

22

Citywide Wireless: Process, Implementation, Execution and Privacy Issues

Steve Monahan and Danielle Shea

We are committed to bring universal, affordable wireless broadband Internet access to all San Francisco's residents and businesses, and today we are one step closer to making good on that commitment. Internet access is the best way to connect to the new knowledge-based economy. Providing that access citywide is the first phase of our TechConnect strategy to reach out to all of our communities.

--Mayor Gavin Newsom,
San Francisco

Across the nation, in coffee shops and small Internet boutiques, there is a growing trend of Wireless Fidelity (WiFi) usage. The airways are becoming increasingly populated by Internet signals going to and from hotspots to computers. People are no longer required to be behind their desk plugged into an Ethernet cord to access the Internet. The public is now able to sit in a Starbucks and log onto any site on the World Wide Web using their wireless enabled laptop. This is a convenience to people who can afford to pay the subscription fee associated with many of these hotspots. Additionally, cell phone companies are offering media access cards that plug into the serial port of a laptop and allow for Internet access over cellular connections. Through these services, people are able to use their computers in more locations with greater ease of use.

The latest trend in accessibility is for local governments and cities to offer large-scale WiFi access programs sponsored by the municipality. These programs are agreements between telecommunication companies and city governments that are designed to provide affordable Internet access to every citizen that wishes to participate. This accomplishes both a political goal of abolishing the "technology divide" between the "haves" and the "have-nots" and a general improvement to the daily lives of the inhabitants of the cities involved with this advancement in technology.

Practical Considerations of Municipal Wireless The Motivations Behind Citywide Networks

With technology reaching a point where large-scale networks are becoming feasible, many local governments are beginning to approach telecommunication companies and develop contracts with those providers to offer wireless Internet over the large areas of their city. Cities such as Orlando, Cupertino and Anaheim have already implemented these large wireless networks in sections of their metropolitan area. Larger cities, such as San Francisco, Houston, and Philadelphia, are currently under negotiations with telecommunication companies or have already developed contracts for wireless networks that cover the entirety of their cities and are currently in the process of installation and implementation.

No matter where this process is taking place, there is a common political thread: affordable Internet. This new system for Internet access would provide a tremendous opportunity for many underprivileged citizens who, under previous circumstances would not be able to afford Internet. This initiative is known as bridging the "technology divide." Due to the increasing speed that the Internet and the corresponding technology behind it is progressing, there is an increasing "divide" or discrepancy between the underprivileged who cannot afford the technology of today and those who can.

The Internet is becoming an increasing asset to those who have access to it. Enabling anyone to get information on anything they desire. It increases the awareness of the social, political and global situations that face humans every day, and it allows for tremendous learning and personal growth potential. By providing the Internet to those who would not otherwise be able to afford it, cities are doing their best to eliminate the "technology divide" and give the underprivileged an opportunity to have access to all of the great benefits of this ever-expanding resource.

In addition to providing the many underprivileged people with access to Internet, this citywide access concept has an additional positive impact on the businesses and people who live and work in these locations. People would have access to Internet on their commute to work, be able to take their computer to any activity that they desired and have connectivity. Businesses could improve their efficiency by having their employees be able to access work no matter where they were, in traffic, at company events outside the office or from their home office, and all of this at a much more reasonable cost than with options that are currently available.

The Political and Business Processes of Establishing Citywide Networks

After the desire and concept of developing a citywide network, there comes the challenge of finding a method to make the concept a reality. There are multiple models under which a citywide network can be developed and executed. Although there are multiple variations and infinite possibilities for minor deviation from the following, the basic options available to a city wishing to develop a citywide network are:

city-owned networks, single private owner, or multiple private owners. The following chart shows the different ownership and operation possibilities and the breakdown of how it works:

Table 1 - Municipal Wi-Fi business models

Who owns? / Who operates?	City	One private actor	Multiple others
City	Public utility	Hosted services	Public overlay
One Private actor	Wholesale	Franchise	Private overlay
Multiple others	Wholesale open platform	Common carrier	Organic mesh

Chart from Bar & Park

Under a city owned network, the original use for the network would be for specific city use (e.g. police authorities, firefighters, medical response units, city based utility operators and repair crews and other municipal employees). If the city decided to allow for public use, there would be several options. The first allows for the city to act as an Internet Service Provider (ISP) and manage the system itself. The second "...option is for the city to act as a wholesaler, reselling excess capacity in the network to a private operator, usually a telecom company or ISP" (Bar & Park 115). The final option would be for the city to act in a similar capacity to the previous example, but "...sell excess capacity to several ISP's, as an open platform" (Bar and Park 115). This last example would create a small market within the network with ISP's competing for subscribers at a certain price point.

A different ownership option for a citywide network is for a single private company to build, operate and maintain the physical network. With this type of ownership there are several options for the provision of the actual Internet service. The first is a city run ISP, with the city creating a telecom company and running through the municipality. No municipality has yet to consider this option as a viable opportunity. The second possibility is for a private company to buy the rights to the provision of services for the network and then directly sell subscriptions to customers. This would be similar to municipal telecom lines being operated by a cable or phone provider. The third option "...is theoretically possible but so far not implemented in practice, [and] would see the private network owner function as a common carrier, making its WiFi network available to multiple ISPs" (Bar & Park 117).

The third ownership option for a citywide network would be for cities to promote the construction of multiple networks by different companies. This would result in multiple different types of businesses and organizations constructing their own physical networks, with the cities' consent, and then the Internet being provided by one of the following options. The first would be a common public overlay that offers citywide accessibility and the individual networks would pay to be a member. The second possibility is a common private provider of Internet service to all networks in the city. The individuals using the

Internet (the public) would pay the ISP and then the ISP would pay the network based on volume of connection provided. The final option for the multiple network scenario would be multiple ISPs providing to multiple networks. This would be similar to the existing hotspot configuration, but on a larger scale, a network over an entire neighborhood, as opposed to just one retail outlet. This would also not provide the same continuity over the entire city that a single provider would allow for, thus, negating the effects of using this network on your commute or in different parts of the city.

With any of these different service provision options, the city plays a large role in ensuring that the original “technology divide” principals are made available. There needs to be an affordable option associated with all types of service so that the needs of underprivileged individual’s could and would be provided for.

The Physical Implementation of a Citywide Network

The technology behind a massive citywide network is not as advanced as one would anticipate. Once an agreement on how the physical network is to be established between the city and its chosen method of deployment, the process of construction would be relatively uniform.

To begin, the chosen contractor would mount wireless base stations on municipally owned property such as light posts, buildings and street signs. These base stations are technologically similar to the existing wireless routers that many people have in their home, but much more powerful. Not only are these base stations able to send out much stronger signals than their home office counterparts, but they are also able to process hundreds more incoming and outgoing signals at any given time. This allows for fewer base stations handling a greater volume of traffic, and thus, fewer of the units are needed. Even though the base stations are more powerful than those available to the everyday consumer, there still needs to be thousands of units dispersed in a large city.

Unfortunately, there is drawback with these base stations; they can only process the signals they receive. Almost all laptop computers created today come equipped with a wireless connectivity device built into the system. In many of these enabled computers, the unit receives the signal, but does not have much “pushing” signal strength. This “pushing” signal strength is what the connectivity device needs to send requests for information to the wireless base station. In a small office or home environment, this lack of pushing power does not represent a problem, as the base station is only meters away. In a large city, this lack of “pushing” power poses more of an issue. With buildings made out of concrete and steel, the different components of equipment in buildings and in the vehicles on the roads, there are many obstacles for the signal to get through to reach the desired base station. In order for people to successfully communicate with their desired base station they would need to purchase an additional device called a “bridge” which boosts outgoing signals and would cost roughly \$40 at a computer retailer. Anyone wishing to avoid timeouts and lag issues with their Internet will most likely need to purchase a bridge.

San Francisco, Earthlink, and Google: A Case Example

San Francisco, Earthlink and Google have recently entered into a contractual agreement for the provision of a citywide WiFi network. San Francisco asked for bids from a number of telecommunication companies and chose the proposal from Earthlink and Google. Under this agreement, Earthlink will provide the entire physical infrastructure associated with building, operating and maintaining the base stations and their connection to the ISP servers. "The Earthlink led consortium is expected to spend \$8 million to \$10 million to build the network in San Francisco" (Flynn).

There will be two options available to actually connect to the Internet through Earthlink's network, one provided by Earthlink and one provided by Google.

From Google, at no cost, [people] will be able to connect to the Internet at the modest speed of 300 kilobits a second, about six times as fast as a dial-up connection but slower than cable service. The trade-off is that they will see a variety of on-screen advertising, through exactly what that will look like is part of the negotiations (Flynn).

The other option is "...for an estimated \$20 a month, subscribers will be able to connect through Earthlink at roughly four times that speed [1.2 megabits per second] and see no advertising" (Flynn).

Earthlink is the ISP on other municipal wireless networks in Anaheim, Milpitas, and Philadelphia. This experience with other networks helped tip the scales in Earthlink's favor in the negotiations with San Francisco. This project is the first major implementation of Internet provision by Google. There are several groups that have stated concerns about the way that Google plans to provide free Internet over this new network. Due to the nature of how Google will create revenue through the free Internet, the usage of questionably invasive advertising, many people and groups are concerned with the privacy implications behind this service. Google would need to keep cookies on the computers of its subscribers to accurately pinpoint its advertising to the right type of consumer. It is also possible that Google would keep a record of websites visited by its subscribers within its own company database and reference the user's history to try and compile advertising to show to people as they surf the Web. This service has also been seen to company outsiders as a move by Google to "...move to expand well beyond search, into areas like local advertising and real estate listings" (Flynn). This has also been seen as a potential issue, as a conflict of interest on Google's part to maintain the privacy of their subscribers.

San Francisco has established a legal framework that is designed to protect the privacy of the individuals that subscribe to this service. The agreement between the City of San Francisco and Earthlink/Google has specific articles that protect the identity of subscribers, but that agreement is superceded by any need for the police to get information on you or by any authority acting under the provisions of the Patriot Act. There is nothing mentioned about the websites that the subscribers visit being logged and kept track of and nothing about to whom that consumer information can be sold.

Municipal Wireless Networks and the Implications on Privacy

There is no doubt about the benefits of a citywide WiFi network and providing that network at no cost to those who cannot afford or who wishes to not pay for the services. The connectivity possibilities of using the Internet on one's commute to work or away from the office, but still having the ability to access vital information on the go, is tremendous. Unfortunately, the amazing possibilities associated with citywide WiFi are overshadowed by cost that many people are unaware of. The cost of this free service in is often the loss of privacy.

Organizations Concerned with Privacy

There are several organizations that are leading a coalition to bring the potential privacy concerns with using public wireless networks. These organizations aim to inform people of what is happening behind the scenes in many of the companies that provide this new Internet accessibility frontier.

The American Civil Liberties Union (ACLU) is a group of concerned citizens of the United States that have come together to represent the civil rights of people who otherwise would have little to no representation in the government of this country. They are a nonprofit organization made of lobbyists and lawyers who fight for issues that they feel are underrepresented (American Civil Liberties Union).

The Electric Frontier Foundation (EFF) is a nonprofit organization that has dedicated its existence to defend the public's rights in the expanding and unpredictable technology sector. As technology progresses, there are increasingly more holes in the legal system that have no legal precedence, and thus, create opportunities for people to exploit those holes to their own advantage and often the disadvantage of people who are not protected by the law (Defending).

The Electric Privacy Information Center (EPIC) is a nonprofit organization that researches privacy issues in the face of new technologies as they present themselves to the public. They promote open government and raise awareness of potential privacy issues to the public (Electronic).

These three groups are spearheading an effort to ensure the privacy rights of the American public are protected in respect to citywide WiFi systems. The groups agree that the potential boons of these systems are great, but they want assurances from local governments and the companies that run the systems about the security of information that is communicated on and through their networks.

Due to the nature of how these citywide systems work, the ISP has many opportunities to collect private information on its customers. Even through a simple login name, a company is able to start a database of information on the user associated with that login. Every website that they connect to is recorded and stored on a database for later use by the company. There are no laws that prohibit companies from selling this information to anyone who desires to purchase it. In most circumstances, a login name is associated with a real name, a credit card, a phone number and a mailing address. With the sale of this information the private habits and consumer habits of the individual are

exposed. The privacy of this individual is now in the hands of the highest bidder to do what they wish with it (Joint).

Many companies, including Google, say any information that is collected is kept on the database for a limited amount of time and then deleted. They also state that the information is retained for intra-company use only. Despite this information, people who work for these companies are still able to access this data and use it as they please, or smuggle data out to sell to a third party. There are also security issues with outside hackers breaking into the system and gaining large quantities of data on hundreds of thousands of people.

The previously mentioned groups want to ensure that there are not only limits on what information companies are able to track and record, but additionally add requirements to what security they enable to protect the data. Part of the proposed concept to limit privacy leakage and increase security, is to allow usage of the free services without needing a login. This enables people to use the Internet with anonymity, prohibiting linking Internet habits to individuals. Where they go and what they do on the Internet can still be recorded, but there would be no link to a name and no clues other than the ones deduced from the Internet habits to their gender, age or socioeconomic status (Privacy).

Other concerns are the linkage of credit cards, and the associated data with those cards, to individuals. The networks that require payment for usage would need to retain billing information on individuals to keep their subscription current. Through this data they can gain insight to how that person lives and interacts with the World Wide Web. This data could be sold to marketers who would then target their marketing profile to certain individuals. Those people would then be at the mercy of marketers who have their own quotas to meet in regards to what they see on the Internet and what information they receive in their e-mail. The advocacy groups believe that people should not be targeted for marketing based on what websites they visit. People have a right to choose for themselves what they want to see in their e-mail inbox and what advertising they see on a day to day basis (Joint).

It is important to consider that some information will need to be collected for certain activities. People who pay for premium service would need to maintain a profile with the ISP to ensure their continued access to what they paid for. Under the Patriot Act, any power that has the authorization necessary would be able to gain access to this data and use it in an investigation. Additionally, police agencies also have authority to use this data under special circumstances. Even if someone is investigated for another crime, their habits on the Internet coming to the attention of police agencies could lead to potential problems in the future. The ISP retaining this info is very dangerous in the hands of the wrong individuals.

Conclusions

Being that Municipal Wireless is such a new and growing trend within the United States, it is not surprising that there are still many issues that need to be worked through to make it a beneficial advancement in technology. As stated before, there are two main questions that need to be answered for citizens to feel secure on a Municipal WiFi network. "How will the network protect consumer

privacy and how will the network protect information transmitted by users" (Joint)? Cities have attempted to answer these questions as thoroughly as possible but there are still issues to be worked out.

One of the largest concerns for those who doubt Municipal Wireless Systems stems from legal pressure. Agencies such as the ACLE, EFF and EPIC have asked how the ISP will deal with legal demands for user's personal information. There is no question that this issue will arise in lawsuits involving the Internet and its abuse by users. It has been stated that those "who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identities" (Joint). From past cases, it has been noted that the service provider is the first person the courts will go to for information regarding Internet and its misuse. The users of Municipal WiFi need to be certain that the ISP protects their privacy. Protection begins with immediate notification of a court subpoena for user activity. The service provider also needs to be weary of giving out personal information to the courts in cases where it is unnecessary and unjust (Joint).

Another unanswered question regards the information transmitted by the users. In order for people to feel secure about using the WiFi system, they need to be certain that hackers cannot intercept information transmitted across the Internet. If users do not have this sense of security, then there is absolutely no point in Municipal WiFi because it will not benefit users who wish to access their bank accounts and medical records online.

Municipal WiFi is a technology that will benefit not only the underprivileged of our nation's cities who cannot afford Internet, but also will provide a convenience for the rest of the community. Municipal WiFi is still a fairly new advancement that leaves many questions unanswered. There is no doubt cities will have to continually improve the technology and its security in order to protect the users' privacy. This is the way of the future, and it will be deployed more and more in the United States as well as internationally.

Works Cited

- "A Privacy Analysis of the Six Proposals for San Francisco Municipal Broadband." Eric.ORG. 5 April 2006. <<http://www.epic.org/privacy/internet/sfan4306.html>>.
- Bar, Francios and Park, Namkee. "Municipal WiFi Networks: The Goals, Practices, and Policy Implications of the U.S. Case. *First Transatlantic Telecom Forum*. 22 November, 2005.
- Flynn, Laura. "Some Worries as San Francisco Goes Wireless." *New York Times* 10 April 2006.
- "Joint Letter on San Francisco Wireless Internet Access." www.epic.org 19 October 2005. <<http://www.epic.org/privacy/internet/sfws10.19.05.html>>.
- American Civil Liberties Union. 15 March 2007. <www.ACLU.com>.

Defending Freedom in the Digital World. Electronic Frontier Foundation. 15 March 2007. < www.Eff.org. >.
Electronic Privacy Information Center. 15 March 2007.
<www.EPIC.org>.