network can be judged as high quality if it meets the needs *all* of its users in the present, especially those who are, for a variety of reasons, users of the lowest tier of available service. The network should also have a clear strategy showing how it will continue to meet user needs in the future. Therefore, part of determining appropriate network speed is to understand the needs of the users the network serves. This may be approached in a number of ways, including stakeholder surveys and focus groups, and an understanding of communication and technological trends that may influence bandwidth demand. With knowledge of local user needs, one network may reasonably settle for lower or higher bandwidth speeds than another given considerations of cost-effectiveness, desire to meet goals of ubiquitous and universal coverage, and to offer affordable service. Assessment for quality can be combined with an assessment of network ubiquity. See the section "Assessing Ubiquity" (p. 24).

HEALTHY – electromagnetic radiation emissions associated with network equipment shall be within known safe limits, and should be routinely monitored. Given that Wi-Fi power levels are relatively low and their placement in relation to human bodies is no more hazardous than existing sources of electro-magnetic radiation (e.g. mobile phones), there should be no additional concerns with wireless. However, the health risks of unusual situations, such as powerful transmitters in close proximity to the body, should be identified.

Health has not generally been an issue with internet access since concerns in the 1970s and 1980s around Video Terminal Displays (VDTs) (DeMatteo 1986), but wireless signals are now controversial. There is concern that the electro-magnetic radiation emitted by them may be harmful to humans. The issue has been taken up both by the scientific research community, and by the public. This section briefly summarizes the scientific and public debates, and gives guidelines for how a broadband network may best address wireless health issues.

The scientific debate on wireless and health has focused on whether electro-magnetic radiation has an affect on human bodies at a biological level, whether these signals may cause health effects, and at what level of signal emitted from wireless devices would be strong enough to be of concern. To date, research on electromagnetic radiation emissions has largely focused on the health effects of mobile phones and powerlines. It has also focused on the effect of emissions on specific populations, such as children, who are more vulnerable than adults (Wood 2006), and on electrosensitivity (Havas and Stetzer 2004; Havas 2006), a controversial disorder affecting people particularly sensitive to electromagnetic radiation.

The general consensus is that there is no significant scientific evidence that electromagnetic radiation emissions associated with wireless network equipment has a negative effect on human health (Jauchem 1993; Valberg 1997; Valberg, van Deventer et al. 2007). To gain a clearer understanding of the potential affects of wireless technology on health, more research is needed. Nevertheless, there is evidence that these emissions do have *some effect* on humans. Sage (2004) provides an overview of studies on radiofrequency and microwave radiation and various aspects of health, within a framework for how this evidence might guide legislation on the subject. Other concerns include the fact that there is no international consensus on exposure guidelines, which range by orders of magnitude in different countries, and that once mobile phone and wireless antennas are set up they are rarely monitored to ensure compliance to within the required ranges (Havas 2007). Given the current state of evidence on the subject, a prudent approach would be to follow standard precautionary principles governing situations where there may be unproven health risks (Adams 2002; Sage 2004), and to take regulatory actions to mitigate potential issues (International Commission for Electromagnetic Safety (ICEMS) 2006).

Despite the lack of convincing evidence that electromagnetic radiation emissions associated with wireless network equipment have a negative affect on human health, there continues to be public concern that they may. This is evident in the public debates that have erupted around events like the announcement of Lakehead University that it will not create a campus wireless network – as is common for universities – partly for health reasons (Gilbert 2007), or an article in the British newspaper, *The Independent*, raising concerns about the possible negative health affects of Wi-Fi, especially on children (Lean 2007). These, and similar news items, have sparked public questioning about the possible health effects of Wi-Fi. Interestingly, these news events seem to have also sparked public counter-responses dismissing these worries as unfounded (Betteridge 2007; Swider 2007). These public debates, and the rationales behind different participants' responses to the issue is an area in need of further investigation.

Assessing Health

Given the lack of compelling evidence that electromagnetic radiation emissions associated with wireless network equipment has a negative affect on human health, health concerns will likely not affect the placement or design of a wireless or wired broadband network. Nevertheless, erring on the side of caution, the results of new studies on the subject should continue to be monitored, and user concerns addressed. In the unlikely case that here is a high level of user concern about potential health effects of a network that cannot be mitigated through discussion and public education, this may be reason enough to opt for a wired rather than wireless network, or to avoid the use of wireless technology in sensitive areas, such as elementary schools.

A network that adequately addresses health is one that makes a commitment to address the health concerns of users, to monitor new scientific evidence on the relationship between electromagnetic radiation emissions and health, and that in the unlikely event that health concerns emerge is prepared to adapt the network accordingly.

COST EFFECTIVE
ACCOUNTABLE & RESPONSIVE

A broadband service in the public interest should be efficient and accountable. It must be **cost effective**, making wise operational decisions to offer stakeholders desired services for the lowest cost possible. This service must also be **accountable and responsive**, that is, it must take responsibility for service quality, availability, as well as other criteria and respond quickly to address service issues or wider systemic problems. Ideally, the design of the system itself helps to enable users to participate in ensuring accountability, enables community-responsive design, and facilitates quick response to issues identified. Cost-effectiveness and accountability are especially important for services that make use of new technologies, such as Wi-Fi, which may pose challenges as the technology and best practice operating principles evolve.

These factors have rarely been an explicit part of the public broadband debate, perhaps because they are implied characteristics of good public infrastructure. Nevertheless, not all networks are efficient and accountable. The following section shows how cost effectiveness and accountability are important to broadband networks, briefly discusses how these issues are relevant to public/private sector debates, and shows how broadband initiatives can be evaluated in terms of these characteristics.

COST EFFECTIVE – Independent of the pricing for affordability mentioned above, public infrastructures should make efficient and effective use of the resources they require to offer service. Wi-Fi makes very efficient use of a spectrum that historically has been regarded as having marginal utility and low value. Where wireless services can be built on top of existing physical, electrical and wireline communications infrastructures, the marginal costs can be kept relatively low. For instance, Toronto Hydro Telecom's One-Zone wireless internet efficiently leverages existing publicly-owned fibre backbones and street lighting in creating a high quality, city-wide service at a fraction of the cost of conventional alternatives.

A service is cost effective if it is economically worthwhile in terms of what is achieved for the amount of money spent (Encarta 1999). Broadband networks can vary widely in their architecture and the type and quality of service they are enabled to provide. At minimum, a consideration of network cost effectiveness should take into account the network's capital and operating expenses, the type of service offered (indoor, outdoor, business, residential, government, public safety, etc.), and levels of network reliability, quality, security and privacy.

Wireless: A Cost-Effective Technology?

Wireless broadband has the potential to be particularly cost effective. Wireless technology, because it operates on the open spectrum and because it can be faster and easier to deploy, can facilitate cost-effective coverage of large areas, including areas not cost-effective to serve by wireline technology. In fact, wireless technology has been a key driver of municipal broadband projects (Bar and Galperin 2004) and has helped to spur the growth of wireless internet service providers now offering service in areas previously un-served by broadband internet companies. Yet, while wireless systems may cost less upfront to deploy, they are not always the best, or most cost-effective solution in the long term. Like the City of Boston, which states that the city's wireless project is in reality a wireless *and* fiber project (Boston Wireless Task Force 2006), communities would do well to consider the trade-offs and synergies between wireless and wireline broadband technologies. This includes comparing technologies not only in terms of price, but also in terms of reliability, security, speed, and projected relevance in the future. Wise infrastructure investments are likely to include support for both wireless and wireline infrastructure (Oram 2007).

Looking Forward: A Cost-Effective Infrastructure Investment?

Both wireless and wired broadband networks may have a much wider infrastructural application than initially anticipated (Cisco 2006), meaning that investments in broadband networks promise to be increasingly cost-effective. An investment in a network that supports only one or two applications may not be cost effective, but if the same investment yields an infrastructure that supports many services, this can be a wise spending decision. For example, Corpus Christi, TX uses a wireless network, initially built for automatic meter reading, for a wide range of public safety and communications applications (Corpus Christi 2007). As additional broadband networks are built and applications developed for them, to what extent they may support multiple services will become more apparent (International Telecommunication Union 2005; International Telecommunication Union 2006).

Public vs. Private Cost-Effectiveness

Ideas about cost-effectiveness have played a prominent role in the debate about whether the public sector or the private sector is better equipped to build and offer broadband service. Advocates for private sector broadband service have argued that municipal initiatives are less likely to be cost-effective than private ones because they are not subject to the same market pressures that encourage efficient operation. Studies of existing projects show that, contrary to this belief municipalities do successfully and cost-effectively run both broadband networks and other utilities (Gillett, Lehr et al. 2003; Daggett 2007a). In addition, some have argued that municipal broadband networks are unwise because if the proposed municipal networks could be provided cost-effectively, they would already be provided by the private sector (Baller 2005). Yet, likely partly as a result of market pressure from municipal projects, private companies are now entering the municipal wireless market more enthusiastically (Perkowski 2007). These public/private debates are relevant to determining what business and ownership models are most cost-effective, but further discussion of them belongs elsewhere.

Assessing Network Cost-Effectiveness

A cost-effective network is one that is economically worthwhile in terms of what is achieved for the amount of money spent. Cost effectiveness of broadband networks can be evaluated in a number of ways.

Firstly, cost-effectiveness can be assessed through a consideration of whether the funds used to build the network were efficiently used, and whether the business plan for future operations continues to be structured cost-effectively. That is, compared to similar networks, does the network in question make more or less efficient use of funds? How does the business plan compare to that of networks that offer similar service in similar environments – for what amount, and by what financial strategies does the network propose to offer service? In general, how good have (wireless, fiber, public, private, public/private, etc.) broadband providers, been at anticipating their costs and revenues? How accurate are this project's projections likely to be? See San Francisco Budget Analyst (2007) and Zhang and Wolff (2004) for costing methods for urban and rural broadband networks.

Cost-effectiveness can also be evaluated in terms of efficient use of existing resources. Does the network make use of existing infrastructure, such as light poles or sewer systems? Does the network make use of previously unused spectrum? Does the network compete with or add to existing broadband services? If it competes with existing services, what is the outcome of this competition for users?

Finally, while calculating cost-effectiveness may seem number-based, a judgment about cost-effectiveness is always, in part, qualitative. Whether a network is cost-effective depends on an assessment of what is needed by and valuable to the community in question. For example, investing a greater amount of capital to build a broadband network with a higher level of reliability may or may not be considered by its stakeholders a worthwhile expenditure, based on their needs. For instance, Fredericton, New Brunswick's best effort wireless network built from excess bandwidth on the city's fiber network (e-Novations 2005) could be considered cost effective because of its efficient use of resources. Because the network is often slow, and does not have guaranteed quality of service, it could also be considered, by some, unusable, and an ineffective use of resources. Therefore, an assessment of cost-effectiveness is in part based on the particular context and stakeholders: Was a stakeholder analysis conducted? How do the services the network offers compare to stakeholder needs, are they under- or over- met?

ACCOUNTABLE & RESPONSIVE – mechanisms of governance and citizen oversight and control to ensure that the service and its operator are responsive to citizen input and needs on issues ranging from network repairs to new service innovation. Wireless access can help expand the modes of citizen involvement and oversight.

Issues of accountability and responsiveness have not been prominent in the public broadband debate, perhaps because they are assumed to be characteristics of good infrastructure. Nevertheless, accountability and responsiveness are especially important in cases where new technologies, like Wi-Fi, are used, and when various ownership models (public/private, etc.) are possible, as different ownership models can affect how accountable a network is to users.

Existing Practices: Approaches to Service Issues

Approaches that have emerged to respond to technical and customer service issues are a part of attending to accountability and responsiveness in broadband networks. These approaches range from the best-effort approaches of ad-supported or other free networks, to traditional internet service provider (ISP) customer service models. In cases where municipalities themselves have taken on customer service responsibilities, some report difficulties, such as keeping up with technical challenges or addressing the volume of customer support needed. These issues have led some communities, in an effort to provide highly responsive service to users, to turn customer service and network management over to the private sector (see, for example, the cases of Corpus Christi, TX (Fleishman 2007a) and Chaska, MN (Communications News 2006)). Other communities, for example, those whose broadband projects have grown out of existing municipal electric utilities (Gillett, Lehr et al. 2006), have met the new service challenges of broadband. How various customer service models for broadband networks – either existing or proposed – look from a public interest perspective is an area that would benefit from further investigation. More widely, models should be identified that incorporate accountability and responsiveness into the network's governance and technical structure.

A Role for Government?

Municipalities acting on behalf of (actual or perceived) citizen demand for better broadband have driven the municipal broadband movement. Likewise, local government may have a role in ensuring that networks, once built, are accountable and responsive to users. Public involvement in network accountability, whether through direct participation or through legislation, can help ensure that users get good coverage and service at fair prices. This oversight can also help to ensure that relevant information about network operations is transparent so that users can judge cost-effectiveness and network quality for themselves. For example, when a municipality is the initiator of a broadband project they can require "proof-of-concept" areas before approving final deployment, and service level agreements or independent quality of service tests (such as those provided by Novarum or VeriWave) to authorize continued operation. For instance, Philadelphia has used both service level agreements and proof-of-concept tests to ensure that its private partner, Earthlink, fulfills the network requirements (Wireless Philadelphia 2005; Wireless Philadelphia 2007c). In any case, communities should take care to evaluate how proposed broadband network models differ in terms of accountability to the community, responsiveness to community needs, and governance mechanisms for ensuring this oversight.

Assessing Network Accountability & Responsiveness

Accountability of a planned or operational network can be assessed through an evaluation of the presence or absence of accountability structures – such as transparency requirements and a clear governance model. Does the network have a clear governance structure? What parties are involved in the network, and who is responsible for what? Responsiveness can be assessed in terms of network customer service policies, including factors like number of staff, response times, and service guarantees. That is, what is the network's stated approach to addressing technical and customer service issues? And, also, what paths are available for user input to network design?

An operational network can also be assessed by how well, in practice, it has taken responsibility for service and wider systemic issues. What do users have to say about the network? How quickly and conclusively have technical and customer issues been addressed? Has user feedback been incorporated into the network? A simple test of this is to approach the system from the perspective of a user: is the service straightforward to use? If not, is it clear how to get help? How quickly, in what manner, and by who is the issue addressed? How are requests for new application areas handled?

SECURE
PRIVACY ENABLING
OPEN
NEUTRAL & NON-DISCRIMINATORY

Broadband networks must address the complex balance between ensuring both openness and security. This balance helps to foster future-ready networks – networks that can adjust to changes in technology, applications, content and services, and that anticipate challenges to security and privacy as electronic data and mobile devices increasingly become part of daily life. In particular, a broadband network in the public interest should be both **secure** and **privacy enabling.** It should also be **open** and **neutral & non-discriminatory**. These characteristics are further defined and discussed in this section, as well as how each one has played a role in public broadband debates. The standards that a network that does well in terms of these areas should meet are also discussed.

SECURE – state of the art technology and best practices should be adopted to ensure that personal communication and internet browsing are secure against unwarranted interception. Non-intrusive means should be incorporated into the service to protect users against spam, viruses, spyware, etc. Reasonable, lawful means should be adopted to protect users against illegal content (e.g. child pornography, hate speech). As an over-the-air service, wireless is more susceptible to interception and corruption than more physically secure wireline transmission. However, commonly available encryption and authentication techniques are currently adequate if implemented properly.

Broadband networks are subject to a number of potential security breaches, ranging from unintended use of the network, to data collection on network users, to malicious attacks (AirDefense 2002-2005a; Fleishman 2007b). Threats to wired and wireless networks differ, as well as methods for securing the networks (Potter 2006). Generally, wireless networks are less secure, and if unsecured can pose a threat to the security of the wired networks they connect to, as these wired networks can be accessed through the wireless network. A range of strategies can be used to secure a network, based on the network type, and the level of security needed. The more sensitive the data passing over the network, and the higher the risk of a security breach, the higher security should be. See Karagiannis (2003) and Linksys (2007) for a basic introduction to wireless security, and Cisco (2007) for an example of outdoor wireless security best practices and technical specifications. In general, to secure a network: all devices that attach to the network should be secured; all users of the network should be educated about the security measures they must take on an individual level; and the network should be actively monitored for weaknesses and breaches (AirDefense 2002-2005b).

While security issues have not been widely discussed in relation to public broadband networks, some questions about it have been raised. Security is more difficult to obtain over wireless networks in part because of their ad-hoc growth pattern – for example, the “lilypad” (Negroponte 2002) networks that have emerged in urban centers as a result of individuals broadcasting open Wi-Fi signals from their hotspots. These ad hoc networks may not be exactly public, in that this not necessarily is their intended use. But, they are, nevertheless open to the public, and pose potential security issues to users. In addition, while growth in Wi-Fi has been rapid, security has not kept pace. For example, in New York, London and Paris the number of Wi-Fi access points have recently risen 49%, 44% and 160% respectively. Yet, encryption was found to be up but only by 6% in London and less than 2% in both New York and Paris (Griffith 2007). In the case of ad hoc public networks, it may be, for now, up to users to ensure their own security, with the safest option being not to use the networks at all (Potter 2006).

Despite potential concerns, wireless networks can be well-secured, especially if they are managed, rather than ad hoc. And, an initial analysis of large-scale municipal wireless networks' security policies seems to indicate that they are, in fact, addressing security issues wisely (Fleishman 2007b). Municipalities can play an important role in ensuring security on city networks by stipulating security standards in the RFP process. For example, support for state-of-the-art, multi-layer security standards was an upfront requirement for potential bidders on San Francisco's wireless network (City and County of San Francisco 2005: 13).

While a basic level of security is prudent for any wireless network, one set of security guidelines does not fit all cases. Security can make a network more difficult for users to use, and even infringe on user privacy. For example, to access the Toronto Hydro OneZone wireless network users must have a credit card, which they use to set up their account (Toronto Hydro One Zone 2007). This links accounts to individuals, and because a login is required for every use, individual activities on the network are potentially traceable, as well as users' physical locations. These identity requirements may be for security purposes, such as to be able to track users engaging in activities such as sharing child pornography. While concern over network use for illegal purposes is valid, other wireless networks have not found such measures necessary. For instance, users of Fredericton, NB's Fred eZone, a free, best-effort city wireless network, are not required to logon, nor are their activities monitored (Longford 2006). Each locality must decide, based on the local context, what level of security is appropriate, and what trade-offs may be acceptable between security and user privacy and network accessibility.

Assessing Network Security

Network security can be measured through technical security tests. Security testing may be required as part of the "proof-of-concept" phase, and should be a part of routine network monitoring. In addition, the network's stated security policy, standards, and monitoring policy should be assessed: Does the network have a security policy, standards, and monitoring policy? How does it compare to that of similar networks? How secure is the network, and what is the rationale behind this level of security? Were stakeholder and risk analyses conducted to inform this decision? What role does the network provider have in ensuring security? What roles and responsibilities do users have? And, finally, do network security measures impose on user privacy, network openness, or neutrality? Are these trade-offs reasonable given the purpose of the network and the risks at hand?

PRIVACY ENABLING – operation of the service shall be fully compliant with applicable privacy laws and best practices. No personally identifying information shall be collected beyond that which is necessary to ensure access to and operation of the network. The service should enable both pseudonymous and anonymous use. Location-based and other services requiring additional personal information may be offered on a strictly voluntary, opt-in basis. As with Security above, wireless internet presents inherent difficulties beyond those already problematic with the wired internet. However, the content of messages (if not traffic patterns) can be protected technically. Some legal and legislative changes may be necessary to deal with the ambiguity of 'personal' communication via 'public' airwaves' and detectable in 'public spaces'.

Broadband networks in the public interest should protect user privacy. This is especially important in the context of wireless networks, because, as access becomes mobile, not only a user's electronic privacy, but also their locational privacy is at risk. That is, wireless technology makes it possible to track both what a user is doing and where the user is. The privacy precedents we set now are important for a future where identification and location tracking devices and infrastructures (including GPS, RFID, Wi-Fi) are increasingly commonplace. This section briefly introduces electronic and mobile privacy issues. It then discusses some problems with the way that privacy issues have been dealt with in public wireless projects, particularly ad-based network models, and suggests guidelines for network privacy standards.

Electronic and Mobile Privacy Concerns

There are a wide range of electronic and mobile privacy issues, including issues that may emerge as more of the devices we use in daily life connect to the internet, and as the internet becomes an increasingly important space for communication and commerce. Electronic privacy issues include things such as monitoring of e-mail and document content, and tracking of online behavior, such as websites visited (for a full range of issues and related legislation see www.epic.org). This data may be used for security measures, for example, information collected under the U.S. Communications Assistance Law Enforcement Act (Electronic Frontier Foundation 2007; Federal Communications Commission 2007), to target online advertising, or conduct other forms of market research. It may also be used for vicious purposes such as cyberstalking, real-world stalking, and video-voyeurism (EPIC 2007).

Mobile privacy issues stem from the ability of new mobile technologies to pinpoint coordinates continuously, and in real-time. This means that people using devices such as a Wi-Fi enabled laptop or a mobile phone could have their location and travels traced anytime or all the time. In addition, the record of all these travels and habits could be stored and even shared between parties for significant lengths of time (Bennett and Crowe 2005; International Telecommunication Union 2005; Lyon, Marmura et al. 2005). While a broadband network cannot protect users from all electronic and mobile privacy issues, it can help to do so by setting network privacy standards, such as those described below. Further electronic and mobile privacy protection can be addressed through innovations in interface access (Laurie 2007; Seltzer 2007), and through privacy legislation (Hoofnagle 2005).

Privacy and Municipal Networks

In terms of public wireless projects, San Francisco's wireless project has received the most visible attention regarding privacy, though similar concerns could be raised about other projects. The public debate about privacy on the proposed San Francisco citywide wireless network to be operated by Earthlink and Google is due in a large part to the actions of a trio of privacy advocates, the ACLU of Northern California, the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC). During the RFP stage of the project, this group submitted a series of letters to San Francisco TechConnect analyzing the proposed privacy policies of bidders on the network (EPIC 2006), as well as the city's privacy requirements for potential network operators (ACLU of Northern California 2005). The purpose of these letters was to encourage the city to carefully evaluate proposals in terms of their implications for users' privacy, and to urge the city to set stricter privacy requirements for all potential bidders.

Ultimately San Francisco chose Earthlink and Google's joint proposal, which measured poorly – along with some, but not all, of the other bids – on privacy (EPIC 2006). Clearly, the Earthlink/Google proposal was chosen because it met a number of desirable criteria for the city, including a commitment by Earthlink and Google to finance the wireless infrastructure, and the guarantee of a basic level of free service (though a slow, and not very private one) for all city residents. San Francisco could have played a better role in enhancing user privacy by requiring higher privacy standards of all bidders, as well as of Earthlink/Google after their initial proposal had been selected – now more difficult as negotiations have been completed, or by choosing a proposal upfront that measured better on the level of privacy it ensured users. Stricter privacy requirements on the part of the city may have eliminated the initial Earthlink/Google proposal, as Google's business model to provide free service, like other ad-based services, is premised on access to user data (Chester 2006; San Francisco Chronicle 2006). But, in the end, stricter privacy requirements may have stimulated the partnership and other bidders to submit proposals for networks that better protected user privacy.

Greg Richardson (2007) of Civitium, the well-known municipal wireless consultancy that helped broker the San Francisco Earthlink/Google deal, says that the privacy concerns of privacy advocates go too far; they could derail an important project that was difficult to negotiate, and delay ubiquitous Wi-Fi for San Francisco. His argument is worth considering. He argues that Earthlink should not be bound by a set of regulations that do not apply to other San Francisco broadband providers – whose privacy policies don't come close to meeting the privacy gold standard proposed by the ACLU, EPIC and EFF (ACLU of Northern California 2006). Richardson also argues that consumers can judge the acceptability of privacy policies for themselves – something that is possible, but given the complexity of privacy law and the obscurity of information handling practices, is very difficult to do. In addition, Richardson says, privacy advocates would be better off fighting such battles at a federal or state legislative level, working for standards that would apply to *all* providers, rather than fighting for them on a case by case basis.

While, as Richardson argues, individual municipal wireless projects should not be expected to make up for all the telecommunications policy shortcomings in the U.S. (and elsewhere), they can help to shift things in the right direction by setting a good example, and putting pressure on legislators. In this way privacy advocates' focus on the San Francisco project is well aimed; while they may not make a difference in this project, the its high media profile has helped to bring needed attention to privacy issues on broadband networks.

While it may seem that users are unconcerned about their electronic and mobile privacy (Vos 2007b), part of this lack of concern may be due to an acceptance of the status quo, one where users don't necessarily bother to read the many service agreements they encounter. Users may be skeptical that their privacy is protected, but decide that using the service is worth the risk since there may be few alternatives. One role that the public sector, together with privacy advocates, might play is to educate users on the difference between privacy policies. Not all policies are the same. While, ultimately, price or other service attributes, may remain a more important decision factor for the majority of users on which broadband network they choose, users should have the option to opt for a network that meets high privacy standards.

We believe, that to the extent possible, public broadband should meet the ALCU, EPIC and EFF model minimum standards for electronic privacy (ACLU of Northern California 2006). Network builders should carefully consider the trade-offs between privacy, and other network attributes, such as cost and security. We recognize that this standard is significantly higher than the status quo for user privacy. Each network built to this standard can help to change that.

Assessing Network Privacy

Network privacy can be assessed through an analysis of the network privacy policy, including how clearly and openly information about privacy practices is communicated to users. In the case of a public-private sector partnership where the private partner runs the network by mandate of the community or municipality the contract between the parties should also be evaluated in terms of how it addresses privacy. That is, are specific privacy standards stipulated? What are they? Both documents can be assessed in terms of the ACLU, EPIC & ECC model minimum standard for electronic privacy (ACLU of Northern California 2006). Areas of concern include:

- What personal information is collected about users?
- How is this information used?
- How long is this information stored?
- With whom is this information shared?
- Is this information commercialized in any way?
- Is this information correlated to a specific user, device or location?
- Are mechanisms available to allow users to opt in or opt out of any service that collects, stores, or profiles information on the searches performed, websites visited, e-mails sent, or any other use of the Network?
- Are mechanisms available to allow users to opt in or opt out of any service that tracks information about the user's physical location?
- Are users enumerated or assigned any unique number that can be used to track them from session to session?
- Are policies in place to respond to legal demands for users' personal information in accordance with applicable laws?
- Are users allowed access to all information collected about them?
- Are users provided with a mechanism to review this information and to correct inaccuracies or delete information?

Network privacy policies will measure up in different ways to this standard – ranging from meeting the standard well, to those that include some questionable practices, and those that rate poorly. In the case that the policy does not meet the standard well, it should be examined in the larger context of the network business model. What are the reasons for these (low) privacy standards? What might network owners and/or operators gain from the ability to gather, or share user information? Would the network business model continue to be viable if measures were taken to better protect user privacy?

Would this put the network at a competitive disadvantage? Is user privacy an acceptable trade-off to being able to offer a service that, otherwise, is in the public interest?

OPEN – the service should be designed to maximize openness at various levels (e.g. openness to a variety of access devices, the use of open source software, and all kinds of content, applications and services.) Unlike in wireless telephony, the key standards and regulations for Wi-Fi communication, notably the 802.11 family, are oriented to openness, not competition among rival incumbents, and sufficiently stable to support the development of an expanding range of interoperable devices and applications (Noam 2001).

Open network models are advocated by an increasing number of stakeholders, including from the consumer perspective (The OPLAN Foundation; Broadband Working Group and Cambridge University Communications Research Network 2006), by municipalities (Citynet Amsterdam; Utah Telecommunication Open Infrastructure Agency 2003; Boston Wireless Task Force 2006; Chew 2006), policymakers (van Winden and Woets 2004; Chew 2006), and even the private sector (Feld 2007; Sacca 2007). In general, an open network can be defined as a network that meets the criteria of the INEC Declaration on Open Networks (International Network of e-Communities (INEC) 2006). Such a network gives users a great deal of freedom in terms of choosing service providers and services, content, and devices. Overall, openness is an essential element in future-oriented network design. Like roads, broadband infrastructure should be built to accommodate, within reason, all forms of traffic. Openness helps to ensure that a network will be widely useful and ready for future developments in technology and use practices.

This section shows where the open access, network neutrality, and municipal wireless movements converge around issues of openness. It further describes open access, discusses openness and network ownership models, and the relationship between openness and competition in the broadband market. Finally, it describes how a network can be assessed in terms of openness.

Open Access and Network Neutrality

Open access and network neutrality are related, but typically have a slightly different focus. Network neutrality and open access are both policies designed to preserve openness on the Internet. In general, open access calls for the openness of attachment facilities, conduits, cable, DSL, fiber, etc. to multiple service providers on an equal basis, meaning that many providers – not just the owner of the network infrastructure – have the opportunity to offer service over it. In turn, network neutrality mandates openness to content and services provided to users over the network, meaning that a provider should not limit user access to content and services. This said, the distinction between open access and network neutrality is not always clear, and the definitions of both terms vary (Hogendorn 2007). Open access policies sometimes cover a wider range of issues, encompassing concerns of both open access and network neutrality. For instance, in its letter on open access to the FCC regarding the 700 MHz spectrum auction, Google advocates for four types of openness: open applications, open devices, open services, and open networks (Sacca 2007). In any case, together, open access and network neutrality cover the spectrum of openness issues facing broadband networks.

Openness, Competition, and the Public and Private Sectors

In terms of ensuring openness and competition it is not so important who owns a network (though this is not irrelevant), but rather, how the network is structured. Open networks, which can be publicly or privately owned, foster competition, which ultimately leads to lower prices and better services for users (The OPLAN Foundation; Consumer Federation of America 2002; Boston Wireless Task Force 2006). In the municipal wireless movement this model is often referred to as a cooperative wholesale model (The Wireless Philadelphia Executive Committee 2005).

The public sector can play a role in ensuring open networks in a number of ways. For example, the public sector can help create an open network through ownership of basic network infrastructure, which the public body then offers service providers (whether public, private, or non-profit) access to on a wholesale basis. Policy conditions are more favorable for this model in the European Union (van Winden and Woets 2004; Chew 2006), but examples also exist in North America.

The UTOPIA Community MetroNet, a fiber network, is an operational example of an open access network in the United States. The network is owned by a collective of municipalities in Utah, who sell access to the network at wholesale rates to companies, who then provide service to users. Currently a number of providers offer service to users over the network, including AT&T, MSTAR, Sisna, Veracity, and Xmission. Incumbent broadband providers, such as AT&T may not favor open networks, because they mean the provider potentially faces more competition, but cases like UTOPIA indicate that when open networks exist, they will participate. In fact, AT&T offers the same basic service over the UTOPIA network that it does elsewhere, for a lower price (Meinrath 2006). A key to UTOPIA's success may be its scale, since, although there are more competitors in the market, AT&T can reach many potential customers through the UTOPIA network, which currently services 14 cities.

The public sector may also play a role in ensuring open networks through policymaking. For example, by legislating that private carriers open their networks to competitors at a wholesale rate. Such legislation in the U.S. at a federal level helped to fuel the growth of wireline ISPs. This increased competition in the ISP market, and ultimately led to better and cheaper (dial-up) internet service for users (Cooper 2004). No similar legislation applies to the broadband market in the US, meaning a limited number of telephone and cable companies currently control the vast majority of broadband service, with little incentive to relinquish their market dominance (Turner 2005a). As of 2002 there was a significant difference between the broadband and narrowband markets: cable and telephone companies had only about 5 percent of the narrowband market, where they have to compete. Conversely, a few companies had captured about 95 percent of the broadband market, where they leverage control of their wires (Consumer Federation of America 2002).

Assessing Openness

In general, assessing openness involves assessing whether multiple service providers may operate on the network, and whether they have equal access to it. Areas of inquiry include: Who owns the network? Who decides what providers can operate on the network? Can any service provider (large, small, incumbent, new, public, private, non-profit) offer service over the network? Can the network accommodate multiple types of service offerings? Does the network favor one type of service over another? Boston's proposed citywide network is a good example of a network that takes both openness and neutrality into consideration in its architecture (Boston Wireless Task Force 2006).

In particular, we believe that networks should follow the basic principles for openness defined in the INEC Declaration on Open Networks (International Network of e-Communities (INEC) 2006), which include the basic issues outline above. Both the network's official policies in terms of openness, and how these policies function in practice should be evaluated. Assessment of network openness overlaps with an assessment of network neutrality & non-discrimination (below).

NEUTRAL & NON-DISCRIMINATORY - no restrictions on access to lawful content/services, and no discrimination on the basis of the source, destination, and ownership content or services (e.g. P2P networks) beyond what is necessary for efficient network operations (Sandvig 2006). The early stage of the establishment of wireless infrastructures provides an opportunity to ensure that network neutrality principles are embedded in them. These wireless networks may provide an alternative to non-neutral wireline networks, and encourage the wider adoption of neutral and non-discriminatory network principles.

This section introduces the network neutrality debate, shows how its concerns intersect with the municipal wireless movement, and discusses how networks can be evaluated in terms of neutrality.

Although the precise meaning of network neutrality is contested, it is generally defined as the principle that all traffic on the public internet be treated equally and without discrimination, regardless of source, ownership, or destination. Advocates of network neutrality argue that this will help to promote the most useful public information network. In practical terms, network neutrality means that ISPs should not influence the content a user sees or the applications they use. That means, all websites will load the same, and users are free to go to sites of their choosing (Wu 2005; CRACIN 2007; Longford 2007a).

The network neutrality debate began in the United States in 2005, following the announcement of major ISPs that they intended to charge content providers a premium to deliver their content faster than their competitors. This type of action was made possible by a change in policy earlier in 2005. It has since been taken up in other countries. A number of non-neutral actions on the part of ISPs have already taken place, for instance, the blocking of pro-union site, and other sites on the same server, by Telus during a labor dispute in Canada (Longford 2007b). Network neutrality can be addressed on a regulatory level. For example, the FCC recently released rules for the auction of the 700 MHz spectrum in the U.S., which include requirements for bidders to allow open devices and open applications (but not open networks and open content) (Freepress.net 2007).

It should be noted that other types of discriminatory practices on the internet have already been occurring for some time (Longford 2007a), and some of them are in the public interest. For example, an ISP may use filtering mechanisms to block spam, and engage in traffic shaping in an effort to enable best overall quality of service. These actions are different from those that use discrimination on content and services to help ISPs increase profits, which now seem to be emerging.

While addressing neutrality through regulation may be the most efficient mechanism for ensuring neutrality and non-discrimination, individual networks also make a difference. For instance, municipal networks – which could guarantee neutral practices – may become increasingly seen as a way to ensure network neutrality. This, in turn, could add more fuel to the municipal broadband movement (Gubbins 2006). At the very least, the presence of basic broadband infrastructure that is open and neutral (such as that proposed by the Boston Wireless Task Force (2006) can help ensure that users have a choice between different content providers' services, so that if one provider discriminates on content or in any other way, the user can choose a different service.

Assessing Neutrality & Non-Discrimination

To assess the level to which a network is neutral and non-discriminatory both official network policy on access to content and services, and the network's structure – e.g. who owns the network and who is allowed to operate on it – can be examined: Are there any restrictions on access to content/services? If so, what is the justification for this? (For example: blocked content is illegal; the network will function most efficiently with prioritization of particular types of content; controlled access to content and services is a key part of the operator's business plan, etc..) Are these restrictions in the best interest of users? Assessment of network neutrality & non-discrimination overlaps with an assessment of network openness (above).

CONCLUSION

In summary, we have argued that broadband networks should be: Ubiquitous & Universal, Widely Useful, Usable, Accessible, Affordable, Reliable, High Quality, Healthy, Cost-Effective, Accountable & Responsive, Secure, Privacy Enabling, Open, and Neutral & Non-Discriminatory. We believe that this tool, a desiderata for broadband in the public interest, can play a valuable role now – a time when broadband infrastructure is being shaped. As a key infrastructure for citizen economic, social, and civic participation it matters over the long term how these networks are being designed, built, and managed. We hope that the criteria articulated in this paper will give guidance to this development process and may help to shift the debate away from whether the public or private sector is better suited to own and operate these networks, to what network characteristics, regardless of public/private involvement, are in the best interest of users.

PART III – RESOURCES

REFERENCES

ACLU of Northern California (2005). Joint Letter on San Francisco Wireless Internet Access.

ACLU of Northern California (2006). Coalition Letter on San Francisco Municipal Broadband.

Adams, M. (2002). "The Precautionary Principle and the Rhetoric Behind It." Journal of Risk Research 5(4): 301-316.

AirDefense (2002-2005a). Wireless LAN Security: What Hackers Know That You Don't AirDefense, Inc.

AirDefense (2002-2005b). Three Steps for Bullet-proof Wireless LAN Security & Management, AirDefense, Inc.

Baker, P. and A. Bell (2007). Accessibility in Municipal Wireless Networks: System Implementation, Policy, and Potential Barriers for People with Disabilities. Prepared for the ICA Pre-conference Workshop "Mobile Communication: Bringing Us Together or Tearing Us Apart?" 57th Annual Conference of the International Communication Association. San Francisco, California.

Bakowski, A. (2005). Municipal Telecommunications Policy: A Guide to New Technologies. The Municipal Advanced Telecommunication Infrastructure Project (MuniTIP) CACP Policy Report.

Baller, J. (2005). Deceptive Myths About Municipal Ownership. Broadband Properties Magazine.

Baller, J. and C. Lide (2006). The Case For Public Fiber-to-the-User Systems, Baller Herbst Law Group.

Banerjee, A. and M. Sirbu (2005). Towards Technologically and Competitively Neutral Fiber to the Home (FTTH) Infrastructure. Broadband Services: Business Models and Technologies for Community Networks. I. Chlamtac, A. Gumaste and C. Czabo. New Jersey, John Wiley.

Bar, F. and H. Galperin (2004). "Building the Wireless Internet Infrastructure: From Cordless Ethernet Archipelagos to Wireless Grids." Communication & Strategies 54(2): 45-68.

Bar, F. and H. Galperin (2004). Building Wireless Infrastructure: Alternative Models. International Workshop on Wireless Communication Policies and Prospects: A Global Perspective, USC.

Bar, F. and N. Park (2005). Municipal Wi-Fi Networks: The Goals, Practices, and Policy Implications of the US Case. First Transatlantic Telecom Industry Forum. IDATE, Montpellier.

Bar, F. and N. Park (2006). "Municipal Wi-Fi Networks: The Goals, Practices, and Policy Implications of the U.S. Case " Communication & Strategies 61(Q1 2006): 107-125.

Bauer, J. (2003). A comparative analysis of spectrum management regimes. Telecommunications Policy and Research Conference. Arlington, VA.

Beachboard, J. C., C. R. McClure, et al. (1997). "A critique of federal telecommunications policy initiatives relating to universal service and open access to the national information infrastructure." Government Information Quarterly 14(1): 11-26.

BelAir Networks (2007) "BelAir Networks First To Guarantee Performance and Coverage in Municipal Wireless Networks."
Belson, K. (2006). What if They Built an Urban Wireless Network and Hardly Anyone Used It? New York Times. New York.
Benjamin, S. (2003). "Spectrum abundance and the choice between private and public control." New York University Law Review 78: 2007-2102.
Bennett, C. J. and L. Crowe (2005). Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada, University of Victoria for the Office of the Privacy Commissioner of Canada's (OPC) Contributions Program.
Berquist, L. and A. E. Grant (1999). The Emerging Municipal Information Infrastructure: The Austin Experience. The First 100 Feet D. Hurley and J. H. Keller. Cambridge, MA, MIT Press: 173-193.
Best, M. L. (2006). A Global Survey of Spectrum License Exemptions. The 34th Research Conference on Communication, Information and Internet Policy, Telecommunications Policy Research Conference (TPRC). Arlington, VA.
Betteridge, I. (2007) "No, Wi-Fi isn't “a health time bomb”." Technovia.
Bleha, T. (2005). "Down to the Wire." Foreign Affairs(May/June 2005).
Boston Wireless Task Force (2006). Wireless in Boston. Boston.
Broadband Working Group and Cambridge University Communications Research Network (2006). Vision of Personal Broadband White Papers, MIT Communications Futures Program (CFP)
Buck, S. (2002). "Replacing spectrum auction with a Spectrum commons. ." Stanford Technology Law Review 2.
Cherry, S. (2006). "A Broadband Utopia." IEEE Spectrum(May 2006): 3.
Chester, J. (2006). Google's Wi-Fi Privacy Ploy. The Nation.
Chew, D. (2006). CityNet Amsterdam: Fibre-to-the-home is becoming a reality, ING Wholesale Banking.
Cho, H. (2006). Explorations in Community and Civic Bandwidth: A Case Study in Community Wireless Networking. Communication and Culture. Toronto, York University. MA.
Cisco (2006). Evolution of Municipal Wireless Networks. White Paper.
Cisco (2007). Best Practices for Outdoor Wireless Security. White Paper.
City and County of San Francisco (2005). Request for Proposals: TechConnect Community Wireless Broadband Network San Francisco.
Citynet Amsterdam.
Clement, A. and L. R. Shade (2000). The Access Rainbow: Conceptualizing Universal Access to the Information/Communication Infrastructure. . Community Informatics: Enabling Communities with Information and Communications Technologies M. Gurstein. Hershey, PA, Idea Group: 32-51.
Cohen, S. M. and C. S. Golvin (2007). Free Muni Wireless Noses Into The Broadband Market: Ad-Supported Muni Wireless Will Find Its Niche With Consumers Trends, Forrester Research.
Communications News (2006) "Chaska turns Wi-Fi over to MSP." Communications News.
Consumer Federation of America (2002). The Importance of ISPs in the Growth of the Commercial Internet, Consumer Federation of America.
Cooper, M. (2004). The Public Interest in Open Communications Networks, Consumer Federation of America.
Cooper, M. (2006). Achieving Dynamic Spectrum Allocation: Governance Rules for a Mixed Private-Commons Regime. The 34th Research Conference on

Communication, Information and Internet Policy, Telecommunications Policy Research Conference (TPRC). Arlington, VA.
Corpus Christi (2007). Corpus Christi Wireless Applications.
CRACIN (2007). What is Net Neutrality? , Canadian Research Alliance for Community Innovation and Networking.
Daggett, B. V. (2006). Is Publicly Owned Information Infrastructure a Wise Public Investment for San Francisco? Institute for Local Self-Reliance & Media Alliance
Daggett, B. V. (2007a). Localizing the Internet: Five Ways Public Ownership Solves the U.S. Broadband Problem Institute for Local Self-Reliance
Daggett, B. V. (2007b) "What About the Word "Public" Is So Hard to Understand?" newrules.org.
Daggett, B. V. (2007c). An Alternative to San Francisco's Wi-Fi Deal. SFPO Dispatch.
Daily Wireless (2007). Municipal Wireless Buyers Guide: Everything you need to know to get started with municipal, metro or mesh WiFi.
DeMatteo, B. (1986). Terminal Shock: The Health Hazards of Video Display Terminals. Toronto, NC Press Limited.
Dowding, M. a. C., A. (2001). National Information Infrastructure Development in Canada and the U.S.: Redefining Universal Access and Universal Service in the Age of Techno-Economic Convergence. . Telecommunications Policy Research Conference.
Dutton, W. H., S. E. Gillett, et al. (2003). Broadband Internet: The Power to Reconfigure Access. Oxford, Oxford Internet Institute.
Dutton, W. H., S. E. Gillett, et al. (2004). "Bridging broadband internet divides: Reconfiguring access to enhance communicative power." Journal of Information Technology 19(1): 28-38.
e-Novations (2005). The Chronicles of e-Novation and Fred e-Zone. Fredericton.
Electronic Frontier Foundation (2007). Communications Assistance for Law Enforcement Act (CALEA): The Perils of Wiretapping the Internet.
Ellig, J. (2006). A Dynamic Perspective on Government Broadband Initiatives Policy Study No. 349 & Policy Summary of Policy Study No. 349, Reason Foundation.
Ellison, C. (2007a) "Becca Vargo Daggett on the Definition of "Public Broadband"." Muniwireless.co.:
Ellison, C. (2007b) "Richardson Blasts San Francisco's Ideological Divide." Muniwireless.com.
Encarta (1999). Encarta® World English Dictionary M. Corporation, Bloomsbury Publishing.
EPIC (2006). A Privacy Analysis of the Six Proposals for San Francisco Municipal Broadband, EPIC.
EPIC (2007). Gender and Electronic Privacy. E. I. P. Center.
Excelsio Communications (2007). Municipal Wireless RFP Evaluation: Practical Pointers.
Federal Communications Commission (2007). Communications Assistance for Law Enforcement Act (CALEA.
Federal Communications Commission (FCC) (2000). Deployment of Advanced Telecommunications Capability: Second Report Washington, DC Federal Communications Commission
Feld, H. (2007) "700 MHz Endgame: Martin Antes. AT&T Raises. Google Calls. Does AT&T Fold or Call?" Wetmachine.
Fischer, C. S. (1988). "Touch Someone: The Telephone Industry Discovers Sociability." Technology and Culture 29: 32-61.

Fischer, C. S. (1992). America calling: a social history of the telephone to 1940. Berkeley, University of California Press.
Fitchard, K. (2003) "Broadband 10 Content Apps That Will Drive Broadband in 2004." Telephony Online.
Fleishman, G. (2006) "Advocates of Wi-Fi in Cities Learn Art of Politics." New York Times.
Fleishman, G. (2006) "Chaska Was A Mess, We Find Out." WiFi Net News.
Fleishman, G. (2007a) "EarthLink Relaunches Corpus Christi." Wi-Fi Net News.
Fleishman, G. (2007b) "Metro-Scale Neworks Seem to Have Security Act Together." Wi-Fi Net News.
Freepress.net (2007). FCC Revises 700 MHz Rules, Federal Communications Commission.
Fuentes-Bautista, M. and N. Inagaki (2005). The Wi-Fi's Promise and Broadband Divides: Reconfiguring Public Internet Access in Austin, Texas. Telecommunication Policy Research Conference. Arlington, VA.
Gilbert, F. (2007). Lakehead University. Wireless Cities Summit Toronto, Canada.
Gillett, S. (2006). "Municipal Wireless Broadband: Hype or Harbinger?" Southern California Law Review 79: 561-594.
Gillett, S. E., W. H. Lehr, et al. (2003). Local Government Broadband Initiatives. Telecommunication Policy Research Conference. Arlington, VA.
Gillett, S. E., W. H. Lehr, et al. (2006). "Municipal electric utilities' role in telecommunications services." Telecommunications Policy 30(8-9): 464-480.
Gillett, S. E., W. H. Lehr, et al. (2006). Measuring Broadband's Economic Impact: Final Report. Washington, DC, U.S. Department of Commerce, Economic Development Administration.
Government Technology (2007) "San Francisco Mayor Announces New Digital Inclusion Plan." Government Technology.
Griffith, E. (2007) "More Wireless, Not Enough Security." Wi-Fi Plane.
Gubbins, E. (2006). "Neutrality and municipalities." Telephony 247(3): 24-27
Gubbins, E. (2007). Fast Enough For You? How Much Bandwidth Is Enough. Telecom/Tech Research 20070511, Bell University Labs.
Gunkel, D. (2004). ""Second Thoughts: Towards a Critique of the Digital Divide." New Media and Society 5(4): 499–522.
Harchaoui, T. and F. Tarkhani (2003). Public Capital and Its Contribution to the Productivity Performance of the Canadian Business Sector. Ottawa, Statistics Canada.
Harchaoui, T. M., F. Tarkhani, et al. (2003). Public Infrastructure in Canada, prepared by Statistics Canada for Infrastructure Canada.
Havas, M. (2006). "Electromagnetic Hypersensitivity: Biological Effects of Dirty Electricity with Emphasis on Diabetes and Multiple Sclerosis." Electromagnetic Biology and Medicine 25: 259–268.
Havas, M. (2007). An Inconvenient Truth . . . Part 2: Radio Frequency Radiation & Our Health Wireless Cities Summit. Toronto, Canada.
Havas, M. and D. Stetzer (2004). Dirty Electricity and Electrical Hypersensitivity: Five Case Studies World Health Organization Workshop on Electrical Hypersensitivity. Prague, Czech Republic.
Ho, D. (2006) "Boston's Wireless Gamble: A 'Disruptive' Path To The Internet." Cox News Service.
Hogendorn, C. (2007). Broadband Internet: Net Neutrality versus Open Access Wesleyan University.

Hoofnagle, C. J. (2005). Privacy Self-Regulation: A Decade of Disappointment, Electronic Privacy Information Center (EPIC). .
Intel (2005). Digital Community Best Practices White Paper Wireless Internet Institute.
International Commission for Electromagnetic Safety (ICEMS) (2006). Benevento Resolution The Precautionary EMF Approach: Rationale, Legislation and Implementation, Benevento, Italy.
International Network of e-Communities (INEC) (2006). Stockholm Declaration on Open Networks. Stockholm, INEC.
International Telecommunication Union (2005). Privacy and Ubiquitous Network Societies International Telecommunication Union.
International Telecommunication Union (2005). Ubiquitous Network Societies: The Case of Japan. ITU Workshop on Ubiquitous Network Societies International Telecommunications Union.
International Telecommunication Union (2006). Ubiquitous Network Societies.
Jaeger, P. T., J. C. Bertot, et al. (2006). "The Policy Implications of Internet Connectivity in Public Libraries " Government Information Quarterly 23(1): 123-141.
Jauchem, J. R. (1993). "Alleged Health Effects of Electromagnetic Fields and Microwaves: Additional Misconceptions in the Literature." J. Microwave Power & Electromag. Energy 2: 140 - 155.
Karagiannis, K. (2003) "Ten Steps to a Secure Wireless Network." PC Magazine.
Katkin, K. (2006). The Global Broadband Satellite Infrastructure Initiative Telecommunications Policy Research Conference. Washington, DC.
Kim, R. (2006). Free wireless a high-wire act: MetroFi needs to draw enough ads to make service add profits
. San Francisco Chronicle. San Francisco.
Laurie, B. (2007). Selective Disclosure, Google.
Lean, G. (2007) "Danger On the Airwaves: Is the Wi-Fi revolution a health time bomb? ." The Independent.
Lehr, W. (2004). Economic Case for Dedicated Unlicensed Spectrum Below 3GHz. New America Foundation Conference.
Lehr, W. and L. W. McKnight (2003). "Wireless Internet access: 3G vs. WiFi?" Telecommunications Policy 27: 351-370.
Lehr, W., M. Sirbu, et al. (2004). Municipal Wireless Broadband: Policy and Business Implications of Emerging Access Technologies. Competition in Networking: Wireless and Wireline, London Business School.
Lehr, W. H., M. A. Sirbu, et al. (2006). "Wireless is Changing the Policy Calculus for Municipal Broadband." Government Information Quarterly forthcoming.
Limbach, I. (2007) "WiMax Gains Momentum " Financial Times.
Linksys (2007) "Wireless Security: Four Steps you need to Take."
Longford, G. (2006) "Municipal WiFi is Coming, and Why Privacy Advocates Should Care." blog*on*nymity: blogging On the Indentity Trail.
Longford, G. (2007a). 'Network Neutraliy' Vs. 'Network Diversity' : A Survey of the Debate, Policy Landscape and Implications for Broadband As An Essential Service for Ontarians, Government of Ontario, Ministry of Government Services.
Longford, G. (2007b). Examples of Non-Neutrality, Canadian Research Alliance for Community Innovation and Networking (CRACIN).
Lyon, D., S. Marmura, et al. (2005). Location Technologies: Mobility, Surveillance and Privacy, A Report to the Office of the Privacy Commissioner of Canada under the Contributions Program.

Meinrath, S. (2005). "Community Wireless Networking and Open Spectrum Usage: a Research Agenda to Support Progressive Policy Reform of the Public Airwaves." The Journal of Community Informatics 1(2).
Meinrath, S. (2006) "Utopia Municipal Fiber Network Demonstrates that Low-Cost Pricing and High-Speed Networking is Doable " Muniwireless.com.
MetroFi.
Middleton, C., G. Longford, et al. (2006). ICT Infrastructure as Public Infrastructure: Exploring the Benefits of Public Wireless Networks. Telecommunications Policy Research Conference (TPRC). Arlington, VA.
MobileTracker (2005) "Total Mobile Subscribers Top 1.8 Billion." MobileTracker.
Mueller, M. (1999). "Universal Service Policies as Wealth Redistribution." Government Information Quarterly 16(4): 353-358.
Muleta, J. (2006). Broadband Spectrum Management. Trends in Telecommunication Reform. ITU. Geneva, ITU.
Muniwireless (2007a). List of US Cities and Regions With Wireless Projects.
National Broadband Task Force (2001). The New National Dream: Networking the Nation for Broadband Access. Ottawa, Industry Canada.
Negroponte, N. (2002). Being Wireless Wired. 10.
Noam, E. (2001). The Next Frontier for Openness: Wireless Communications. New York, Columbia Institute for Tele-Information (CITI).
Noam, E. M. (1995). Taking the Next Step Beyond Spectrum Auctions: Open Spectrum Access. IEEE Communications Magazine. 33.
Novarum (2007). Wireless Broadband Rankings.
OECD (2007). OECD Principles on Private Participation in Public Infrastructure OCED.
Ontario Ministry of Public Infrastructure Renewal (2004). Building a Better Tomorrow Framework: An Infrastructure Planning, Financing and Procurement for Ontario's Public Sector, Ontario Ministry of Public Infrastructure Renewal.
Oram, A. (2007) "MuniWireless Conference: City Politicians Need to Understand the Lay of the LAN."
Organisation for Economic Co-operation and Development (OCED) (2006). The Spectrum Divided: Spectrum Management Issues. W. P. o. T. a. I. S. Policies, Organisation for Economic Co-operation and Development (OCED).
Organization for Economic Co-operation and Development, D. f. S. T. a. I. (2006). The Implications of WiMAX for Competition and Regulation. Paris, OECD.
Perkowski, M. (2007). Crossing the Chasm? New Research Predicts a Billion-Dollar Municipal Wireless Market in Two Years. MuniWireless Newsletter. March 2007: 6-7.
Perkowski, M. (2007). Umatilla County built a network for an application it doesn't want to deploy... and now uses it for everything else. Muniwireless Newletter: 28-34.
Perlman, A. (2007). A Perfect Match: How the Marriage of WiFi and AMR Could Transform Meter Reading Muniwireless Newsletter: 18-27.
Potter, B. (2006). "Wireless Hotspot: Petri Dish of Wireless Security." Communications of the ACM 49(6): 51-56.
Powell, A. (2007). Initial Report on Frederiction eZone Case Study. C. T. Meeting. Toronto, Ontario, Canada.
Powell, A. and L. Regan Shade (2006). "Going Wi-Fi in Canada: Municipal, and Community Initiatives." Government Information Quarterly 23(3-4): 381-403
Reardon, M. (2006) "Cities Deploying Wi-Fi Face Challenges." C-Net News.
Reardon, M. (2007) "Facing Economic Realities of Muni Wi-Fi." C-Net|News.
Richardson, G. (2005). Municipal Wireless: Request for Proposal (RFP) - Best Practices Civitium.

Richardson, G. (2007) "Municipal Wi-Ideology." Civitium's Weblog.
Richardson, M. and P. Ryan (2006). "WiMax: Opportunity or Hype?" ITERA.
Rideout, V. N. and A. J. Reddick (2005). "Sustaining community access to technology: Who should pay and why." The Journal of Community Informatics 1(2): 45-62.
Ross, S. S. (2006) "WiFi: A Great Amenity, A Lousy Cure for The Digital Divide."
Sacca, C. (2007) "Our Commitment to Open Broadband Platforms." Google Public Policy Blog.
Sage, C. (2004). An Overview of Radiofrequency/Microwave Radiation Studies Relevant to Wireless Communications and Data Santa Barbara, CA, Sage Associates.
San Francisco Budget Analyst (2007). Fiscal Feasibility Analysis of a Municipally-Owned Citywide Wireless Broadband Network. Prepared for the Board of Supervisors of the City and County of San Francisco. San Francisco, City of San Francisco.
San Francisco Chronicle (2006) "Hidden Cost of 'Free' Wireless." San Francisco Chronicle.
Sandvig, C. (2002). Disorderly Infrastructure: Wi-Fi in the Shadow of the Rural Telephone Cooperative. Casting a Wider Net: Integrating Research and Policy on the Social Impacts of the Internet, Oxford.
Sandvig, C. (2004). "An Initial Assessment of Cooperative Action in Wi-Fi Networking." Telecommunications Policy 28(7/8): 579-602.
Sandvig, C. (2006). Cartography of the Electromagnetic Spectrum: A Review of Wireless Visualization and its Consequences. The 34th Research Conference on Communication, Information and Internet Policy, Telecommunications Policy Research Conference (TPRC). Arlington, VA.
Sandvig, C. (2006). "Network Neutrality is the New Common Carriage." Info: The Journal of Policy, Regulation, and Strategy.
Sawhney, H. (1992). "Public telephone network: Stages in infrastructure development,." Telecommunications Policy 16(7): 538-552.
Schaefer, R. J. (1995). "National information infrastructure policy: a theoretical and normative approach." Internet Research 5(2): 4-13.
Schwartz, E. (2005). "Cellular Data Ramps Up." InfoWorld 27 (12).
Seltzer, W. (2007) "Selective Disclosure and Privacy." wendy.seltzer.org.
Settles, C. (2006). What's the Price of "Free"? Municipal Wireless Snapshot.
Shamp, S. A. (2004). Wi-Fi Clouds and Zones: A Survey of Municipal Wireless Initiatives. Mobile Media Consortium, University of Georgia. .
Sicker, D. C., D. Grunwald, et al. (2006). Examining The Wireless Commons. The 34th Research Conference on Communication, Information and Internet Policy, Telecommunications Policy Research Conference (TPRC). Arlington, VA.
Stone, M., C. Maitland, et al. (2006). "Making IT Work for Municipalities: Building Municipal Wireless Networks." Government Information Quarterly 23(3): 359-380.
Swider, P. (2007) "Is Wi-Fi Bad for Your Health?" Wi-Fi Planet.
Tapia, A. H. and J. A. Ortiz (2006). Municipal Responses to State-Level Broadband Internet Policy. Telecommunications Policy Research Conference (TPRC).
Tapia, A. H., M. Stone, et al. (2005). Public-Private Partnerships and the Role of State and Federal Legislation in Wireless Municipal Networks. Telecommunication Policy Research Conference, Arlington, VA.
The OPLAN Foundation.
The Wireless Philadelphia Executive Committee (2005). Wireless Philadelphia business plan: Wireless broadband as the foundation for a digital city.
Third Generation Partnership Project.
Toronto Hydro One Zone (2007). Toronto Hydro One Zone FAQ.
Toronto Public Library (2007). Reserve A Computer.

Turner, S. D. (2005a). Broadband reality check: The FCC ignores America's digital divide,
Free Press.
Turner, S. D. (2005b). Free American Broadband! Salon.com.
Utah Telecommunication Open Infrastructure Agency (2003). Utah's Public-Private Fiber-to-the-Premises Initiative White Paper
UTOPIA.
Valberg, P. A. (1997). "Radio frequency radiation (RFR): the nature of exposure and carcinogenic potential." Cancer Causes and Control 1997(8): 323-332.
Valberg, P. A., T. E. van Deventer, et al. (2007). "Base stations and wireless networks-radiofrequency (RF) exposures and health consequences." Environmental Health Perspectives 115(3): 416-424.
van Winden, W. and P. Woets (2004). "Urban Broadband Internet Policies in Europe: A Critical Review " Urban Studies 41(10): 2043–2059.
Vander Ploeg, C. G. (2003). Municipal Infrastructure in Canada: Issues of Terminology and Methodology, Canada West Foundation.
VeriWave (2007). Master Test Plan: Wireless LAN & Muni-Wireless Testing. White Paper.
Vos, E. (2005) "Help Solve the Orlando Wi-Fi Mystery." Muniwireless.com.
Vos, E. (2006d) "St. Cloud, Florida Citywide Wi-Fi Update: Launch Plus 10 Days." Muniwireless.com.
Vos, E. (2006g) "Wireless Philadelphia-EarthLink Contract: An Analysis." Muniwireless.com.
Vos, E. (2007a) "Detailed Analysis of EarthLink-San Francisco Contract." Muniwireless.com.
Vos, E. (2007b) "Privacy on Public Wi-Fi Networks: Is Tracking Necessarily a Bad Thing? ." Muniwireless.com.
Wareham, J., A. Levy, et al. (2004). "Wireless diffusion and mobile computing: implications for the digital divide." Telecommunications Policy 28(5-6): 439-457.
Wi-Max.com (2007) "What is Unlicensed Spectrum? What Frequencies Are They In?"
Williams, J. E., C. M. Wallace, et al. (2005). "Free Internet as Agent of Community Transformation " The Journal of Community Informatics 2(1).
WiMax Forum.
Wireless Philadelphia (2005). Wireless Philadelphia Request for Proposals For A Citywide Network: Section 2.3, Proof of Concept Philadelphia, PA: 19.
Wireless Philadelphia. (2007a). "Digital Inclusion Program." from http://www.wirelessphiladelphia.org/digital_inclusion.cfm.
Wireless Philadelphia. (2007b). "Our Mission." Retrieved August 16, 2007, from http://www.wirelessphiladelphia.org/about_mission.cfm.
Wireless Philadelphia (2007c) "Proof of Concept Acceptance " Wireless Philadelphia Blog.
Wood, A. W. (2006). "How Dangerous Are Mobile Phones, Transmission Masts, and Electricity Pylons?." Arch Diseases Childhood 91: 361 - 366.
Wu, T. (2005). "Network Neutrality, Broadband Discrimination." Journal of Telecommunications and High Technology Law 2.
Xavier, P. (2003). "Should Broadband Be Part of Universal Service Obligations?" Info: The Journal of Policy, Regulation, and Strategy 5(1): 8–25.
Zager, M. (2007). Broadband Access Empowers Low-Income Families, OneEconomy.
Zhang, M. and R. S. Wolff (2004). "Crossing the Digital Divide: Cost-Effective Broadband Wireless Access for Rural and Remote Areas." IEEE Communications Magazine(February): 99-105.

DESIDERATA SUMMARY TABLE

DESIDERATA	DEFINITION	WIFI	KEY ISSUES	ASSESSMENT
UBIQUITOUS & UNIVERSAL	Service coverage should include every household, business, organization, public space, tourist destination, and public transit corridor in the network's coverage area, within the limits of what is technically feasible. Ultimately, the service should be *universal*, that is, it should reach every person when and where they need it.	Wireless contributes to enlarging service coverage to areas that are not easily reachable by wireline	Role of government in bridging the digital divide. Municipal wireless focus on ubiquity and the digital divide. Municipal role in ensuring universal service. The difference between universality and ubiquity. Is ubiquity really necessary? Usefulness of ubiquitous coverage for Internet service vs. for other applications.	Technical testing for service availability. Evaluation of network coverage policy – where and for whom does the network intend to offer service? Potential number of subscribers vs. actual number of subscribers. Number of subscribers before and after network deployment. Network use patterns: where the network gets the most and least use, and reasons for why this might be the case. Coverage area of previously existing broadband service in the community. User POV on how ubiquitous and universal the service is in practice.
WIDELY USEFUL	Good infrastructures allow for a wide range of applications that people find useful in conducting their daily affairs. While some of the most important ones can be anticipated and designed for,	Wireless brings obvious benefits of portability and mobility, but also opens up new possibilities (such as location-based services) that were not previously feasible. This expands usefulness, while serving as a platform	Preparing for ubiquitous network societies. Digital divide.	Readiness of network for future applications (open, neutral, ubiquitous, etc.).

	others will emerge over time.	stimulating new economic activity as suppliers enter with new service offerings.		

USABLE	Ideally infrastructures 'disappear' in the sense that they can be taken for granted – always ready to be used effortlessly, but never getting in the way of the immediate task at hand.	Wireless internet offers a significant step towards this ideal with its potential ubiquity and growing availability of easy to use wireless-enabled devices.	Network that meets the needs of the local community and is easy for them to use. Bad network planning can lead to an under-used network.	Evidence that users use the network. Evidence that the network is straightforward and easy to use. User POV on network accessibility and usability.
ACCESSIBLE	Access to the system should be as barrier-free as possible, accommodating a wide range of cognitive and physical disabilities. The service should also accommodate a community's linguistic diversity. Conducting user needs analysis at the design stage and providing technical support can help to ensure that a network is accessible.	Wireless enhancement can help make Internet services more adaptable to particular populations and individual user needs.	Network that meets the needs of the local community and is easy for them to use. Disability, language, culture, etc. barriers to connectivity.	Evidence of stakeholder consultation. Responsive network design, targeted to local needs. Availability of quality technical support. Challenges the network has faced, including common user complaints.
AFFORDABLE	In order to ensure universal access for all, including low-income households, the service should be available at affordable rates (e.g. <$10 per month) and preferably for free. Ideally, the service should provide free access to basic	Wireless service, because it can greatly reduce the cost for extending service into areas where wireline is relatively expensive, can help make Internet access more affordable.	Digital Divide. What business models can offer the most affordable service? Free Wi-Fi debate. Tiered service and digital inclusion rates. Calculating reasonable user	How user fees compare to user fees for comparable service. Assessment of business model to determine the rationale behind the user fee. Evidence of awareness of what is affordable to the community the

	broadband service (e.g. 1.5 Mbps, bi-directional as specified by National Broadband Task Force, 2001), with the possibility of fees for premium, higher speed services to support high bandwidth uses.		fees.	network serves.
RELIABLE	The service should be as reliable as the other common utilities, such as water, power, and the telephone, with clear performance standards established (99.99% availability, 4 hours mean time to repair).	Reliability likely represents the major technical challenge to wireless internet, as the unlicensed 2.4 Ghz spectrum used by 802.11b/g protocols is subject to interference by other devices (e.g. microwaves, door openers) and is highly susceptible to attenuation (e.g. by trees in residential areas).	Overview of Wi-Fi reliability issues. The unlicensed spectrum and reliability. Trade-offs between reliability and other desirable network characteristics, such as affordability.	Technical testing for reliability. Stated reliability standards and evidence of method for achieving them. User POV on reliability.

HIGH QUALITY	The service should maintain a good standard of throughput and response time for streaming or other time sensitive transmissions requiring particular Quality of Service (QoS) standards (e.g. public emergency, telemedicine). However, these should not be discriminatory in the sense of allowing the network provider to favor arbitrarily some communicants over others or permit inspection of packet content.	As with Reliability above, wireless internet is challenging in this regard because of spectrum contingencies, such as interference and variable attenuation, as well as the greater difficulty in determining device identities as the basis for assigning bandwidth priorities.	How much bandwidth is enough? Various perspectives and approaches to determining this figure. Upstream and downstream speeds. Dangers of setting bandwidth requirements too low or too high. Tiered service and minimum bandwidth speed. Trade-offs between quality and other desirable network characteristics, such as affordability.	Technical testing of network speed. Network speed meets the minimum standard of bi-directional 1.5 Mb/s. Evidence of stakeholder consultation on bandwidth needs. Meets users bandwidth needs, and has a clear strategy to continue to meet user needs in the future. User POV on quality.
HEALTHY	Electromagnetic radiation emissions associated with network equipment shall be within known safe limits, and should be routinely monitored.	Given that Wi-Fi power levels are relatively low and their placement in relation to human bodies is no more hazardous than existing sources of electro-magnetic radiation (e.g. mobile phones), there should be no additional concerns with wireless. However, the health risks of unusual situations should be identified.	Results of scientific research to date on electromagnetic radiation emissions. Public concerns and debate on Wi-Fi and health.	Commitment to monitor results of new studies on the issue, and to adjust the network accordingly. Commitment to respond to the health concerns of users.
COST-EFFECTIVE	Independent of the pricing for affordability mentioned above, public	Wi-Fi makes very efficient use of a spectrum that historically has been regarded as	Cost-effective use of spectrum. Cost-effective use of existing	Assessment of business plan: were funds to build the network cost-effectively used? Is

	infrastructures should make efficient and effective use of the resources they require to offer service.	having marginal utility and low value. Where wireless services can be built on top of existing physical, electrical and wireline communications infrastructures, the marginal costs can be kept relatively low. For instance, Toronto Hydro Telecom's One-Zone wireless internet efficiently leverages existing publicly-owned fibre backbones and street lighting in creating a high quality, city-wide service at a fraction of the cost of conventional alternatives.	resources, such as utility poles. Cost-effective infrastructure investments – multi-application and future-proof networks. Cost-effectiveness of investment in fiber vs. Wi-Fi. Public vs. private cost-effectiveness.	the plan for future operations structured in a cost-effective manner? How does the plan address short vs. long-term cost-effectiveness? Evidence of cost-effective use of existing resources, such as utility poles and spectrum. Assessment of whether the network under- or over- meets user needs.
ACCOUNTABLE & RESPONSIVE	Mechanisms of governance and citizen oversight and control to ensure that the service and its operator are responsive to citizen input and needs on issues ranging from network repairs to new service innovation.	Wireless access can help expand the modes of citizen involvement and oversight.	The role for the public sector in ensuring network accountability and responsiveness. Municipal wireless projects and customer service issues.	Do accountability structures, such as transparency and a clear governance model, exist? What is the network approach to addressing technical and customer service issues? What paths are available for user input? User POV on network responsiveness.
SECURE	State of the art technology and best practices should be adopted to ensure that personal	As an over-the-air service, wireless is more susceptible to interception and corruption than more physically	Electronic and mobile security issues. Wireless security issues, and how a wireless network	Technical security test. Evidence of security policy and adequate security standards.

	communication and internet browsing are secure against unwarranted interception. Non-intrusive means should be incorporated into the service to protect users against spam, viruses, spyware, etc. Reasonable, lawful means should be adopted to protect users against illegal content (e.g. child pornography, hate speech).	secure wireline transmission. However, commonly available encryption and authentication techniques are currently adequate if implemented properly.	can be secured. Security vs. privacy, a delicate balance.	Rationale behind level of security and potential privacy trade-offs. Roles of network provider and network users in network security.
PRIVACY ENABLING	Operation of the service shall be fully compliant with applicable privacy laws and best practices. No personally identifying information shall be collected beyond that which is necessary to ensure access to and operation of the network. The service should enable both pseudonymous and anonymous use. Location-based and other services requiring additional personal information may be offered on a strictly voluntary, opt-in basis.	As with Security above, wireless internet presents inherent difficulties beyond those already problematic with the wired internet. However, the content of messages (if not traffic patterns) can be protected technically. Some Legal and legislative changes may be necessary to deal with the ambiguity of 'personal' communication via 'public' airwaves' and detectable in 'public spaces'.	Electronic and mobile privacy issues. Privacy and free ad-supported Wi-Fi network models (ex: San Francisco). EPIC/ACLU/EFF model minimum standards. Federal vs. local role in ensuring electronic privacy.	Does the network meet the EPIC/ACLU/EFF model minimum standards for privacy? How clearly is the network privacy policy communicated to users?

OPEN	The service should be designed to maximize openness at various levels (e.g. openness to a variety of access devices, the use of open source software, and all kinds of content, applications and services.)	Unlike in wireless telephony, the key standards and regulations for Wi-Fi communication, notably the 802.11 family, are oriented to openness, not competition among rival incumbents, and sufficiently stable to support the development of an expanding range of interoperable devices and applications (Noam, 2001).	Open Access and Network Neutrality movements. Municipal wireless and the cooperative wholesale model. Feasibility of open network structures based on community size and local politics. Open networks and competition. Preparing for ubiquitous network societies.	Does the network meet the principles of the INEC Declaration on Open Networks? What is the structure of the network? Are the infrastructure and content layers separate? Are there any restrictions on who can provide service over the network? What is the rationale for this restriction?
NEUTRAL & NON-DISCRIMINATORY	No restrictions on access to lawful content/services, and no discrimination on the basis of content or services (e.g. P2P networks) beyond what is necessary for efficient network operations (Sandvig, forthcoming).	The early stage of the establishment of wireless infrastructures provides an opportunity to ensure that network neutrality principles are embedded in them. These wireless networks may provide an alternative to non-neutral wireline networks, and encourage the wider adoption of neutral and non-discriminatory network principles.	Network neutrality debate. Justifications for QoS discrimination.	Are there any restrictions on who can provide service or content, or what content and service can be provided? What is the rationale for these restrictions?