JOURNAL OF INTERNET LAW
VOLUME 14
NUMBER 2
ASPEN PUBLISHERS
AUGUST 2010
EDITED BY DLA PIPER

A Postmortem Look at Citywide WiFi

By Eric M. Fraser

In March 2010, the Federal Communications Commission (FCC) released *Connecting America: The National Broadband Plan*. The National Broaband Plan is a set of goals and recommendations for broadening the availability of access to broadband Internet and increasing the speed of access. It references WiFi in only five of its 375 pages, describing it as an "important complement[] to licensed mobile networks and to fixed wireline networks."[1] This is a big change from the treatment that WiFi got in the Federal Trade Commission's 2006 report, *Municipal Provision of Wireless Internet*,[2] which listed WiFi first in its list of major technologies used to provide citywide wireless internet access. WiFi was demoted in the intervening four years because of the sensible realization that WiFi has no place in providing wide-area Internet access.

Almost everyone was fooled by the promise of citywide WiFi. Beginning in the early 2000s, more than 100 municipalities bought into the dream of providing cheap or free Internet access throughout the city using the same technology that residents were already using to unwire homes and businesses. Municipalities dreamed of residents connecting to the Internet while sitting on a park bench, on a couch, in an office, or in a car. Local governments would be able to install Internet-connected parking meters and high-speed Internet access emergency vehicles. Low-income families would be able to connect to the Internet for the first time, bridging the digital divide. That was the dream. Crews began installing WiFi hotspots in City Halls and on top of lampposts.

By the end of the decade that dream died as everyone involved realized that WiFi could not realistically be expected to provide citywide Internet access. To be sure, the importance of WiFi has only grown over the last decade. Many people are fortunate to have WiFi access where they work, live, and travel. It is even available in airplanes and on boats. It cannot, however, blanket Los Angeles.

Many technical, regulatory, and commercial factors worked together to prevent the success of

Continued on page 7

Eric M. Fraser is the Executive Director for Research at the Committee on Capital Markets Regulation. *This article is condensed and adapted with permission from the* Journal of Technology Law & Policy *© 2009. See Eric M. Fraser, "The Failure of Public WiFi," 14 J.* Tech. L. & Pol'y *161 (2009).*

IN THIS ISSUE

Wolters Kluwer
Law & Business

A Postmortem Look at Citywide WiFi
Continued from page 1

citywide WiFi. Too few users would use the limited wireless network that a city can realistically provide. In areas where the public WiFi network would operate exclusively, the user experience is inadequate. Where the public WiFi network would be absent or would overlap existing networks, users have better options. Cities and private partners could never hope to recover high fixed build-out costs and marginal operating costs from the limited networks that WiFi allows. This article explains why.

PUBLIC WIFI MODEL

Public WiFi was supposed to be a "wireless fantasy land."[3] Independent market research firms, expressly claiming to be free of "a simple 'me-too' mentality," predicted that citywide WiFi would generate value for "citizens, government, and local businesses."[4] Above all, public WiFi was supposed to solve the "last mile" problem. The last mile is the connection between a house or apartment and the local hub that links a much larger local area. Unlike the other connections in a network, the costs of the last mile cannot be distributed among large groups of users. Each house or apartment must be connected to a larger network; establishing the connection often involves the expensive process of digging trenches along streets and through yards or stringing cables between poles. With no wires, WiFi should avoid the costs of the last mile entirely because many users can share access from one access point.

Because of these grand possibilities, public WiFi captured the attention of municipalities across the country. Philadelphia, San Francisco, and Chicago initially launched high-profile efforts;[5] eventually, more than 200 municipalities in the United States announced plans for citywide or countywide public WiFi.[6] Different cities adopted different business models, from publicly owned and operated to semi-priviate networks. Some involved local subsidies, some would be supported by advertising, and some would require payment.[7]

REGULATORY FRAMEWORK

Several different regulatory regimes govern various aspects of public WiFi. First, the FCC regulates the radio spectrum. Various private parties have licenses to operate equipment using different slices of the spectrum. The FCC also established some slices that do not require licenses; in these slices, devices must simply conform to a few restrictions on frequency, power output, and noninterference but are otherwise unrestricted.[8] Next, the Pole Attachments Act[9] may provide statutory authority to use utility poles for public WiFi, at least in conjunction with a private company.[10] If so, then the FCC may aid municipalities in using utility poles as access point mounting locations if the municipality partners with a telecommunications provider that provides, for example, cable television services in addition to Internet access.[11]

There are also local regulations. Under pressure from telecommunications companies, several states have passed laws restricting public WiFi. Pennsylvania's 2004 H.B. 30 has received the most attention. It effectively gives local incumbent telecommunications companies a right of first refusal if a municipality wants to offer public WiFi.[12] Colorado, Nebraska, and others have also passed laws regulating public WiFi.[13]

TECHNICAL AND REGULATORY LIMITATIONS OF WIFI

WiFi sends information via radio waves, but radio signals at a receiver do not match perfectly those at the transmitter. Various properties of radio waves attenuate, or dampen, the signal as it propagates. Even in completely free space, a receiver far from the transmitter will receive a signal weaker than a receiver close to the transmitter because of the physical concept known as free-space propagation. The signal degrades nonlinearly; the signal strength is inversely proportional to the square of the distance from the receiver.

Interference from obstacles and other wireless signals further degrades the signal. Users of mobile phones or GPS devices who have lost signal in a tunnel are familiar with obstacles severely attenuating radio signals. Various physical forces, including reflection, transmission, diffraction, and scattering, dampen signals when an object comes between the transmitter and the receiver. The level of attenuation is a complex interaction between the wave's frequency and the obstacle's composition, surface,

and design. For signals like WiFi, ordinary objects such as walls, windows, furniture, cars, and trees can significantly attenuate a signal. For these types of objects, lower-frequency (longer wavelength) signals are generally less susceptible to interference.[14] Other radio signals, particularly those operating near the same frequency, can destructively interfere with a signal. Think of this phenomenon as the one driving noise-cancelling headphones. If one signal takes the exact opposite form of another signal, the two sum together to cancel out each other. Interference is a problem even when signals are not exactly the same because, if even very small, short sections overlap in places, those parts of the signal can cause data loss. To complicate things even more, a signal can even interfere with itself if obstacles bend a signal through diffraction and reflection. These limitations are particularly severe for WiFi because it is unlicensed and operates at a non-ideal frequency.

In 1985, the FCC acted to allow certain unlicensed transmissions.[15] This action paved the way for the introduction and widespread adoption of WiFi a decade later. The change in regulation allowed for the transmission of signals, within certain guidelines, without an operator license. Part 15 of the FCC regulations limits these unlicensed transmissions to 900 MHz, 2.4 GHz, or 5 GHz.[16] WiFi generally operates at only two of those frequencies, 2.4 GHz and 5 GHz, due to issues with international standards.

Signal attenuation from obstacles, however, depends on frequency. Selecting an ideal frequency involves considering many factors, but lower frequencies typically reduce attenuation from everyday objects. Compare these WiFi frequencies to the lower frequencies used by many technologies that typically experience less signal loss from everyday objects: 1-2 kHz for AM radio and 30 MHz-300 MHz for FM radio and VHF television, all of which can penetrate cars and homes to deliver radio and television signals.[17] With WiFi constrained to these non-ideal frequencies, the signal significantly degrades when passing through trees, cars, walls, windows, and household furniture.

Although the specific available frequencies cause problems, the mere limitation of frequencies and the lack of a license requirement together lead to interference-causing traffic congestion. WiFi may operate only in two frequency bands. Other electronic devices may operate in these bands as well. Buyers of portable telephones (not cellular phones) will recognize that portable phones are available in these frequencies, as are baby monitors and many other wireless devices. Commercial wireless operators with licensed and assigned spectrum slices design and manage networks in order to minimize interference from other devices. The *ad hoc* nature of the unlicensed frequencies, however, allows anyone to install a device that could interfere with a public WiFi project.[18] Just as a neighbor's baby monitor can knock out a home network, unknowing residents could plug in legitimate devices that could wreak havoc on a municipal network.

The FCC restricts not only frequency but also power output. Specifically, it restricts peak output power to 1 watt.[19] That one watt degrades from free-space propagation, obstacles, and signal interference. Consider a message sent using Morse Code in flashes of light from a small flashlight with a weak battery. Free-space propagation would make it difficult to detect the message from a mile away. Viewing the signal from behind an obstacle like tinted glass would further diminish the signal. And a car's headlights would interfere with the signal. Now imagine that the sender replaced the batteries with fresh batteries, increasing the power of the light output. Or imagine that the sender replaced the flashlight with airport landing lights or searchlights. Now the signal should be clearly visible a mile away in open air, and it will probably still be visible even though the obstacle of tinted glass and over a car's headlights. In short, if the power of a signal is strong enough, the receiver can still understand the message even if several physical phenomena attenuate the signal.

Although signals of different formats and frequencies do not compare directly, consider that television stations typically broadcast at powers four to six orders of magnitude larger—between 20 kW and 5,000 kW for the major networks in Chicago, for example.[20] Users of any of the typical unlicensed devices know that one cannot venture far from the base station before losing the signal, particularly with other signals present in an indoor setting. One watt simply cannot overcome the physical properties acting against the signal at those frequencies.

These three factors—imperfect frequency, congestion within the frequency bands, and limited signal strength—combine to require high-density installations. As a rough guide, to blanket an area with coverage no point should be more than a few

hundred feet from an access point. In environments with obstacles and interference, the signal will not propagate as far, requiring even higher density.

Installing access points is a high-touch activity. Each access point must physically be mounted somewhere, and a worker must secure it to prevent theft. Each access point also needs power, at a minimum, and maybe even a wired network connection.[21] In large open spaces, blanketing the area with WiFi signal requires many access points. A municipality may be able to provide outdoor access quite effectively if workers can mount access points on existing infrastructure. In public parks, for example, lampposts could double as access points if they are dense enough. Along streets, utility poles could serve the same function, particularly if the Pole Act allows the FCC to help pave the way. Indoor settings, however, require higher-density installations. Obstacles such as walls and furniture will significantly limit the signal. Private ownership of buildings naturally makes high-density, high-touch installations difficult. Even if building owners were willing to allow public WiFi access point installations,[22] the coordination and expense involved would make it almost impossible. Installations would require running cables, drilling, permanently mounting equipment, and, perhaps most troubling to many business owners, nearly complete access to the inside of buildings because of the high density required.

TECHNICAL ALTERNATIVES

Several different technologies exist that can provide wireless Internet more effectively. For example, 3G and 4G cellular networks and WiMax can all provide high-speed access at longer ranges than WiFi. To overcome the wireless challenges outlined above, these alternative technologies use higher power output levels, lower frequency bands, or both. But to do so in the United States, they must use licensed spectrum bands. Higher power and lower frequency allow signals to go farther and penetrate more structures with less signal loss. Additionally, using licensed frequencies reduces interference because it allows for coordination of such things as transmitter placement.

Even though alternatives may have technical advantages over WiFi, network effects from WiFi's popularity probably caused municipalities and their partners to opt for a WiFi network.[23] First, after Apple introduced its iBook laptop with built-in WiFi (called Airport) in 1999, many consumer and business portables gained built-in WiFi cards. Because potential users already have WiFi-ready equipment, municipalities can offer public wireless Internet access through WiFi without requiring users to purchase new equipment. This network effect from compatibility reduces startup costs for users and speeds adoption. In addition, the proliferation of WiFi technologies in homes and businesses created economies of scale for production, competition in the marketplace, and widespread availability of compatible hardware equipment. WiMax was still too new to have the benefit of reduced costs from economies of scale; the limited market and FCC licensing issues surrounding 3G and 4G technologies prevented widespread availability.

SUCCESSFUL PUBLIC WIFI: LIMITED SCOPE AND SCALE

Despite these problems, public WiFi has been successful in certain situations. Successful networks all have limited scale. Enabling public WiFi in government buildings such as libraries may be very valuable because at most it duplicates the 3G networks, but no other private networks, and because the ratio of expected users to the cost of installation in a single building probably far exceeds that of a citywide deployment. Municipalities also offer the valuable service of offering public WiFi in schools, high-trafficked public parks, and other public areas.

Additionally, many small, rural municipalities have found success deploying public WiFi. First, in many rural areas high-speed Internet access is not widely available. Home and small business customers may not have access from cable companies, telephone companies, or even 3G wireless providers. With no alternatives, public WiFi may be attractive and efficient even with its limitations. In addition, if a small municipality wants to use WiFi to extend access to only a few locations, then it can use directional equipment instead of omnidirectional equipment. In other words, it can aim the signal at a particular point instead of blasting the signal in all directions. This reduces the signal drop from free-space propagation described above. Finally, in rural areas fewer obstacles and maybe even fewer interference-causing devices degrade the signal less than in highly developed urban areas.

CONCLUSION

Public WiFi was supposed to solve many problems, from the digital divide to the modernization of public safety forces. Large and small cities all over the country partnered with major companies. Proponents of public WiFi thought that if they built it then users would come. But municipalities could not build the networks as promised, and users had little reason to come to the limited networks that they delivered.

WiFi cannot deliver a citywide network because technical and regulatory limitations combine to require access points at least every few hundred feet outside and even closer together indoors. Mounting that many access points is generally too expensive and is nearly impossible inside private buildings. WiFi deployments require high-touch, high-density installations. Meanwhile, users often have WiFi access in homes, at work, at coffee shops, in hotels and airports, and in select government buildings. For users who require wireless access outside those areas, private cellular companies offer high-speed 3G wireless data networks using technologies better suited for widespread coverage (because of not only technical differences but also regulatory differences). As a result, the major public WiFi projects were destined for failure and municipalities instead should devote resources to small, focused networks.

NOTES

1. Federal Communications Commission, *Connecting America: The National Broadband Plan*, available at *www.broadband.gov*, at 77 (Mar. 2010).
2. Available at *http://www.ftc.gov/os/2006/10/V060021municipalprovwirelessinternet.pdf*.
3. Adam L. Penenberg, "The Fight over Wireless," *Slate* (Oct. 24, 2005), *http://www.slate.com/id/2128632* (describing established telecommunications companies' resistance to municipal wireless Internet access initiatives).
4. Sally M. Cohen, "Monetizing Municipal Wireless Networks," Forrester Research (July 23, 2007) (highlighting the various opportunities for all players to benefit from public WiFi).
5. *See, e.g.,* Wendy Tanaka, "Philadelphia Near Goal to Be the First Wireless Major City," *Philadelphia Inquirer*, Oct. 30, 2004 (Philadelphia); Verne Kopytoff, "Free Wireless Access in S.F. a Step Closer: Google, Earthlink Sign Pact with City to Operate Network," *S.F. Chronicle*, Jan. 6, 2007, at A1 (San Francisco); Jon Van, "It's a Wi-Fi Kind of Town: Chicago Seeks Proposals for Citywide Internet Access," *Chi. Tribune*, Feb. 17, 2006, at A1 (Chicago).
6. See MuniWireless.com, List of US Cities and Counties with WiFi (2007), *http://www.muniwireless.com/reports/docs/Aug-1-2007summary.pdf*.
7. For a detailed description of the various business options, *see* François Bar & Namkee Park, "Municipal Wi-Fi Networks: The Goals, Practices, and Policy Implications of the U.S. Case," 61 *Comm. & Strat.* 107, 113-119 (2006)
8. *See* 47 C.F.R. § 15.126 (1985).
9. 47 U.S.C. § 224 (2000).
10. The FCC may have regulatory authority over wireless internet access points mounted on utility poles. *Seeid.*; Nat'l Cable & Telecomm. Ass'n, Inc. v. Gulf Power Co., 534 U.S. 327, 339-341 (2002) (deferring to FCC's interpretation of Pole Attachments Act that purely wireless equipment may be an attachment) (citing Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984)); 47 U.S.C. §§ 153(46), 153(43) (definitions of "telecommunications service" and "telecommunications"). *But see* 47 U.S.C. § 153(20) (definition of "information service"); In re Inquiry Concerning High-Speed Access to Internet Over Cable and Other Facilities, 15 F.C.C.R. 19287, 19294 (2000) (inviting comment on the classification of internet service); *See* Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Serv., 545 U.S. 967, 1000 (2005) (deferring to FCC on classification of internet). The FCC may revisit the issue after the D.C. Circuit's decision in Comcast Corp. v. FCC, 600 F.3d 642 (2010).
11. Note, however, that projects may still face significant hurdles to gaining access to poles. *See, e.g.*, Jennifer Chambers, "Utility Pole Access Delays $100M Wi-Fi Project," *Detroit News*, Apr. 21, 2006, at 3B (Oakland County ed.) ("Plans to blanket all 910 square miles of Oakland County with wireless Internet are at a standstill after the firm in charge of the project found it needs 20,000 additional access points to get the system running. . . . 'Each pole must be permitted. DTE [Energy] said we have to identify the pole, send the information to them. They have to send someone out to look at the pole.'").
12. *See* H.B. 30, 2003-04 Sess. (Pa. 2004), codified in 66 Pa. Code § 3014. In order to accommodate Philadelphia's then-active plans to bring public WiFi to the city, however, Pennsylvania legislators compromised and allowed Philadelphia to continue what it had started. *Seeid.* at § 3014(h)(3).
13. *See* Colo. Rev. Stat. § 29-27-101 to §29-27-304 (2006); Neb. Rev. Stat. § 86-593 to §86-599 (2006).
14. *See* H. Sizun, Radio Wave Propagation for Telecommunication Applications, 1-2 (Springer 2004); Thomas A. Moore, Six Ideas that Shaped Physics: Unit E: Electric and Magnetic Fields Are Unified, Chapter E16 (2d ed., McGraw-Hill 2002).
15. *See* In re Authorization of Spread Spectrum and other Wideband Emissions not Presently Provided for in the FCC Rules and Regulations, 101 F.C.C.2d 419 (May 24, 1985) ("The Commission proposes to accommodate spread spectrum systems by reducing regulation to the maximum extent feasible. The Commission believes that such action will lead to a more rapid development of spread spectrum technology in the civilian sector."), codified in 47 C.F.R. Parts 2, 15, 90 (1985).
16. *See* 47 C.F.R. § 15.126 (1985). Note that for worldwide compatibility, 2.4 GHz and 5 GHz frequencies are typically unlicensed in many parts of the world, while 900 MHz is only unlicensed in a few regions, including the United States.
17. For a complete picture of spectrum allocation in the United States, *see* U.S. Department of Commerce, "United States Frequency Allocations: The Radio Spectrum" (Oct. 2003), available at *http://www.ntia.doc.gov/osmhome/allochrt.pdf*.
18. As residents in high-density apartment complexes know, transaction costs cause bargaining failures so coordination between users of WiFi, portable phones, baby monitors, and other devices rarely occurs. Transaction costs include identifying the owners of offending equipment, coordinating channel assignments, the technical challenges involved in reducing interference, and general neighborly issues. *Cf.* R.H. Coase, "The Problem of Social Cost," 3 *J. L. & Econ.* 1 (1960) (introducing what is now known as the Coase Theorem). Note also that while the FCC regulation

specifically prohibits unlicensed devices from interfering with the signals from *licensed* operations, it remains silent on interfering with other unlicensed operations. *See* 47 C.F.R. § 15.126(c) (1985).

19. *See* 47 C.F.R. § 15.126(a) (1985).
20. *See* Station Index, *Chicago*, *http://www.stationindex.com/tv/markets/Chicago* (2008) (listing output power of Chicago television stations).
21. With "mesh" networks, access points wirelessly share network connectivity with each other, so a signal from an initial wired connection bounces from wireless access point to wireless access point before finally reaching the user. *See* Ian F. Akyildiz, Xudong Wang, & Weilin Wang, "Wireless Mesh Networks: A Survey," 47 *Comp. Netw. & ISDN Sys.* 445 (2005) (detailing wireless mesh network deployments). But of course at least one access point must be connected to the internet and in practice many must connect directly to the internet to maintain performance, stability, and reliability. *See id.*
22. Cooperation with building owners, rather than mandating installations, is probably the only way to accomplish public WiFi installations. Among many other problems with requiring installations, such requirements would probably be considered takings. *See* Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419 (1982) (holding that a law requiring building owners to permit cable television wire installation is a taking on the grounds that the law enables a permanent physical occupation of property).
23. For a general analysis of these systems-based network effects, *see* Michael L. Katz & Carl Shapiro, "Systems Competition and Network Effects," 8 *J. Econ. Persp.* 93 (1994).