Journal of Technology Law & Policy

Volume 14 | Issue 2 Article 2

December 2009

The Failure of Public WiFi

Eric M. Fraser

THE FAILURE OF PUBLIC WIFI

Eric M. Fraser[*]

* Law Clerk, U.S. Court of Appeals for the District of Columbia Circuit (2009 term); J.D., University of Chicago Law School (2009); M.B.A., Economics, University of Chicago Booth School of Business (2009); B.A., Physics, Pomona College (2005). This research was generously sponsored by the John M. Olin Program in Law and Economics at the University of Chicago Law School. Special thanks to Douglas Lichtman, UCLA School of Law, and Marc Berejka, Microsoft Corp., for helpful feedback in the early stages of this Article.

I. INTRODUCTION

Public WiFi[1] was supposed to be the next big thing in connectivity. Residents were supposed to be able to connect to the Internet sitting anywhere, such as on a park bench, on a couch, in an office, or in a car. Some municipalities would even offer this access for free. Local governments would install Internet-connected parking meters, high-speed Internet access in police squad cars and fire trucks, and paperless court systems. Low-income families would be able to connect to the Internet for the first time. Tourists, including conference attendees, would be able to connect to the Internet not just in convention centers and hotels, but anywhere.

More than one hundred municipalities bought into this dream. Dozens signed agreements with major companies to build and operate public WiFi networks. Crews began installing WiFi hotspots in city halls and on top of lampposts. Then, in 2007, the dream died as the major public WiFi projects collapsed. This Article explains why.

Many technical, regulatory, and commercial factors on both the supply side and the demand side worked together to prevent the success of public WiFi. WiFi, given its technical and regulatory limitations, cannot realistically unwire an entire city. Too few users would use the limited wireless network that cities can realistically provide. In areas where the public WiFi network operates exclusively, the user experience proves inadequate. Where the public WiFi network is absent or overlaps existing networks, users often have superior options. Municipalities and private partners could never hope to recover high fixed buildout costs and marginal operating costs from the limited networks WiFi allows.

This Article proceeds in four parts. Part II explains the public WiFi model, including its promise, various business model choices, and the existing regulatory framework. Part III dives into wave physics to lay the foundation for WiFi's technical limitations. It explains first how waves propagate in free space, then how waves interact with obstacles and other waves. Part IV, the bulk of the Article, explores the failure of public WiFi projects. It asserts that the technical and regulatory issues described earlier limit the network's feasible scope and the user experience. It also describes how competition to public WiFi projects nearly destroys the market for public WiFi. Finally, Part V explains how and why some limited-scope projects may be successful.

---

1. WiFi is also commonly hyphenated as Wi-Fi, referred to by standard number IEEE 802.11b (or 802.11a, n, g, and others), or called various commercial names such as AirPort by Apple. For more, *see generally A Brief History of Wi-Fi*, ECONOMIST, June 10, 2004, at 27. This Article uses the term public WiFi, while others use terms like municipal wireless Internet or muni-WiFi.

II. PUBLIC WIFI MODEL

A. The Promise of Public WiFi

Public WiFi was supposed to be a "wireless fantasy land."[2] Independent market research firms, expressly claiming to be free of "a simple 'me-too' mentality," predicted that public WiFi would generate value for "citizens, government, and local businesses."[3] In addition to traditional consumer Internet activities such as web browsing, online shopping, and email, public WiFi was supposed to bridge the "digital divide" between those who have access to technology and those who do not. Municipalities, the networks' anchor tenants, were to use public WiFi for first responders, field workers, and even parking and utility meters. Local businesses could draw in customers with public WiFi and allow employees and clients to work untethered.[4]

Above all, public WiFi was supposed to solve the "last mile" problem. The last mile is the link between an individual user and the broader network. The last mile typically costs more per user than other legs of the network because the costs of running and maintaining that leg may be allocated to only one user, or at most a household or business.[5] Many users, in contrast, may share the costs of other legs of the network.[6] For example, in a residence the last mile describes the connection from the house to the street or local hub.

With no wires, WiFi should avoid the costs of the last mile entirely. Many users can share access from one access point. Anyone who has set up a home WiFi system should understand this principle. To expand Internet access to many rooms in a house, installing a WiFi system may be easier than running Ethernet cables through walls and around furniture. Deployment of telephone technologies in emerging markets seems to support this idea. In many emerging markets, a person's first

---

2. 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).

3. Sally M. Cohen, *Monetizing Municipal Wireless Networks*, FORRESTER RESEARCH, July 23, 2007, at 2 (highlighting the various opportunities for all players to benefit from public WiFi).

4. *See* Sharon E. Gillett, *Municipal Wireless Broadband: Hype or Harbinger?*, 79 S. CAL. L. REV. 561, 569–71 (2006) (explaining public safety and other government uses for public WiFi); François Bar & Namkee Park, *Municipal Wi-Fi Networks: The Goals, Practices, and Policy Implications of the U.S. Case*, 61 COMM. & STRAT. 107, 111 (2006) (explaining various motivations for public WiFi).

5. *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 398–99 (Yale Univ. Press 2007) (tangentially explaining the last mile).

6. *Id.*

telephone is often a mobile phone because deploying mobile networks may be faster and less expensive.[7] Wireless technologies seem like the perfect solution to the last mile problem.

Due to these grand possibilities, public WiFi captured the attention of municipalities across the country. Philadelphia, San Francisco, and Chicago initially launched high-profile efforts;[8] eventually, more than two hundred municipalities in the United States announced plans for citywide or countywide public WiFi.[9]

B. *The Business Model of Public WiFi*

A municipality could use any one of several different business models to provide public WiFi. The variables in the business model include, among other things, the owner, operator, and financier of the network. François Bar and Namkee Park provided a useful framework, depicted below in Table 1, for the first two variables, ownership and operation.

Ownership / Operation	**Municipality**	**Single private actor**	**Multiple actors**
Municipality	Public utility	Hosted services	Public overlay
Single private actor	Wholesale	Franchise	Private overlay
Multiple actors	Wholesale open platform	Common carrier	Organic mesh

Table 1: Ownership/operation matrix[10]

7. *Cf.* Jacqueline Hamilton, *Are Main Lines and Mobile Phones Substitutes or Complements?: Evidence from Africa*, 27 TELECOMM. POL'Y 109, 111 (2003) ("For instance, cellular phones may be an attractive alternative where it is difficult to install fixed-line networks.").

8. *See, e.g.*, Wendy Tanaka, *Philadelphia Near Goal to Be the First Wireless Major City*, PHILA. INQUIRER, Oct. 30, 2004, at D01; Verne Kopytoff, *Free Wireless Access in S.F. a Step Closer: Google, Earthlink Sign Pact with City to Operate Network*, S.F. CHRON., Jan. 6, 2007, at A1; Jon Van, *It's a Wi-Fi Kind of Town: Chicago Seeks Proposals for Citywide Internet Access*, CHI. TRIB., Feb. 17, 2006, at C1.

9. *See* MuniWireless.com, *List of US Cities and Counties with WiFi* (2007), http://www.muni wireless.com/reports/docs/Aug-1-2007summary.pdf.

10. Excerpted from Bar & Park, *supra* note 4, at 114.

Table 1 explains the primary ownership/operating models, with either the municipality, a single private actor, or multiple actors owning or operating the network. On one extreme is municipality ownership and operation, in which the service becomes a utility like a public water service in small cities. On the other end is an organic mesh network where residents and businesses add to the network and the municipality primarily provides incentives to expand the network and to install access points in municipal buildings. Most announced public WiFi agreements take the form of franchise, wholesale, or wholesale open platform. Under these arrangements, a municipality would cooperate with one or more private actors who would operate or own the network.[11]

Municipalities must also decide who will pay for the service. Again, municipalities have several options. A municipality may offer it as an unsubsidized service, a partially subsidized service, a fully subsidized service, or a service supported partially or fully by advertising. Different agreements have used each of these forms. In Philadelphia, for example, residents paid for service, with the city subsidizing part of the cost for those with low income.[12] In libraries, patrons may often use WiFi free of charge. In San Francisco, Google and Earthlink planned to recover some costs through advertising.[13]

These decisions largely come down to public choice. Regardless of the choices, someone must pay to build the network, maintain the network, and offer service. Total payments from the municipality, users, and advertisers must exceed fixed costs and marginal costs over some period of time in order to survive.

C. *Regulatory Framework*

Several different regulatory regimes govern various aspects of public WiFi. Randal Picker has already addressed the question of who should regulate entry,[14] and the FCC has created a task force to explore the issue.[15] Rather than looking to the future, this section explores current

---

11. For a more complete analysis of each model and the implications of the choices, see *id.* at 113–19.

12. Tanaka, *supra* note 8.

13. Kopytoof, *supra* note 8.

14. *See generally* Randal C. Picker, *Who Should Regulate Entry into IPTV and Municipal Wireless?* (Chicago: John M. Olin Law & Econ. Working Paper No. 308, 2d Series, 2006).

15. *See* Press Release, FCC, FCC Chairman Michael K. Powell Announces Formation of Wireless Broadband Access Task Force (May 5, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-246852A1.pdf; *see also* FCC, *Wireless Broadband Access Task Force*, http://www.fcc.gov/wbatf (2005). Note that the Task Force's website has not been updated since March 2005.

regulatory regimes, including FCC regulations, the Pole Attachments Act, and state laws regulating public WiFi.

First, the FCC regulates the radio spectrum. Various private parties receive licenses to operate equipment using different parts 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 and power output.[16] Part IV.A.1 explains how WiFi makes use of this unlicensed spectrum.

Next, the Pole Attachments Act[17] may provide statutory authority to use utility poles for public WiFi. The Pole Attachments Act provides that the FCC may regulate "pole attachments."[18] The definitions subsection of the Pole Attachments Act defines "pole attachment" as "any attachment by a . . . provider of telecommunications service to a pole . . . controlled by a utility."[19] If a wireless Internet access point is an attachment under the Act, and if a company providing wireless Internet is a "provider of telecommunications service" under the Act, then the FCC has regulatory authority over wireless Internet access points mounted on utility poles.

The Supreme Court has answered the first question. Even purely wireless equipment may be an "attachment" under the Act because of an FCC interpretation reasoning that wireless equipment falls under "associated equipment."[20] The statute defines the term "telecommunications service" as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used."[21] The same section also defines "telecommunications" as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."[22]

But another section of the Code includes a separate definition for "information service,"[23] distinguishing telecommunications service from information service. Although the Supreme Court has not addressed the issue of the classification of Internet service, neither the Eleventh Circuit nor the FCC consider Internet service a

16. *See* 47 C.F.R. § 15.126 (1985); *see also* Part V.A.1, *infra*.

17. 47 U.S.C. § 224 (2000).

18. *See id.*

19. *Id.*

20. *See* Nat'l Cable & Telecomm. Ass'n, Inc. v. Gulf Power Co., 534 U.S. 327, 339–41 (2002) (deferring to FCC's interpretation of Pole Attachments Act that purely wireless equipment may be an attachment). The Court deferred to the FCC based on its holding in *Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837 (1984).

21. 47 U.S.C. § 153(46) (2000).

22. 47 U.S.C. § 153(43).

23. 47 U.S.C. § 153(20).

telecommunications service.[24] The FCC has suggested that it is willing to reconsider the classification,[25] but it has not yet changed the classification. In fact, the Supreme Court again confirmed that the FCC does not consider Internet access a telecommunications service because that chapter of the Code has a separate definition for information services.[26]

In short, the FCC may aid a municipality in using utility poles as access point mounting locations if the municipality partners with a telecommunications provider that provides, for example, cable television services as well as Internet access.[27]

Finally, 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.[28] Colorado, Nebraska, and

---

24. *Nat'l Cable*, 534 U.S. at 336–38 (citing *In re Implementation of section 703(e) of the Telecommunications Act of 1996*, 13 F.C.C.R. 6777, 6794-95 (1998)).

25. *See 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 issue).

26. *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).

27. 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.

> 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."

Id.

28. *See* H.B. 30, 2003–04 Sess. (Pa. 2004), codified in 66 PA. CODE § 3014. Specifically, the statute states that:

> a political subdivision or any entity established by a political subdivision may not provide to the public for compensation any telecommunications services, including advanced and broadband services, within the service territory of a local exchange telecommunications company operating under a network modernization plan, [unless] . . . the political subdivision has submitted a written request for the deployment of such service to the local exchange telecommunications company serving the area and, within two months of receipt of the request, the local exchange telecommunications company or one of its affiliates has not agreed to provide the data speeds requested.

66 PA. CODE § 3014(h) (2006).

others have also passed laws regulating public WiFi.[29]

No regulation governs all of public WiFi. In fact, most of the applicable regulations were passed long before WiFi existed. Although some commentators debated whether state or federal officials should regulate public WiFi, the early projects had to rely upon existing federal regulation in responding to new state regulations.

III. SOME BASIC WAVE PHYSICS

WiFi sends information via radio waves. But radio signals at a receiver do not perfectly match those at the transmitter. Various properties of radio waves attenuate, or dampen, the signal as it propagates. This Part explores those properties because the physical effects will combine with FCC regulation of radio waves to make WiFi an imperfect choice for citywide Internet access.

A. Free-Space Wave Propagation

A receiver far from the transmitter receives a signal weaker than a receiver close to the transmitter. "Free-space propagation" describes this phenomenon.[30] Free-space propagation is a matter of geometry. Consider a transmitter as a simple point. A signal leaving that point will propagate radially outward, visualized as a spherical shell centered at the transmitter and increasing in radius. Close to the transmitter, the signal spreads out over a given area. Think of it as the surface area of the shell carved out in space by tracing each point at that fixed distance away from the sphere in any direction. As the distance from the transmitter increases, however, the signal must spread out over a larger area. Carving a shell in space of all of the points far away from the central source creates a larger shell; the signal must reach each point on that shell. For a signal with a given source power, the power of the signal at the receiver decreases as distance increases. Because the surface area of a sphere increases by the *square* of the distance from the center ($4\pi r^2$), the power of the signal decreases by the distance squared.

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. *See id.* § 3014(h)(3).

29. *See* COLO. REV. STAT. § 29-27-101 to § 29-27-304 (2006); NEB. REV. STAT. § 86-593 to § 86-599 (2006).

30. *See* HERVÉ SIZUN, RADIO WAVE PROPAGATION FOR TELECOMMUNICATION APPLICATIONS, 1–2 (2004) (briefly explaining free-space propagation). For a more approachable explanation of electromagnetic waves, see THOMAS A. MOORE, SIX IDEAS THAT SHAPED PHYSICS: UNIT E: ELECTRIC AND MAGNETIC FIELDS ARE UNIFIED, 320-38 (2d ed. 2002).

Free-space propagation explains the dominant force behind the fact that even in an empty room, a close light bulb illuminates a book more than a distant light bulb of the same wattage. By the time the light from a distant bulb reaches the book, it has spread out over a large area, creating a less intense illumination. Free-space propagation is particularly problematic for technologies like WiFi that use omnidirectional transmitters because unlike some transmitters, omnidirectional transmitters send signals in all directions.[31]

B. *Obstacles*

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. 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.[32]

C. *Interference*

Other radio signals, particularly those operating near the same frequency, can destructively interfere with a signal. Think of this phenomenon as noise-cancelling headphones. If one signal takes the exact opposite form of another signal, the two sum together to cancel each other out. Interference is a problem even when signals are not exactly the same because when 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.[33]

---

31. To extend the light analogy, lasers are useful in small part because their signals do not spread very much, so they do not suffer very much from the geometrical signal-spreading problem of free-space propagation. The signals spread a bit, and various other forces such as dust can attenuate the signal, but they do not suffer the same magnitude of spacial attenuation as conventional light bulbs, which are essentially omnidirectional, because lasers emit nearly unidirectional light (based on the author's personal experience).

32. *See* SIZUN, *supra* note 30, at 1–5, 35–66, 403–13 (documenting how obstacles attenuate radio signals).

33. *See id.* at 52 (briefly explaining signal interference).

IV. THE FAILURE OF PUBLIC WIFI

Even though more than two hundred municipalities hoped for successful public WiFi deployments, the idea has largely collapsed as the major projects failed. In 2007, Philadelphia, Chicago, San Francisco, and many other cities watched as private partners filed for bankruptcy or pulled out of the deals.[34]

Failures in both supply and demand explain the failure of public WiFi. On the supply side, the systems simply could not deliver what proponents promised. Because of WiFi's technical and regulatory limitations on frequency and power output, blanketing a city proved to be prohibitively expensive. Outdoor areas and a few buildings could be wired for wireless access, but no one could deliver anywhere-Internet using WiFi. Signals from streets could not penetrate large buildings, and property rights prevented municipalities from installing the required number of access points inside private buildings. As a result, public WiFi networks could be used only in limited areas.

Demand suffered, also. Inside, users already have access to wired or wireless networks. Outside, the user experience falls short of usability for most people. Moreover, municipalities began to roll out public WiFi networks just as private companies rolled out nationwide 3G data networks, cutting off demand for public WiFi.

A. *Technical and Regulatory Limitations*

1. Frequency, Congestion, and Power

In 1985, the FCC acted to allow certain unlicensed transmissions.[35] This action paved the way for the introduction and widespread adoption of WiFi a decade later. The regulation limited the ability of WiFi to provide citywide wireless Internet access because it imposed critical restrictions on frequency and power output of unlicensed transmissions.

---

34. *See generally* Tim Wu, *Where's My Free Wi-Fi?*, SLATE, Sept. 27, 2007, http://www.slate. com/id/2174858 ("[O]ne city after another has either canceled deployments or offered a product that's hardly up to the hype."); *Reality Bites: American Cities' Plans for Ubiquitous Internet Access Are Running into Trouble*, ECONOMIST, Aug. 30, 2007 ("[T]he numbers do not add up.").

35. *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).

Part 15 of the FCC regulations limits these unlicensed transmissions to 900 MHz, 2.4 GHz, or 5 GHz.[36] 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. Accordingly, WiFi operates at 2.4 GHz and 5 GHz.

Recall from Part III.B, however, that signal attenuation from obstacles depends on frequency. Selecting an ideal frequency involves many factors, but lower frequencies typically reduce attenuation from everyday objects. Compare these 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.[37] With WiFi constrained to these non-ideal frequencies, the signal degrades significantly 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 enable interference-causing traffic congestion. WiFi may only operate in two or three frequency bands.[38] Other electronic devices may also operate in these bands. Portable telephones, baby monitors, and other devices use the same bands. Commercial wireless operators with licensed and assigned spectrum slices design and manage networks to minimize interference from other devices. The ad hoc nature of the unlicensed WiFi space, however, allows anyone to install a device that could interfere with a public WiFi project.[39] 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.

---

36. *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.

37. 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.

38. *See supra* note 36 (explaining that 900 MHz would geographically limit WiFi, leaving 2.4 GHz and 5 GHz as the only worldwide standards).

39. 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 although 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).

The FCC restricts not just frequency, but also power output. Specifically, it restricts peak output power to 1 watt.[40] Recall from Part III that free-space propagation, obstacles, and signal interference all attenuate a radio signal. 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. A car's headlights would interfere with the signal. Now imagine the sender replaced the batteries with fresh batteries, increasing the power of the light output. Or imagine if 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 despite tinted glass or 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.

But the FCC limits unlicensed output to 1 W. 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.[41] 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.

2. Consequences from Technical Limitations

Imperfect frequency, congestion within the frequency bands, and limited signal strength combine to require high-density installations. In order to blanket an area with coverage no point should be more than 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 be physically mounted somewhere. A worker must also secure it to prevent theft. To add to the high-touch difficulty, each access point needs power and sometimes even a wired network connection.[42]

---

40. *See* 47 C.F.R. § 15.126(a) (1985).

41. *See* Station Index, *Chicago*, http://www.stationindex. com/tv/markets/Chicago (2008) (listing output power of Chicago television stations).

42. With "mesh" networks, access points wirelessly share network connectivity with each other, so an initial wired connection bounces from a wireless access point to a wireless access point before finally reaching the user. *See generally* Ian F. Akyildiz et al., *Wireless Mesh*

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. Part II.C described how the Pole Attachments Act may allow municipalities, in partnership with private telecommunications providers, to mount wireless equipment on utility poles.

Indoor settings, however, require higher-density installations. Obstacles such as walls and furniture will significantly limit the signal, as described in Part III.B. Interference from other wireless signals will further limit users' abilities to effectively receive the signal, as described in Part III.C. These factors, together with free-space propagation, combine to require higher-density installations inside.

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,[43] 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.

3. Technical Alternatives

Several different technologies exist that can provide wireless Internet more effectively. For example, WiMax and 3G cellular networks can both provide high-speed access at longer ranges than WiFi.[44] To overcome the wireless challenges outlined in Part III, these alternative technologies may use higher power output levels, or lower frequency bands. But to do so in the United States, they must use licensed

---

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.* at 524.

43. 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).

44. *See generally* LOUTFI NUAYMI, WIMAX: TECHNOLOGY FOR BROADBAND WIRELESS ACCESS (2007) (describing WiMax technology); JAANA LAIHO ET AL., RADIO NETWORK PLANNING AND OPTIMISATION FOR UMTS (2d ed. 2006) (explaining technologies behind 3G cellular networks).

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.[45] After Apple introduced its iBook laptop with built-in WiFi ("Airport") in 1999,[46] many consumer and business portables gained built-in WiFi cards. If potential users already have WiFi-ready equipment, municipalities can offer public wireless Internet access through WiFi without requiring users to purchase new equipment. This compatibility network effect reduces startup costs for users and encourages adoption. Additionally, the proliferation of WiFi technologies in homes and businesses created economies of scale, competition in the marketplace, and widespread availability of compatible hardware. WiMax was still too new to have the benefit of reduced costs from economies of scale. Moreover, the limited market and FCC licensing issues surrounding cellular technologies prevented widespread availability.

B. *User Experience*

The preceding sections explained how various regulatory and technical hurdles prevent public WiFi from truly blanketing a signal in WiFi signals. Municipalities can realistically cover outdoor areas and municipal buildings such as libraries, but expanding coverage into homes and businesses dramatically increases cost, complexity, and coordination problems. WiFi signals from streets or parks may penetrate partway into houses and street-facing businesses, depending upon the location of the nearest access point, building materials and other obstructions, and interference from other wireless signals in the area. But WiFi signals from municipal property or rights of way will not reach larger homes, apartment complexes, skyscrapers, or large corporate campuses without cooperation from property owners and considerable expenses. This unfortunate arrangement reverses the ideal-use scenario.

Proponents of public WiFi envisioned laptops and other devices in public parks, but this vision falls short of reality because people use computers indoors. Again, technical hurdles receive the blame. Laptop

---

45. 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).

46. *See* Steve Lohr, *Apple Offers iMac's Laptop Offspring, the iBook*, N.Y. TIMES, July 22, 1999, at C1 ("The iBook communicates with the [Airport] base station via two antennas built into the notebook computer.").

screens lack the brightness required to compete with sunlight, so using laptops in the sun often creates an inadequate work environment. Second, handheld tools with brighter screens like PDAs and cell phones (ignoring for the moment that the latter example already connects to the Internet through a carrier) do not typically work well for long periods of work because of small screens and awkward input mechanisms. Aside from these technical device limitations, people tend to work inside because of the availability of paper documents, office equipment, colleagues, desks, and adequate lighting after sunset. Although some users may choose to do light work outdoors, and although we can envision other uses for outdoor wireless Internet access (such as municipal vehicles), these niche users might not provide enough revenue to recover large fixed costs, particularly with the existence of alternatives.

C. *Competition*

1. Pervasive Wireless Internet

For users who want pervasive wireless Internet, all of the major wireless telcos offer 3G Internet with broader coverage than public WiFi could realistically hope to offer.[47] These plans cost about $60 per month for nationwide coverage.[48] These plans provide healthy competition to public WiFi. Because of the technical and regulatory differences, they can nearly blanket a city in signals. As a result, they are substitutes for not only public WiFi, but also perhaps even Internet access at home.[49]

---

47. *See* AT&T, *AT&T Coverage Viewer*, http://www.wireless.att.com/coverageviewer; Verizon Wireless, *Coverage Locator*, http://www.verizonwireless.com/b2c/CoverageLocator Controller; Sprint, *Sprint Coverage Tool*, http://coverage.sprintpcs.com/IMPACT.jsp; T-Mobile, *Personal Coverage Check*, http://www.t-mobile.com/coverage/pcc.aspx.

48. *See* AT&T, *DataConnect Plans*, http://www.wireless.att. com/cell-phone-service/cell-phone-plans/data-connect-plans.jsp ($60/month for 5 GB of data); Verizon Wireless, *BroadbandAccess Data Plans*, http://www.verizonwireless.com/b2c/store/controller?item=plan First&action=viewPlanList&sortOption=priceSort&typeId=5&subtypeId=13&catId=409 ($40/ month for 50 MB of data; $70/month for 5 GB of data); Sprint, *Mobile Broadband Connection Plans*, http://nextelonline.nextel.com/NASApp/onlinestore/en/Action/SubmitRegionAction?is UpgradePathForCoverage=false&nextPage=DisplayPlans&equipmentSKUurlPart=%3Fcurrent Page%3DratePlanPage&newZipCode=20001 ($60/month for 5 GB of data); T-Mobile, *Internet & E-mail Data Plans*, http://www.t-mobile.com/shop/plans/Default.aspx?plancategory=7# Internet+Only ($50/month for unlimited data).

49. *See* Walter S. Mossberg, *Novatel Laptop Cards Can Access Internet, But Services Vary*, WALL ST. J., Aug. 31, 2006, at B1 ("Unlike commercial public Wi-Fi services, which require users to be near a 'hot spot,' these services can be used anywhere in a metro area, even in a moving car or train.").

In fact, these plans could satisfy many of the stated goals of public WiFi. Public safety officers could use these private networks for all of the reported uses of public WiFi. A municipality does not need to build its own network for officials to use the network. For example, municipalities currently pay for public safety officials to use cellular phones on private networks. Similarly, municipalities can bridge the digital divide without building a public network by subsidizing access on private networks.

2. Competition with MC=0

Additionally, many people already have Internet access—often through WiFi—in frequently-visited places. People may access the Internet at home through cable, DSL, dialup, satellite, or even 3G wireless networks. Inexpensive wireless routers exist to provide wireless access in the home. Many employees already have Internet access at the office, and many companies have already completed the burdensome task of installing WiFi throughout the office (often requiring hundreds of access points because of the technical issues outlined in Part III). Hotels, airports, coffee shops, and cafes often provide wireless Internet access for free or for a small fee. Finally, schools and public libraries typically have Internet access. These last two categories are important. Public WiFi may be very important in public buildings such as libraries. But installing WiFi in these locations often predates pervasive municipal WiFi projects. Simply put, municipalities may provide WiFi in a few key areas without building citywide networks.

Private parties have already provided Internet access in places people typically live, work, study, and travel. Pervasive public WiFi projects would try to duplicate these private networks—often ineffectively. Providing access to a network frequently involves large fixed costs but very low marginal costs. With that cost structure, adding another redundant network is frequently expensive, wasteful, and unsuccessful. Here, cable companies, telephone companies, employers, and the hospitality industry have already expended large fixed costs to provide access. For the end user, the marginal cost of an additional byte of data is essentially zero. We should not expect many users to pay for public WiFi access in this case.

V. SUCCESSFUL PUBLIC WIFI: LIMITED SCOPE AND SCALE

Even with all of these problems, public WiFi might be successful in some instances. Enabling public WiFi in government buildings such as libraries is valuable because the ratio of expected users to the cost of installation in a single building exceeds that of a citywide deployment. Municipalities might also succeed when offering public WiFi in schools, high-trafficked public parks, and courthouses.

Additionally, many small, rural municipalities have found success deploying public WiFi. This Article provided the framework to evaluate why. 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. Additionally, if a small municipality wants to use WiFi to extend access to only a few locations, 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 in Part III.A. Finally, rural areas as opposed to highly developed urban areas have fewer obstacles and even fewer interference-causing devices to degrade the signal.

VI. 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. Like a Hollywood movie, proponents of public WiFi thought that if they built it, users would come.[50] But municipalities could not build the networks as promised, and users had little reason to come to the limited networks they delivered.

WiFi could not deliver a citywide network because technical and regulatory limitations combine to require access points at least every few hundred feet outside, and even closer indoors. Mounting that many access points is too expensive and nearly impossible inside private buildings. WiFi deployments require high-touch, high-density installations. As a result, municipalities could roll out costly but limited networks, at best. 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.

50. *Cf.* FIELD OF DREAMS (Universal 1989) ("If you build it, he will come.").