A Policy Maker's Guide to Wi-Fi Networks

Walter Siembab
Siembab Planning Associates
www.siembab.com
January, 2005

Topics

What is Wi-Fi?

Wireless Fidelity (Wi-Fi) is an inexpensive, short range, line-of-sight, broadband wireless technology that uses the same *unregulated* radio frequencies as microwave ovens and cordless phones. It is essentially a wireless local area network that can be deployed so as to serve a single business such as a coffee shop, or deployed citywide in what is referred to as a *mesh* network. A business model is still emerging.

Wi-Fi's appeal is that it is can be deployed at a much lower cost than other broadband network technologies (about 10% the cost of fiber optics) so that its products, like high-speed Internet access, can be offered at relatively low prices. By changing the economics of high speed Internet access, Wi-Fi has the potential to dramatically increase the number of people and businesses who have access to e-commerce, distance education, e-government, telemedicine and other electronic services.

Critics claim the transmission is unreliable, susceptible to weather disruptions and, in any case, not *carrier class*.

A Wi-Fi network has four basic elements:

- Access Points (radio transmitters on poles)
- Wired or wireless connection to a base station
- A Wireless ISP (WISP)
- Wired or wireless connection from base station to the WISP's server.

User must have the appropriate network card that matches the standard used by the radio transmitter. Cards are widely available for between $50 and $150, depending on quality. A high quality card is like a good antennae that can pick up a weaker signal at the outer reaches of the radio transmitter. Virtually every new laptop computer comes factory-equipped with a Wi-Fi card.

The following are the terms used to describe the types of Wi-Fi coverage area (based on definitions from the Mobile Media Consortium at the University of Georgia):

Hotspot – A single Wi-Fi coverage area, like a single building or a park usually covering an area no larger than a football field. There are about 22,000 hot spots in the United States today and their number is forecast to grow to 40,000 by 2007. Coverage provided by hotspots is isolated and sporadic.

Wi-Fi Zone – A zone is unified by service, not geography. It is an aggregation of cooperating hotspots sharing a single management system. A single login allows an end-user to access the network anywhere in the geographic area covered by the zone. A zone may cover a large area like a mall or convention center, but the area covered need not be contiguous.

Copyright Walter Siembab, January 2005

Wi-Fi Cloud – Offers contiguous and unified coverage over a significant portion of a city's geographic area, usually using multiple hot spots. Although clouds may differ greatly in their size, they offer coverage with no gaps. The cloud is the most significant step toward ubiquitous and pervasive coverage in the Wi-Fi movement.

Public Access – A hot spot, zone, or cloud wherein anyone meeting established membership requirements (such as registering with the provider or purchasing a subscription) can access the network. Public access can be free or for-fee. Private access is where the network is dedicated to a certain group of end-users such as government public safety personnel or employees of a particular entity.

Where did Wi-Fi come from?

Wi-Fi has emerged as a potentially significant element of the urban telecommunications infrastructure in a relatively short period of time. The following describes its recent evolution.

Living rooms and offices
Wi-fi started in living rooms and small offices as a cheap and easy way to link a room full of computers to the Internet that would normally require extensive wiring.

Unintentional hot spots
Because the signal could go through windows and walls, passersby on the street found they could jump on the Internet through the *hot spot* that was created up to a football field away from the source. The term *war chalking* was coined by a NewYorker in May, 2002. The term refers to the ad hoc practice of discovering hot spots and indicating their presence for others by drawing symbols in chalk on sidewalks and adjacent buildings.

Commercial hot spots
Hot spots are developed in coffee shops, hotel lobbies, airport terminals and other public waiting areas, usually with the goal of attracting business to those places. Commercial (for fee) hot spots began to appear, usually in national chains like McDonalds and Starbucks ($30/mo. for unlimited access). Most hot spots remain free, which undercuts the ability of others to charge. Commercial hot spot retailers are aggregating into national brands that offer travelers roaming capabilities. Boingo Wireless is one such aggregator.

Factory, medical and college campus hot zones
Manufacturing plants, college campuses and health care facilities were next to deploy hot spots to facilitate intra-campus connectivity.

City hot zones and clouds
Cities and the idea of municipal Wi-Fi became the big market in 2004. The evolution of Wi-Fi markets has happened so quickly that business models have not yet been developed.

Copyright Walter Siembab, January 2005

What government regulations apply to Wi-Fi deployment?

Virtually none in comparison to other technologies. The federal government has traditionally circumscribed municipal policy on cable television. The federal and state governments together regulate telephony. Wi-Fi, for the most part, uses un-regulated spectrum and is free from any other federal or state oversight. The exception is the growing movement for states to prohibit municipal Wi-Fi networks offering services in competition with private broadband providers. About 17 states have passed or are considering passing such legislation. In contrast, Michigan has a Broadband Development Authority which funds the Digital Divide Investment Program as a way of providing grants to local governments to help them acquire broadband infrastructure.

Why do cities want Wi-Fi?
How realistic are the benefits?

Network technologies while ever more powerful and cost/effective also tend to be over-promised as a causal force, particularly during the sales phase of decision making. The industry refers to this as the "technology hype-cycle".

For example, Wi-Fi advocates repeat the phrase *no broadband, no jobs* as a justification for rapid and widespread deployment of hot spots, zones and clouds. It is true that economic backwaters usually lack a robust broadband infrastructure, and concentrations of high paying jobs are always supported by extensive broadband options. However, it is not true that adding a broadband infrastructure will, by itself, heat the economy and create jobs.

In other words, better infrastructure is almost always a good thing depending on the cost, but it is not *plug and play*. The promises associated with new infrastructure can be realized only when it is a catalyst to other programs and initiatives. Jurisdictions need to get better at creating these companion initiatives as well as verifying the benefit-capture upon which the decision to proceed was based.

Therefore, it is useful to not only examine the reasons why local governments embrace the Wi-Fi infrastructure, but also the realistic expectation that the benefits can be realized.

The justifications for municipal wireless follow three main themes:

- Constituents want broadband but do not have it or it is not affordable.
- Wi-Fi will lead to economic development.
- Local government can use Wi-Fi to lower costs or improve services.

Constituents want broadband but do not have it or it is not affordable.

Incumbent local exchange carriers, competitive local exchange carriers and cable companies have not made the infrastructure investments required to provide high speed

Internet access in many of the low income, low density suburbs. Those are prime locations for Wi-Fi clouds that are cheaper to deploy than equivalent wired networks. The need is real and the benefit is tangible – the Wi-Fi infrastructure makes service available where it previously wasn't.

Other cities may have DSL or digital cable service but with large un-served pockets and/or relatively high prices. These are often low income central cities and their immediate suburbs where the need is real and the desired outcome can be measured. Wi-Fi can close broadband service gaps and overlay an entire city with a reasonable expectation that competition will generally lower costs and improve customer service.

Evaluating whether the promised benefits are realized involves knowing the location of the un-served pockets and the prevailing rates before and after Wi-Fi deployment. This is relatively easy to accomplish so the benefits are verifiable.

Walla Walla County in rural Washington provides a dramatic example. The community electric utility developed a cloud over 1,500 square miles (an area larger than the state of Rhode Island) to bring high speed Internet access to an area for which wired service was completely unaffordable because of its extent, low density and low income.

Wi-Fi will lead to economic development.

The next most common rationale for pursuing Wi-Fi is economic development. This is often expressed as a Wi-Fi network will:

- Attract visitors to the area
- Attract businesses to relocate to the area
- Improve the image of the city
- Improve competitiveness of a particular retail district
- Promote local business through advertising on the entry page
- Close the digital divide

These assertions may hold true in some circumstances, but economic outcomes are hard to verify after the fact. For example, many factors influence in complex ways visitation or city image so that causality or even influence may be difficult to demonstrate. In the end, very few jurisdictions attempt to assess the promises made at the time a technology is adopted.

In the case of municipal Wi-Fi, most examples are either being planned, are currently being deployed, or have been operating for less than a year. Consequently, there are no studies of the economic impacts actually experienced following implementation of Wi-Fi. In other words, no one really knows the extent to which Wi-Fi clouds or zones actually stimulate desired economic activity, but advocates claim that it does so.

What can be done easily and affordably is monitor network usage. Evan allowing that usage will grow over time, usage in the first year of operations where it has been

measured is far from overwhelming. Registered uses in Culver City and Hermosa Beach, California are running between 1% and 2% of each city's residential population. Daily regular users in Culver City are less than .001 % of the residential population.

The ultimate economic value of Wi-Fi will grow over time, particularly as 3rd generation cellular wireless integrates with municipal clouds, and voice over Internet protocol becomes a reality facilitated by dual mode telephone handsets. The future is discussed in the final section of this Guide.

Local government can use Wi-Fi to lower costs or improve services.

Some cities approach Wi-Fi as a tool that will help reach specific goals.

Corpus Christi, Texas owned a fiber backbone network that reached 2/3 of the City as part of a signal-control traffic management system. The city wanted to automate gas and water meter reading (AMR) in order to reduce labor costs and to better manage water and gas distribution through real time meter monitors. A metro-wide Wi-Fi mesh network provided the least cost method of extending the reach of the fiber network in order to relay gas and water meter data from AMR concentrators to the City's Utilities business system.

Cook County, Illinois is using Wi-Fi as the basis for a public safety network that will eventually support mobile police and fire units over 940 square miles. The network will make over 95% of Cook County observable from video cameras carried in police amd fire vehicles. Fighting crime and terrorism and helping fire fighters see the extent of a fire before arriving are the main applications.

Although not its initial reason for pursuing a fiber-Wi-Fi hybrid network, reducing the City's costs for leased T1 lines is part of the justification for building the system in Brockton, Massachusetts.

Spokane's plan for a city-wide wireless broadband network has two domains: (1) the city's private domain which it will use for public safety, mobile workforce, and automated parking enforcement and (2) the public domain (SpokaneHotzone) which is devoted to public access offered through OneEighty Networks, a local WISP.

How have cities gone about obtaining Wi-Fi Infrastructure?

There has been no single path that cities have used to obtain Wi-Fi. A wide variety of approaches have been tried that reflect state law, the status of the existing network infrastructure and the technology aspirations of the jurisdiction.

Most Wi-Fi hot spots have been privately developed in small places. Local governments get involved in these situations only when public property is needed to place the radio transmitters.

Copyright Walter Siembab, January 2005

There are examples of extensive hot spots that do not involve the local government. The firm Wi-Fi Metro deployed a hot spot in downtown Palo Alto without using city property. The Austin Wireless City Project created by a community non-profit corporation uses volunteers and donations to deploy free Internet access in a variety of privately-owned venues open to the public.

The first level of organizing the national experience is into two broad categories – initiatives introduced by private vendors and initiatives designed by local government, although usually implemented by the private sector. Then within each there are a number of variations, some with complex arrangements.

Initiatives introduced by private vendors

There are two approaches in this category. The first is those cities that make no investment in the Wi-Fi network. The cities simply lease pole or building space to the vendor via a straight-forward administrative process. Examples include Santa Clara and neighboring cities like Mountain View and Cupertino, all in California.

The second approach involves the city making some kind of investment in the initiative. It is unusual in the realm of local government contracting to give a sole source contract to a vendor presenting an unsolicited proposal. As Appendix 2 shows, that happens with some regularity with Wi-Fi networks.

There are at least three reasons for this practice.

- Wi-Fi networks are novel and most local governments don't themselves know how to go about it even if they had previously thought about it, which most haven't.

- The low cost, relatively uncomplicated nature of a Wi-Fi network eliminates barriers to entry so that the industry has been characterized so far by start-ups, although established players like T-Mobile and Cingular Wireless are gaining momentum. The vendor was a small, local start-up in virtually every example of a private vendor driving the initiative. This creates the look and feel of local economic development.

- The cost of deploying a downtown hot spot is comparatively not much more than the cost of issuing and evaluating an RFP, and a lot less work.

Examples of this approach include Culver City and Long Beach in California plus Dayton, Ohio and Grand Rapids, Michigan.

Dayton agreed to pay about $10,000 annually for the backhaul in addition to providing free access to city property. However, Dayton says it intends to issue an RFP for a developer if it decides to expand the downtown hot spot to a citywide cloud.

Grand Rapids is especially interesting because the vendor brought the idea to the city, proposed a very ambitious network and made a profit-sharing arrangement with the city. The network is a cloud that covers 6 square miles of the city plus provides service to boaters on Lake Michigan up to 15 miles from shore. Voice over Internet Protocol is in beta test and unlimited calling to any location in the United States will be sold for $30 per month. The city gets 5% of the revenues.

Local government initiatives

Local government initiatives tend to be more complex and varied than vendor-driven initiatives, and more numerous. Some of these networks were developed entirely for government use (Cook County, Corpus Christi, Brockton, Cleveland), some for both government and public use (Spokane, Dayton, Las Vegas), some offer public services for free (Hermosa Beach, West Hollywood) and some for a fee (Chaska, Lompoc, Rio Rancho), most issued an RFP (Los Angeles, West Hollywood, Muskegon County, Corpus Christi), but some did not (Cerritos, Spokane).

Starting with a pilot project hot spot in one part of town, such as downtown and, depending on its success, expanding to a citywide cloud is a common but not universal development pattern.

The following thumbnail sketches illustrate the variety and complexity of the municipal Wi-Fi experience to date:

Under pressure from its citizens to attract a broadband vendor, Cerritos reached out to a particular vendor without the use of an RFP. The city waived pole attachment fees and generally helped the vendor set up business. Its arrangement is <u>not</u> exclusive.

Lompoc's utility department is building on its reputation as a reliable electric utility to deliver broadband as a utility throughout the city. It borrowed from its reserve fund to deploy in the near term a citywide cloud which will help generate the revenue needed to develop fiber-to-the-home in the long term.

Spokane got interested in Wi-Fi because of its experience with the technology for displaying scores from a basketball tournament on panels on the top of city hall. The vendor relationships established for that event blossomed into a 100 block cloud over downtown.

In the meantime, the debate continues over the legitimate level of municipal involvement in Wi-Fi developments. The Intel Corporation, manufacturer of the chip sets used in Wi-Fi and WiMax networks, recently joined the discussion over the efficacy of municipal Wi-Fi networks. Intel opposes state legislation prohibiting municipal wireless but urges cooperative public-private ventures. Intel's position is that local governments should determine their needs and then issue an RFP for private developers to bid-on.

What business plan supports Wi-Fi development?

There is no established business plan for Wi-Fi hot spots, zones or clouds, whether they are commercial enterprise or a free utility.

Because hot spots are relatively small geographic areas, their cost of deployment and operation is relatively low. The minimal equipment required -- a radio transmitter and backhaul connection to an ISP usually provided by a DSL line – have been easily affordable to small retail storefronts such as coffee shops.

The ready availability of free hot spots to a large extent undermines the ability of commercial operators to charge for access. Rational consumers will not pay Starbucks $30 per month for Internet access when a free municipal hot spot is available next door.

Because of low deployment costs, even relatively large hot spots with free access do not require a business plan. For example, the City of L.A.'s Pershing Square Wi-Fi network can be developed and maintained for a year for $25,000, easily affordable by a large municipal corporation.

A business plan must be found as the scale and therefore the cost of deployment increases, for example, in national networks of hot zones and in municipal citywide clouds.

National networks of hot zones have been able to base their business plans on subscription fees because their target market is the inter-city road warrior who needs roaming capabilities. A subscriber to Oingo Wireless or T-Mobile is able to use the same log-on with assured compatibility at any particular hot spot in the national hot zone. This has value to a business traveler who will be in Chicago O'Hare at lunch and the San Francisco Marriott for dinner.

In the absence of the financing required to build a national hot zone, firms like Oingo Wireless and Wayport have begun to aggregate under their umbrella hundreds of *mom and pop* hot spots, along with national chains such as McDonalds. The aggregator serves as the Wireless Internet Service Provider (WISP), provides the client software, monitors usage, does the billing and splits the proceeds with the retailer.

Municipal citywide clouds, while cheaper to deploy than an equivalent wired network, still require a significant amount of capital. The budget for the Hermosa Beach cloud is over $200,000 and it is around $1 million for the Lompoc cloud. Costs of that magnitude require a business plan.

The business plan that is emerging in the public sector is based on two main sources of income – advertising on the entry page is the anchor revenue source in virtually every case, and where the service is not offered as a free amenity, subscription fees. There are two other possible sources of revenue but few systems have developed them – program

content and network services (such as virtual private networks – a more advanced offering than simple public Internet access).

One final observation regarding business plans -- because WiFi can be deployed quickly at very small scale, the industry has attracted agile start-ups while the established broadband players have been relatively slow to move. While established players such as the incumbent local exchange carriers (ILECs) have more capital, they generally require a stronger business case before investing.

What are the risks?

As with any initiative, cities involved in Wi-Fi deployment will face a few risks. As mentioned in the discussion of benefits, there is not yet enough experience with municipal Wi-Fi to empirically evaluate which situations are high risks.

Security

Network security should be at the top of the list of any concerns over risk. This applies only in cases where the city intends to use the network but, given enough time, that might well include all cities with Wi-Fi. The security issues can be resolved with careful planning.

Wireless transmission is inherently vulnerable to interception and invasion. One extremely disastrous scenario is that a criminal can use a wireless connection as a backdoor into the computer system of the user's employer. The result could be loss of valuable data, debilitating viruses, embedded Trojan horses which can control the system, attacks on other systems, and so forth. Wireless invasion is extremely difficult to trace so that the damage will appear to have been caused by the employee who opened the door rather than the criminal that walked through it.

There is the possibility of an *evil twin* – a rogue access point which jams the user's connection to a legitimate transmitter in order to intercept the information being sent by the user to the Internet. This information could be financial, personal, or political which through misuse by the rogue or loss unrecognized by the sender could have serious repercussions.

Before a local government commits to using Wi-Fi, it should direct its Information Technology Department to thoroughly examine the security protections built into the Wi-Fi network and determine the protections needed for its municipal network. There may be some applications that are too risky to try.

Public liability

The security problems of Wi-Fi can also result in losses to individuals and other corporations who use the network. Identity theft is one example. There are also potential problems with network reliability from weather disruption or denial of service attacks

Copyright Walter Siembab, January 2005

that could result in losses for those users who depend on the availability of the network. Local governments need to ensure that they are protected against responsibility for any third party losses.

Abandonment

Although unlikely in the future, vendor abandonment of its equipment in-place has happened in the past. The Ricochet equipment, an early version of Wi-Fi technology was left on poles in Cerritos and West Hollywood when the company sponsoring these early networks, Metrocom, went bankrupt. The abandoned equipment either remains in place and is unsightly or must be removed at city expense.

Privacy

The low cost of Wi-Fi makes wide spread video surveillance of public places much more cost feasible than ever before. Indeed, video surveillance is one of the leading municipal Wi-Fi applications discussed by cities planning or deploying the network. While fighting crime and terrorism are legitimate activities, appropriate privacy protections should be established to guard against overzealous surveillance that could become oppressive and invasive.

Political conflict

The network industry is in some turmoil, largely due to the instability caused by technological innovation that challenges incumbent carriers and established network industries; and exceeds the organizational innovation necessary to expand the technology markets.

The continuous bursts of technological innovation create winners and losers. Potential losers will seek government action to protect their interests. Verizon, reacting to Philadelphia's plan to create a citywide Wi-Fi cloud, conducted a high profile legislative campaign to block municipal wireless in the state of Pennsylvania. Lobbying in opposition to public sector participation in Wi-Fi should be expected at all levels of government in the coming year.

Experience in other cities suggests that downtown hot spots do not attract opposition but citywide clouds do. A track record of quality service delivery in other utilities such as electricity provides a basis for cities who want to become more directly involved in building and operating a network utility based on Wi-Fi or fiber. Lompoc is an example.

What's in the future?

Assuming no serious decline in the national economy occurs, the high levels of technological innovation of the past will continue into the future.

The challenges that incumbent networks face will go well beyond Wi-Fi. Voice over the Internet (abbreviated VoIP -- essentially packet switched instead of circuit switched phone calls) promises to revolutionize voice telephony, the bread and butter telecommunications market for over 100 years. VoIP eliminates distance, time of day, and length of call from the pricing equation by offering unlimited calls to international locations for a low fixed price.

Wi-Fi exacerbates the VoIP situation by providing a low cost ubiquitous mode of access to the Internet. Once Wi-Fi and dual mode (3rd generation cellular and Wi-Fi compatible) handsets enter the market, probably no later than 2006, the traditional voice telephony markets could enter a free fall. It is during this period that a Wi-Fi infrastructure could have important economic benefits for cities.

WiMax, the next generation of Wi-Fi, is being promoted by the Intel Corporation. WiMax promises to deliver even faster speeds over greater distances than Wi-Fi, thereby reducing the number of radio transmitters necessary to create citywide cloud. WiMax, currently in limited use, could be on the market by 2006

There may be conflicts between Wi-Fi and cellular vendors. Wi-Fi provides much greater bandwidth and therefore much faster transmission speeds than even 3G cellular. At this point Wi-Fi provides stationery wireless connectivity while cellular provides true mobile connectivity. Innovations are being rolled out that will allow mobility of users within a cloud. The dream for the future is that 3G and clouds will be deployed together with seamless transition between the two as users move about. Realizing that dream will also create winners and losers.

But potential losers from technological innovation may well include cities as well as incumbent telecommunications carriers. The Sacramento region, for example, could lose jobs as VoIP is in the early stages of replacing call centers with *virtual* call centers that are geographically dispersed rather than centralized. There are many call center jobs in Sacramento's suburbs that could be lost in the conversion to this innovative service and new way of doing business.

Cities and regions should plan their strategic direction to cope with this turbulent future. The current Wi-Fi opportunity could be called the *tip of the innovation iceberg.* Cities that thrive in the future will be those that adapt their business practices, organizational structure, and economic and transportation initiatives to the capabilities of the emerging technologies. The future will belong to those who match organizational innovation to technological innovation.

Copyright Walter Siembab, January 2005