ANNENBERG RESEARCH NETWORK ON INTERNATIONAL COMMUNICATION

Building the Wireless Infrastructure: Alternative Models

Annenberg Research Network on International Communication

François Bar
Annenberg School for Communication
University of Southern California

Hernan Galperin
Annenberg School for Communication
University of Southern California

A research report prepared for the International Workshop on Wireless Communication Policies and Prospects: A Global Perspective, held at the Annenberg School for Communication, University of Southern California, Los Angeles, October 8th and 9th 2004.

Building the Wireless Infrastructure: Alternative Models

Abstract

Despite (or perhaps because of) the lack of central planning, Wi-Fi is fast reaching 'infrastructure' scale: Almost unknown three years ago, about 26.5 million Wi-Fi capable devices were sold in 2002 alone, and have been deployed by a multitude of individuals and organizations. Historically, decentralized network segments based on new technologies often served initially to extend previous generation infrastructure, and then eventually expanded to become the dominant infrastructure. Will this be true of Wi-Fi as well? To be sure, not all Wi-Fi deployment is decentralized. Several industrial actors, among them the incumbent telephone companies, are proceeding in a centralized and systematic fashion. Next to them however, a growing number of grass-roots organizations, non-profits, and local governments are deploying local extensions to the existing Internet infrastructure. And an emerging category of consolidators attempt to offer users unified access to these disparate infrastructures. To date however, most Wi-Fi deployment has simply amounted to the addition of "wireless tails", last-mile extensions to the existing Internet infrastructure. In the future however, one can imagine scenarios under which these uncoordinated initiatives coalesce into a new infrastructure, perhaps one based on mesh networking. This paper reviews current efforts to deploy Wi-Fi infrastructure, along three key dimensions: architecture, coordination, and control. It situates them within a broad theoretical framework describing the evolution of information infrastructures. The framework builds on several core concepts, including the tension between centralized and decentralized deployment efforts, the historical patterns of infrastructure deployment and substitution, the role of users in shaping the evolution of technology, and the co-evolution of usage and technical systems.

1. Introduction

The future of communications will be un-tethered and mobile: cellular phones now outnumber fixed ones, most laptops come equipped with wireless data connections, and we increasingly expect to remain connected always, everywhere. But just as mobile technologies come to define how we communicate, we face fundamental choices about the architecture, coordination, and control of the underlying network infrastructure. At the heart, these choices are about allocating power between the center and the edge. They mirror the tension between traditional hierarchical telecommunication networks and distributed systems such as the Internet Their resolution will profoundly shape our emerging mobile information societies, with considerable economic, social and political consequences.

One evolutionary path for mobile communications would extend the long-established centralized approach to the world of wireless communications. Licensed by the state, wireless service providers deploy top-down, centrally controlled, closed-architecture networks. Their economic strategies rest on tight control over spectrum and wireless standards, and on their ability to raise massive amounts of capital to secure licenses, build out networks, and subsidize terminal equipment. They largely determine what communication applications can use their networks. In such a system, innovation comes from the center, and that center also typically controls content distribution. At the other extreme, a radically decentralized approach would allow the spontaneous emergence of bottom-up mobile networks. Within an open ‘spectrum commons’, autonomous radios would assemble as needed to create ad-hoc mesh networks that require no centralized control. Assuming a dense enough distribution of such radios, network coverage would become nearly ubiquitous. Collectively, the end-devices would control how the network is used. New communication services could be invented and implemented at the edge of the network, and propagated throughout the network from peer to peer.

The evolution of the mobile Internet currently stands at a critical juncture, with many possible trajectories lying between these two extremes. Each will imply distinct ways to foster mobile technology development, different policy mechanisms governing the use of radio spectrum, different industrial strategies for the deployment of wireless networks and mobile devices, and diverse social and economic use patterns for the resulting communication applications. In this paper, we identify three key dimensions of these choices: architecture, coordination, and control. We illustrate them through a case study of the recent evolution of Wi-Fi.

The dominant *architecture* of today’s networks uses wireless mainly as ‘tails’ to wired networks. In cellular phone networks, wireless links connect phone users to their provider’s nearest tower, where calls are handed over to the wired network. In Wi-Fi networks, wireless carries data for a few hundred feet to an access point where it is transferred to a wired broadband connection. A few exceptions have started to emerge, such as the 'mesh' networks deployed by several municipalities, where communications hop from one radio to the next, traveling long distances before touching a wire. Pushing that alternative architecture further, we could imagine extensive wireless grids, creating a mostly-wireless network infrastructure where wires progressively recede in the background.

Similarly, *coordination* of the deployment and operation of traditional wireless networks is largely centralized in the hands of large operators and equipment manufacturers, as well as government agencies which dole out licenses to use the airwaves in a carefully planned manner to avoid potential interference. However, recent developments in wireless technologies and in spectrum management policies suggest that a different approach is possible: a multitude of user co-operatives, municipalities, and small companies are creating wireless networks from the bottom-up, in an unplanned manner. The resulting decentralized infrastructure could become a source of vibrant innovation and competition. Alternatively, some fear, it could also mark a return to the Darwinian cacophony of radio's early days.

In established wireless networks, *control* rests with the operator, centralized much like in the old telephone network. The end devices, cell phones or PDAs, remain essentially dumb terminals, kept in check by operators who determine many aspects of their operations, such as the conditions under which they can connect with other devices, roam on competitors networks, or what data applications –and what content– they might use. But as today's wireless terminals become increasingly powerful, aware of the usage characteristics of the radio spectrum around them and able to adapt dynamically, we can envision a alternative model where greater control resides in the devices at the edge of the wireless networks.

The traditional approach to deploying wireless infrastructure sits at one extreme of these three axes: wireless links are used as extensions to a primarily wired network, with centralized coordination and control of the resulting infrastructure. However, three current trends converge to permit departure from that tradition: the emergence of more flexible spectrum policies, in particular the success of unlicensed spectrum bands; the advent of new wireless technologies that create the potential for more independent wireless terminals such as cognitive radios and mesh networking; and the entrance of many business and non-profit actors eager to play new roles in the creation and use of new wireless networks. Together, they open the possibilities for change along each of the three axes we have identified: architecture, coordination and control. Yet movements are possible along each axis somewhat independently from the others: one could build a centrally coordinated wireless grid, or imagine giving greater independence and control to terminal devices within current cellular networks. In this paper, we argue that different sets of choices along each of the three axes would imply significantly distinct wireless infrastructures, with correspondingly different implications for communication uses. For illustration, we explore the associated trade-offs in the case of Wi-Fi.

The paper is organized as follows: in the first part we outline our theoretical perspective which draws on three related bodies of literature: the social constructivist history of large technical systems, the work of economic historians concerned with the evolution of technology and technical standards, and the theory of common-pool resources. We then review the key stages in the development of Wi-Fi and examine different deployment patterns. Next we discuss the technical, economic, and regulatory issues most likely to affect the architecture, coordination, and control of emerging wireless networks, with a focus on the challenges for scaling-up existing Wi-Fi networks into an integrated public grid. While our lenses are focused on the U.S. case, similar past trajectories and future challenges are likely to be found elsewhere. We conclude by drawing parallels between the evolution of the wired Internet and the potential for disruptive change in the wireless Internet case.

2. How Networks Are Built, for What, and by Whom

Our approach to the study of wireless communications infrastructure stems from the confluence of three bodies of research. First, we draw on the social constructivist approach to technology and the development of so-called "large technical systems" (Joerges, 1988). These scholars share a common interest in the historical evolution of a broad range of networks (from railroads and waterways to the telephone and the Internet), with particular attention to the patterns by which new technologies and their associated infrastructure displace old ones. The underlying assumption is that, because new networks grow within an environment already populated by old ones, it is critical to understand the historical patterns of accommodation and displacement between them.

A classic model is presented by Hughes (1983). Drawing upon his study of the American electricity system, Hughes distinguishes three main phases in the growth of large network systems. The first phase is that of *invention and innovation*, when maverick inventors attempt to create and perfect the technology. In this phase, adoption is limited to isolated experiments where the possibilities offered by the new technology are tested. The second phase is that of *transfer*, when the new technology is deployed under different geographical, economic and legal environments. In this phase, users often innovate and adapt the new technology to local conditions, and connections begin to be made between previously isolated deployments. The third and final phase is that of *growth and consolidation*, characterized by the scaling up of the network through the interconnection of local or regional system into an integrated national grid. In this phase, government and large corporations replace users as key actors as the need for financing and coordination of resources escalates.

This theoretical framework is useful to conceptualize how new technologies such as Wi-Fi progress from invention to large-scale adoption (or failure), how they interact with existing systems, and how different actors (users, incumbent firms, would-be entrants, governments) shape its trajectory. There are several consistent findings in this literature that relate to new wireless networks. One of them suggests that the initial phase of development for network technologies tends to be driven by the uncoordinated actions of end-users rather than guided by a grand plan.[1] A second relevant finding is that new technologies are often conceived as appendices for existing systems, only later to become dominant. A third relevant finding is that new technologies rarely evolve according to their original design, and more important, that experimentation by users is critical in the initial stages of deployment (Nye, 1990; Fischer, 1992). The amateur radio operator of the early 20th century is perhaps the best example. As Douglas (1987) and others reveal, users experimented extensively with early radio equipment and introduced important modifications to extend its range and performance, often taking the dominant industry players (notably RCA) by complete surprise.

As we shall see, the lessons from the evolution of previous network technologies bear much relevance to our case study. Much like the telephone was once considered a feeder for the telegraph, or radio an extension of telegraphy into the sea, Wi-Fi was originally conceived as a cordless extension of the wired Internet – essentially as a substitute for cable on closed LANs within homes or office buildings. It was only when users and small entrepreneurs started taking Wi-Fi beyond these boundaries that alternative possibilities were revealed. Moreover, much like RCA and other incumbents were taken by surprise by amateur radio operators, incumbent wireless carriers have wrestled with the unexpected mushrooming Wi-Fi networks, particularly as this represents a potential threat to large investments in competing wireless technologies such as 3G mobile telephony. Lastly, similarly to the cases of early radio and electricity, significant improvements to the reach and functionality of Wi-Fi networks have been made by Wi-Fi enthusiasts, including routing protocols for mesh networks, authentication tools, and the real-life testing of signal propagation and interference problems.[2]

A second relevant approach to the study of wireless networks is the work of economic historians concerned with the evolution of technology and technical standards

---

[1] This is particularly true in the U.S. context, where fragmentation of political authority and a normative orientation in favor of private entrepreneurship discourages centralized network planning by government authorities. In Europe, by contrast, centralized network planning has historically been more acceptable and politically feasible.

[2] It is interesting to note that the notorious Pringles “cantenna” used by many Wi-Fi enthusiasts has a precedent in the history of radio, for early radio amateurs often used Quaker Oats containers to build radio tuners.

(Rosenberg, 1982; David, 1985; Arthur, 1989). Of particular relevance to our case is the concept of path dependency. This concept suggests that the long-term evolution of a technological system depends on the specific historical circumstances of its origins, and emphasizes the importance of present-time small events in the future trajectory of the system as a whole. An important insight is that the process of technological evolution – as well as many others that are based on durable arrangements such as sunk investments and complex political institutions – is what statisticians call non-ergodic: how it got there matters for where it is going in the future. To some extent, this questions the notion that new technologies will replace (or find accommodation with) old ones in a predictable pattern. Path dependency instead suggests that new technologies are, in their initial phase, open to multiple possible trajectories in terms of deployment and use (including of course failure). Over time, however, the accumulation of sunk investments and durable institutional arrangements channels the technology along one specific trajectory, thus foreclosing once possible alternatives.

These concepts have interesting implications for considering both stability and change in the evolution of wireless networks. First, they call attention to the significance of choices made by policymakers, firms, and early adopters in the initial stages of deployment. Non-ergodicity suggests, for example, that in the present context several trajectories are still possible for Wi-Fi, but that the range of opportunities will soon begin to close as the technology matures and investments continue to be made in equipment, networks, R&D, training, and so forth. Second, this framework is also useful to theorize the relation between Wi-Fi and other wireless technologies such as 3G mobile telephony. While today these technologies differ enough to be considered complementary (Wi-Fi for short-range, high-speed access, and 3G for long-range, low-speed access), it is possible to imagine near-future scenarios in which they represent rival networks (Lehr and McKnight, 2003). In fact, it has often been the case that network technologies once considered complementary turned into direct competitors. For example, the direct current (DC) and the alternating current (AC) electricity systems were once considered complementary, based on their technical strengths and constraints.[3] However, as improvements were made to both systems, head-to-head rivalry followed. Similarly, as new wireless technologies mature, learning effects (Rosenberg, 1982), network externalities (David, 1985), lock-in effects (Arthur, 1989) and other dynamics associated with path dependency will shape their battle.

The concept of path dependency also calls attention to the importance of so-called critical junctures. These are narrow windows in time, typically in the early stages of technology adoption, when random events or choices made by key players have a decisive effect on the evolutionary path of the technology. Because large technical systems are built sequentially by market actors that continually adapt their strategies to the changing political, economic, and technological environment, the process tends to be highly discontinuous, characterized by critical junctures in which seemingly small events steer the technology along a certain path and thus forecloses others. The Titanic tragedy in 1912, which lead to considerable limitations on the operation of amateur radio (Douglas, 1987), and the unexpected decision to open the NSFNET backbone to commercial traffic in the late 1980s (David, 2002) are examples of small events that significantly shaped the evolution of radio and the Internet respectively. We argue below that Wi-Fi is today at a critical juncture. Small choices made by key players are likely to determine whether this fledging technology evolves as an appendage to existing broadband services within a centralized deployment model, or whether it opens the door for a radical reconfiguration of wireless infrastructure based on the spontaneous emergence of local wireless networks.

Finally, we draw from the theory of common-pool resources to understand how coordination problems affect the deployment of new wireless networks. This theory originates in response to the work on collective action by Olson (1965) and in Hardin's influential article "The Tragedy of the Commons" (1968). The gist of Olson's argument is that no self-interested individual is likely to contribute to the production of a public good. Hardin takes the argument a step further and logically demonstrates that, when

---

[3] The low voltage DC system had limited long-distance capabilities, whereas AC was plagued by security concerns as well as the lack of efficient conversion for existing motors, which made it unsuitable for industrial applications. See Nye (1990).

resources are shared by rational, profit-seeking individuals, each will appropriate from the resource pool until expected benefits equals costs, and since individuals will tend to ignore costs imposed on others, the cumulative result will be resource depletion through overexploitation. The policy implication is that, because individual cannot overcome collective action problems in a commons, externally-imposed rules are needed to achieve their own long-term interest.

The theory of common-pool resources started from the simple observation of everyday life examples of cooperative behavior between individuals that contradict Hardin's argument. Scholars thus began efforts to identify the conditions under which individuals are in fact able to successfully organize and manage a common resource collectively. By drawing from a variety of case studies ranging from fisheries in Canada to irrigation systems in India, Ostrom (1990) and others have identified a series of general design principles that characterize self-organized regimes for the use and management of common resources, among them clear boundary rules, congruence between appropriation rules and local conditions, participation by those affected by the regime in the creation of rules, self-monitoring, graduated sanction for non-compliance, and the existence of low-cost conflict-resolution mechanisms. The key insights from these studies are, first, that more solutions exist to the collective action problem of common resource use than Hardin envisioned, and second, that shared norms (both formal and informal) for the sustainable management of common resources can be formulated and enforced by communities of users.

The theory of common-pool resources is particularly useful for conceptualizing the challenges associated with the emergence of decentralized wireless networks. This scenario, in which low-power transceivers operating on unlicensed bands connect to each other to form an ad-hoc wireless mesh, presupposes large-scale cooperation among users in a number of different ways (Benkler, 2002). The first and most obvious is spectrum sharing. Spectrum commons advocates correctly point out that recent advances in digital signal processing and modulation technologies coupled with cost reductions in processing have drastically reduced the problem of interference, possibly to a point where users need not compete for a fixed number of channels (e.g., Werbach, 2002). While the validity of these propositions is yet to be tested, it remains that shared norms about equipment specifications and performance will need to be formulated and enforced by those participating in the wireless grid (Satapathy and Peha, 1997).

Another example of cooperation stems from the very idea of a mesh architecture in which each user will both send and receive its own data traffic as well as help relay that of others. Some suggest this architecture may be able to defeat the idea of a "tragedy of the commons" in spectrum management altogether, for network capacity would increase (rather than decrease) as more nodes are added to the mesh (e.g., Reed, 2002). However, as critics note, relaying messages is not cost-free: it consumes both transmission capacity and computational power, not to mention battery power (Benjamin, 2003). This results in a classic free-riding problem: individual users may adopt devices that benefit from relaying by others but do not forward others' traffic.

There are thus a number of collective action problems associated with decentralized wireless deployment that the theory of common-pool resources helps formulate. For example, shared norms will need to be created and enforced to coordinate the use of network resources and constrain the behavior of users. Will these norms be hardwired in radio equipment or will they be embedded in network communication protocols developed locally? How would compliance be enforced, and by whom? Will the growing movement of Wi-Fi community activism be able to overcome these collective action problems? Below we review the existing evidence about the emergence of such regimes for the use of common resources in decentralized wireless networks and suggest possible alternatives based on the general design principles identified by common-pool resource theory.

3. Wi-Fi Deployment Patterns: The Cordless Ethernet, the Public Hotspot and the Community Mesh

Wi-Fi networks have experienced extraordinary growth since 1997, when the IEEE finalized the 802.11 standard. Among the many factors explaining this rapid growth, three are particularly noteworthy: Wi-Fi's technical performance (high-speed and low cost), industry-wide standardization and use of unlicensed spectrum. First, Wi-Fi connections can deliver Ethernet speeds (roughly 10Mb/s to 54Mb/s, depending on the specific standard) within a range of about 150 feet. This makes them an effective replacement for wired networks within homes or office clusters, particularly as large volumes resulted in significant reduction in equipment prices. Second, there is widespread industry support for the Wi-Fi standard, coordinated through the Wi-Fi Alliance, an industry organization including over 200 equipment makers worldwide. The Wi-Fi Alliance was formed in 1999 to certify interoperability of various wireless LAN products based on the IEEE 802.11 specification. Since it began its certification program in 2000, the group has certified over 1,000 products. As a result, consumers can expect Wi-Fi client devices and access points made by different vendors to interconnect relatively easily. A third key to the technology's success resides in the lack of regulatory overhead: for the most part, Wi-Fi networks can be deployed without a license, which has made possible for a wide variety of actors to build wireless networks without any of the delays and expenses traditionally associated with obtaining a radio license.

So far, the deployment of Wi-Fi networks has followed three main patterns. We call these the cordless Ethernet, the public hotspot, and the community mesh. Each represents a distinct economic and social model of deployment, and creates different potential challenges for existing wireless operators. Each entails different choices with respect to network architecture, coordination and control. While driven by different logics of deployment these three categories have important synergies, for each increases the density of Wi-Fi devices and user familiarity with this network approach, and given broad equipment interoperability, network externalities make adoption more attractive for all.

Cordless Ethernet, the deployment of private Wi-Fi networks in homes and offices, represents the initial, most obvious and most widespread use of Wi-Fi. Here, the goal is simply the removal of the Ethernet or phone cable linking a computer to the network. In this incarnation, Wi-Fi is similar to cordless phones: it lets the laptop user wander away from the desk, dispensing with tangled cords. While this obviously saves wiring expense, it also comes with significant mobility benefits (or rather, move-ability – this isn't so much about computing while moving, but computing in different places). Further, because access points typically include routers, they serve readily as the hub of home networks that can connect several computers together, and with other devices such as printers or media servers, sound systems and televisions. As a result, Wi-Fi could serve to interconnect a variety of appliances in homes, expanding beyond simple cordless internet access for laptop computers.

There are similar logics promoting the deployment of these cordless Ethernet networks within the home and on corporate or university campuses. The latter are obviously more complex, requiring the deployment of many access points, and tighter management, in particular for authentication and security. Both however are contained within private spaces, and provide access to well known and regular users: household members in one case, employees and students in the other. The two also naturally reinforce each other, since laptop users equipped with Wi-Fi at home can also connect simply when at their friends houses, or at the office, or in any public place that has Wi-Fi. In fact, having Wi-Fi in one place often prompts the need to install it in the other. These private networks account for the overwhelming bulk of Wi-Fi's sales so far. Yet, for all Wi-Fi's success, the market is still far from saturation, and the resulting patchwork of private Wi-Fi networks is still sparse.[4]

Both residential and campus Wi-Fi networks use wireless links to extend the reach of wired networks by a few hundred feet. Coordination of the wireless links deployment is generally distributed among home owners and campus information systems organizations. In some cases, DSL or Cable connectivity providers also supply their residential customers with wireless access points, extending their reach to coordinate the

---

[4] The Metagroup estimates that Wi-Fi is only available in about 10% of U.S. companies (in Business Week, Special Report, op. cit.).

wireless tail attached to their wired network. However, control over these wireless extensions largely escapes the providers of wired connectivity. Residential users and Campus managers have full power over the kinds of applications they run over their cordless Ethernets and the kinds of authentication or security scheme they enforce. This highlight a significant potential departure from the cordless Ethernet pattern: since end-users effectively control who connects to their access points, they can chose to grow the network in ways that escape the control of their wired access provider.[5] Ultimately, this leaves the door open for growing cordless Ethernets into bigger networks that could bypass portions of the wired network.[6]

Public Hotspots represent another deployment logic. These are networks established in locations frequented by the public, offering wireless connectivity as a service to passing users. In the past few years, public hotspots have appeared in cafes, hotel lobbies, airport lounges, fast-food restaurants, public parks and libraries, among others. There, the idea is not to 'cut the cord', since there seldom was a cord to begin with – the provision of internet connectivity in public places usually is a new service. Three categories of actors have established such hotspot networks, each with its own motivation: commercial operators, grassroots cooperatives, and public agencies.

Commercial hotspot operators offer wireless connectivity for-profit, and most sell subscriptions to their service. A related, and comparatively small so far, category of commercial providers offer free wireless access to encourage consumers to buy something else – a cappuccino, or a night's stay in a hotel. The first wave of such companies were start-ups that emerged in the late 1990s and early 2000s, companies like Wayport or Surf 'n Sip. The central challenge they faced was to convince enough individual location owners to install one of their wireless access points in order to lure subscribers to the service. Wayport, for example, has been able to enlist several hotel

---

[5] DSL and Cable providers are well aware of this, and several have imposed restrictions on wireless AP sharing (discussed below).

[6] This would repeat the typical historical pattern described among others by Sawhney (2003), which has seen canals supplanted by rail feeders, or telegraph networks supplanted by phone links initially used for the local relay of telegraph messages.

chains and airports, and now offers wireless access in 700 U.S. hotels and 12 airports. It is estimated that in early 2004 there were almost 100 commercial hotspot operators in the U.S. alone and 250 worldwide.[7] Estimates vary somewhat about the total number of hotspots they cumulatively operate, generally in the range of 10,000 to 20,000 hotspots in the U.S.[8] Even assuming that the higher numbers are correct, this still represents a tiny portion of the areas where customers would want to expect reliable connectivity.

Therefore the appeal of individual networks necessarily remains limited. They are primarily aimed at business travelers who stick to the same routes and hotel chains. A second wave of commercial providers has emerged to patch together disparate networks: consolidators that re-sell wireless access from several physical network operators and offer simplified access and centralized billing through a single account. Companies in this category include iPass, Boingo, GRIC, NetNearU. Each consolidator federates distinct sub-sets of the commercial Wi-Fi service provider population, offering access points ranging in the thousands (for example, iPass claims over 2,500, and Boingo claims 2,400 live hotspots[9]). As they each try to reach critical mass, their current competitive strategies exclude reciprocal roaming agreements. As a result, unless users establish multiple accounts, they cannot expect to obtain access to the full 10-20,000 hotspots. This may be one reason why subscription and use of such for-fee hotspot access remains relatively limited to date. According to a recent survey by Jupiter, while 70% of consumers who use the Web were aware of public Wi-Fi service at the end of 2003, only 15% of those surveyed had ever used Wi-Fi at all (that includes home networks), only 6% had ever used a public hotspot (free or paid access), and only 1% had ever paid to use a hotspot.[10]

---

[7] Definitive numbers are hard to come by, but a good indication of the order of magnitude is given by Wi-Fi hotspot lists such as www.hotspot-locations.com (which lists 72 commercial hotspot providers in the US, 242 worldwide as of February 25, 2004)

[8] BW cites estimates of 20,000 to 25,000 commercial hotspots in the U.S., while the www.hotspot-locations.com directory counts 3,580, and www.wifinder.com lists 5,177 as of February 25, 2004.

[9] See company sites, at http://www.ipass.com/services/services_wifi.html and http://boingo.com, visited Feb 29, 2004

[10] Wired, “Wi-Fi Grows, but Profits Don't“ Dec. 16, 2003 (http://www.wired.com/news/wireless/0,1382,61618,00.html?tw=wn_tophead_2).

The situation could change as major telecom industry players enter the fray. Indeed, a third wave of commercial offering is now emerging, reflecting the entry of incumbent telecom providers on the Wi-Fi scene. The first was T-Mobile, the mobile communications subsidiary of Deutsche Telekom, which as part of its 2001 purchase of cellular carrier Voicestream, acquired a Wi-Fi network serving 1,200 Starbucks locations that had initially been established by MobileStar. It has expanded since then to 2,200 locations, and is bringing Wi-Fi to 410 Borders bookstores, airport lounges and selected Kinko's copy stores, for a total of 4,226 hotspot locations in the U.S.[11] T-Mobile had the only carrier-owned and operated Wi-Fi network as of 2003, and remains at the front of the pack, with Wayport currently a distant second. Further expanding access for its customers, T-Mobile now has a roaming agreement with iPass.[12] Other Telecom carriers are now joining in, although with various degrees of enthusiasm. SBC has recently announced plans to deploy 20,000 hotspots in 6,000 venues over the next three years.[13] Sprint PCS follows a different approach and has announced plans to roll out Wi-Fi service initially through roaming agreements with Wayport and Airpath locations, which it plans to complement later by building 1,300 hot spots of its own.[14] Verizon by contrast, had started with a limited deployment of about 150 hotspots in Manhattan, offering free access to its DSL subscribers, but the company has now postponed plans to expand its own network.[15] Instead, it currently resells Wayport service.[16] Overall, the telecom carriers' varied degree of support for Wi-Fi reflect the still-uncertain business models behind public Wi-Fi, as well as the tension between their Wi-Fi and 3G strategies.

Regardless of their particular business model, these various commercial offerings have all adopted the same architecture, existing wired data networks with wireless tails. Although

---

[11] T-Mobile web site, at http://locations.hotspot.t-mobile.com/, visited Feb. 29, 2004

[12] Eric Griffith, Roaming Comes to Starbucks, Wi-Fi Planet
December 16, 2003 (http://www.wi-fiplanet.com/news/article.php/3289701)

[13] August 6, 2003 company press release
(http://www.sbc.com/gen/pressroom?pid=4800&cdvn=news&newsarticleid=20609).

[14] Glenn Fleishman, "Technology Briefing | Telecommunications: Sprint PCS To Offer Wi-Fi Service", New York Times, July 22, 2003, Section C , Page 2.

[15] Kevin Fitchard, "Verizon's Wi-Fi Experiment Yields Results", Telephony, Jan 12, 2004 (http://telephonyonline.com/ar/telecom_verizons_wifi_experiment/index.htm).

[16] Eric Griffith "Verizon Wireless Roams with Wayport", Wi-Fi Planet, August 5, 2003 (http://www.wi-fiplanet.com/news/article.php/2244641).

a growing number of equipment providers now offer mesh networking equipment, we are just now seeing the emergence of a few commercial service providers relying on a mesh architecture, perhaps because the commercial failure of mesh pioneer Ricochet is still fresh in the industry's minds. Coordination of the deployment of these commercial hot-spots rests within individual companies, without any apparent attempt by aggregators to encourage complementary coverage. Service providers exert a significant degree of control over the use of the resulting hot-spots, in particular through the billing and authentication software they use to collect fees from their users.

Beside these commercial networks, a number of Wi-Fi networks have been deployed by non-commercial entities. The first and currently largest category comprises wireless community networks. These grassroots clusters of linked, neighborhood or citywide networks aim to provide wireless access to the members of the cooperative groups who build them, to their friends, and to the public in general. Community wireless networks are mostly made up of their members' access points, intentionally left open and made available to anyone within range. Some of them, such as the Bay Area Wireless User Group (BAWUG) also operate long-range connections (2 miles and more) linking clusters of access points. Wireless cooperatives pursue a wide variety of goals: some simply provide a forum for their members to exchange information about wireless technologies, while others are actively engaged in building wireless networks to experiment with the possibilities of Wi-Fi technologies. There are a few dozens community networks in the U.S., each typically ranging from a few nodes to a few dozen nodes.[17] There are also many individuals (or organizations) who volunteer to open their own access point to the public, without necessarily belonging to an organized cooperative, and advertise that fact on directories such as nodeDB.com.[18]

Despite much publicity, the assemblage of these community networks is today of small significance in terms of the network infrastructure it provides. Further, it is unclear how many people are effectively taking advantage of this free Wi-Fi access. In cases where

---

[17] There are 29 such networks listed in www.hotspot-locations.com.

[18] As of February 25, 2004, nodeDB.com lists 1,128 such nodes in the U.S.

the community organizations track usage of these open networks, there seems to be relatively few takers.[19] Anecdotal evidence indicates that the main users of these community networks are the community members themselves (Sandvig, 2003). Nevertheless, these networks play an important role in the emerging ecology of Wi-Fi. If nothing else, they represent a clear disincentive for investments in commercial hotspots operations. Verizon cites the availability of free wireless access in several areas of Manhattan as the reason why it decided to offer free Wi-Fi access to its existing DSL customers. Further, one can expect these not-for-profit networks to develop trajectories different from those of commercial networks. In particular, they have shown a keen interest in exploring alternative network architectures. The experimental work undertaken by BAWUG (long-range Wi-Fi connections) or by the Champaign-Urbana Community Wireless Network (mesh routing) are examples of these possibilities. Somewhat surprisingly, coordination among the various community wireless groups appear relatively limited, with different groups often reinventing the wheel.[20] The groups vary in how they choose to exert control over network use, but by and large they tend to give much control to end-users.

A second and more recent category of non-commercial networks are municipal Wi-Fi networks, deployed by city governments largely as an economic development strategy. By providing free downtown Wi-Fi access, some cities hope to help attract businesses to these areas, or to boost customer traffic. They also seek to lure conference organizers to their convention centers by making it easy for conference-goers to stay connected. This was for example the explicit goal behind the launch of free Wi-Fi access by the city of Long Beach, CA in its downtown, airport and convention center.[21] Not all municipalities intend to provide free Wi-Fi access however. In Cerritos, CA, the plan is to deploy city-wide wireless access in partnership with wireless ISP Aiirmesh, primarily to provide wireless access for municipal government buildings, mobile city workers, security and emergency services. Aiirmesh will then sell Wi-Fi access to Cerritos residents, most of

---

[19] See for example the usage statistics of Seattle-wireless at http://stats.seattlewireless.net.

[20] Based on interviews with 60 community groups conducted by Christian Sandvig (2003).

[21] Interviews with Chris Dalton, City of Long Beach Economic Development Office, February 6, 2004. See also John Markoff, "More Cities Set Up Wireless Networks", New York Times, January 6, 2003.

whom cannot get DSL or cable modem access.[22] When it completes its deployment later this year, Aiirmesh's Cerritos network will cover 8.6 contiguous square miles, making this the world's largest Wi-Fi zone. Similar projects are now turning up in a number of U.S. cities, including Lafayette, LA, Grand Haven, MI, Charleston, NC, and others.[23] In pursuing these deployments, municipal governments have a considerable advantage over commercial entities or community groups: they control prime antenna locations in the form of light posts and traffic signs, all of which have built-in electrical supply that can serve to power access points. They also have a direct need to provide mobile connectivity for their many city employees. Thus, municipal Wi-Fi deployments start with a significant economic advantage: they have at least one large, reliable, paying city government customer, which can often justify building the network in the first place, before adding on residential or business customers.

A significant number of these municipal networks use a mesh architecture: rather than connecting each Wi-Fi base station to the wired network, as in the case of residential access points or commercial hotspots, devices relay traffic to one-another with only a few of them hard-wired to the Internet. They are programmed to detect nearby devices and spontaneously adjust routing when new devices are added, or to find ways around devices that fail. Municipalities have an inherent advantage in pursuing a mesh architecture since they control a large number of prime locations for antenna locations, such as light posts, traffic signs or urban furniture, dispersed through the city and equipped with power supply. This architecture allows much more cost-effective deployment than bringing a broadband connection to each antenna site. This is the solution adopted in cities like Cerritos[24] and San Mateo, where a city-wide Wi-Fi mesh network serves the Police Department.[25] Cities typically coordinate the deployment of mesh networks throughout their territory, often relying on specialized contractors such as *Bel Air Networks* or *Tropos Networks*. Control over the resulting networks typically rests with the

---

[22] Broadband-deprived Cerritos turns to WiFi, San Jose Mercury News, Dec. 11, 2003.

[23] For descriptions of these municipal wireless projects in the U.S. and elsewhere see http://www.muniwireless.com.

[24] Dan O'Shea, "The Future of Wi-Fi is One Big Mesh", Wireless Review, Jan 1, 2004 (http://wirelessreview.com/ar/wireless_future_wifi_one/index.htm)

[25] "Wi-Fi Lets Computers, Cops Roam Free", San Mateo County Times, September 18, 2003.

municipalities and reflect the goals of each particular network deployment: from tightly closed wireless networks for law enforcement and emergency support, to wide-open networks to encourage economic development.

In the future, mesh networks could spontaneously emerge when enough Wi-Fi devices are present within an area. Indeed, there is no fundamental difference between Wi-Fi access points and clients, so that all Wi-Fi devices can be programmed to detect other devices within range and create ad-hoc connections. Traffic can then be routed through a series of short hops, bouncing from one device to the next until it reaches a backhaul link. Of course, this only works if there are enough Wi-Fi devices in an area, but this becomes increasingly possible as Wi-Fi prices come down and as Wi-Fi gets built into many devices beyond laptops such as cell-phones and PDAs. Consider the prediction that by 2008, 28 million cars will come equipped with local networking devices.[26] These would not only serve to connect various systems within the vehicle, but to support communications with outside systems, for applications ranging from telephony to safety and cashless payment systems. Ultimately, since cars are typically always within less than a hundred feet from one another (and have a built-in power supply), one could imagine how they would provide the basis for a mobile mesh networks. Of course, many technical issues remain to be solved for such networks to become practical, including the development of adaptive routing software that can keep up with intermittent mobile nodes (Agarwal, Norman, and Gupta, 2004). But the rapidly growing number of Wi-Fi devices present in the environment creates the potential for such wireless grids to emerge, bridging the gaps between the distant islands of today's cordless archipelagos.

4. Will a Thousand Wi-Fi Flowers Ever Blossom?

For many scholars and industry analysts, Wi-Fi represents a disruptive technology, particularly for the last-mile delivery of broadband services (e.g., Werbach,

---

[26] ABI Research, 2003, *Automotive Wireless Networks Opportunities for Wi-Fi, Bluetooth, RFID, Satellite and Other Emerging Wireless Technologies* (http://www.abiresearch.com/reports/AWN.html).

2002; Johnston and Snider, 2003; Sawhney, 2003). One of the most influential visions about such challenge was popularized by Nicholas Negroponte, who has predicted that as more Wi-Fi networks emerge and, more important, as these local networks start connecting to each other, the data would be relayed from one wireless network to the other, thus bypassing the wired infrastructure. In his own words:

> "think of a pond with one water lily, then two, then four, then many overlapping, with their stems reaching into the Internet (…). In the future, each Wi-Fi system will also act like a small router, relaying to its nearest neighbors. Messages can hop peer-to-peer, leaping from lily to lily like frogs – the stems are not required. You have a broadband telecommunications system, built by the people, for the people. Carriers are aware of this, but they discount it because they do not feel there will be sufficient coverage. They are wrong" (2002: 116).[27]

Or are they? The idea of a network built from the bottom-up, " by the people, for the people" is a persuasive vision that resonates with what Bar, Richards, and Sandvig (2002) have called the Jeffersonian syndrome that has permeated social thinking about the Internet from its origins. Yet the consolidation of today's archipelagos of wireless connectivity into an integrated grid that rivals existing wired alternatives faces several challenges. It will require the transformation of what today is a patchwork quilt of mostly private – though often inadvertently unsecured – networks extending only a few feet beyond their wireline "stems" into a public system that allows seamless relay across large areas. This would not only demand substantial investments to ensure proper coverage (as noted, the installed base of access points, though growing rapidly, is clearly inadequate). More important, it would also require a shared system for the management of traffic, the sharing of resources, and the use of standardized traffic protocols, to mention just a few challenges. And this coordination will have to take place between a fragmented collection

---

[27] Nicholas Negroponte, Being wireless, *Wired* 10.10, p.116 (2002). As Negroponte notes the water lily analogy should be credited to Alessandro Ovi (European Commission technology adviser).

of networks run by private users and organizations ranging from grassroots co-operatives to universities to large corporations.

These challenges are of course not unique to Wi-Fi. As noted, large networks have often started as a collection of disconnected systems, which over the years were connected to each other to form regional and later national grids. In this section we draw upon the lessons of older network technologies to identify the forces shaping the architecture, coordination, and control of emerging wireless networks. The historical evidence points to three major issues: technical standards, interconnection, and regulation.

Standards. Technical compatibility has traditionally been a major challenge for the integration and growth of large networks. From railroad gauges of different sizes to power systems of different cycles, the early history of network technologies is rife with standard battles that prevented seamless integration between local systems (Hughes, 1983; Lipartito, 1989). Wi-Fi has also emerged amidst competition from alternative standards for wireless local area networks (WLANs), notably HomeRF and HiperLAN. Interestingly, because these standards emerged from within the computer rather than the telecom industry, the standardization process has been largely led by the private sector, organized around industry consortia such as the HomeRF Working Group and semi-public organizations such as the IEEE. Unlike the contentious case of 3G standards (see Cowhey, Aronson, and Richards, 2003), the role of governments and multilateral organizations such as the ITU has been minimal.[28]

So far, standards battles in the deployment of WLANs have been minimized by the early commercial success of Apple's *Airport*, the adoption of Wi-Fi by corporate users, and the early establishment of an equipment certification program under the auspices of the Wi-Fi Alliance, all of which tipped the market balance in favor of Wi-Fi. While proprietary versions such as 802.11b+ have gained some acceptance, cooperation between a semi-public standards-setting body (the IEEE) and a private consortia (the Wi-Fi Alliance) has

---

[28] The only possible exception is HiperLan, a standard developed by the ETSI (European Telecommunications Standards Institute) as an European alternative to Wi-Fi.

so far resulted in broad interoperability of Wi-Fi equipment. Today the development of HomeRF has been largely abandoned, and while the new generation of the HiperLAN standard (HiperLAN2) gained some momentum in the EU as a result of ETSI (European Telecommunications Standards Institute) rules related to the use of unlicensed spectrum in the 5GHz band that delayed the launch of 802.11a products in the European market, analysts agree that this Wi-Fi competitor will, at best, fill a small niche in the corporate market.

Nonetheless, as the technology matures and widespread adoption of WLAN technology creates higher requirements in terms of capacity, security, reliability, and coverage, new standards challenges are certain to arise. In a sense, standardization problems have so far been minimal because of the very fact that the Wi-Fi networks deployed at this early stage are quite rudimentary, providing little in terms of security, reliability, coverage and quality of service. As the complexity of the technology and the range of services increase, so will the stakes for equipment vendors and network operators. China raised the interoperability red flag when it required that Wi-Fi devices sold in the country include a proprietary security standard developed locally (enforcement was suspended after much protest from the major equipment vendors). Standardization efforts for the next-generation of wireless networking technologies such as IEEE 802.16 (WiMax), which is designed to provide much wider coverage than Wi-Fi, are proving significantly more challenging.[29] It is likely that the coordination mechanisms that have driven the initial growth of Wi-Fi will not suffice to accommodate the range of interests created by its own success, therefore creating interoperability obstacles for decentralized deployment.

Interconnection and traffic arrangements. Skeptics contend that decentralized network growth will be frustrated by the need to establish arrangements for data relay, traffic management, billing, and so forth among thousands of separate wireless networks in a dynamic, ad-hoc environment. Yet it is forgotten that large integrated systems are often little more than arrangements between scores of separate entities – in other words, virtual

---

[29] Existing WiMax specifications can reach 75mb/s for up to 30 miles, with a typical cell radius of 4-6 miles.

networks. At the height of the railroad expansion in the 1920s there were over a thousand railroad companies in the U.S.. Yet through uniform operating, billing and accounting procedures both people and goods could be moved around the nation on a single car, often coordinated by system aggregators – the so-called express and fast-freight companies (Chandler, 1977). In the case of the telephone, it was the Kingsbury agreement of 1913 that transformed the industry from one divided between Bell and thousands of local independents (which for the most part provided only local service) into an integrated telecommunications system spanning the entire nation (Brock, 1981). In the case of radio, the American Radio Relay League (ARRL) was created in 1914 to coordinate the relaying of messages among thousands of radio amateurs, thus resulting in the first coast-to-coast communications network (Douglas, 1987).[30] While these industries would later undergo significant consolidation as a result of a variety of economic and political forces, our point is that integration has been often achieved through the federation of fragmented networks.

The historical evidence suggest that the challenges for the integration of decentralized wireless networks into a public system will be not so much technological as organizational. The evidence also suggest that the role of consolidators will be critical. As discussed, these have already appeared in the case of Wi-Fi under different models. For the most part, existing aggregators are simply providing unified billing and network authentication services on the basis of roaming agreements that allow customers to tap into different local Wi-Fi networks. However, there are also grassroots efforts to connect small local networks to each other in a truly decentralized mesh architecture. For example, the Consume project is a London-based collaborative effort to peer community Wi-Fi networks. Interestingly, the group has developed a model contract for cooperation called the Pico Peering Agreement, which outlines the rights and obligations of peering parties (in essence, it is a simplified version of existing peering agreements between Tier 1 backbone operators).[31] Much like in the case of open source software, these efforts are based on the voluntary spirit of like-minded (and technically-proficient) individuals who

---

[30] AT&T inaugurated its transcontinental service shortly after in 1915.

[31] Available at www.picopeer.net.

agree to provide free transit across their network. While simple contracts such as the Pico Peering Agreement might prove useful for peering among small community networks, more complex arrangements are likely to be required for the integration of Wi-Fi networks of different sizes and complexity, as well as users and organizations with different needs and expertise (Sandvig, 2003).

On the other hand, there are a number of factors that could facilitate integration in the case of Wi-Fi. The first is the architecture of the Internet itself. The Internet is the ultimate example of a decentralized system that integrates an ever-increasing number of constituent networks managed separately and built under different technical specifications. Such design did not happen by accident, but rather reflects the incentives and needs of the original Internet architects (David, 2002). Initially, the system was organized around a core backbone (ARPANET and later NSFNET) through which the separate networks connected. This later evolved into a decentralized system whereby a variety of organizations exchange traffic under various commercial and peering agreements. This contrasts with older network technologies that required centralized control (e.g., traditional telephone switching) to ensure proper traffic management. There are also economic incentives for Wi-Fi network operators to interconnect in order to economize on expensive backhaul links (the “stems” in the Negroponte’s analogy). As more networks join the wireless grid, fewer and fewer wired backhaul links will be needed. This is particularly true if a significant portion of the traffic is local, which some investigations suggest is the case for wireless community networks (see Auray, Beauvallet, Charbit, and Fernandez, 2003).

Another advantage is that wireless networks are not subject to the same economies of scale as wired networks, which makes decentralized deployment more feasible. For example, lack of capital for laying wires and operating expensive switching equipment created significant obstacles for the growth of independent telephone companies in the early 20th century, thus favoring absorption into the Bell system (Brock, 1981). With Wi-Fi, infrastructure investments (and to some extent network management functions) are being made by users themselves (either individually or organized locally), and because wireless dispenses of the labor costs typically associated with building wired networks, network expansion does not require large companies or government agencies capable of amassing the resources associated with earlier technologies.

Regulation and policy. Existing spectrum policies significantly shape the deployment of wireless networks in favor of centralized control and the traditional architecture of wireless as a tail to wired networks. This results from allocation and licensing rules that inflate the cost of scarce wireless licenses as well as strict limitations on the use of so-called unlicensed bands. In the case of Wi-Fi, this reflects the fact that Wi-Fi networks have flourished from a modest experiment in spectrum management initiated by the FCC in 1985. The Commission decided then to allow low-power radios to operate on the so-called Industrial, Scientific and Medical (ISM) bands on a license-exempt basis. Such operation was nonetheless subject to the Commission's Part 15 rules, which prescribe that devices must not cause interference to licensed services, and that devices must accept any interference received. At the time the Commission allocated about 200MHz, spread over three bands (at 900MHz, 2.4GHz, and 5GHz). In 1997, an additional 300MHz was added with the allocation of the so-called U-NII (Unlicensed National Information Infrastructure) frequencies in the 5GHz band.[32] There is currently a pending proposal to allocate more unlicensed spectrum in the 3GHz band as well as in the more desirable (and in some cases lightly used) UHF and VHF bands currently occupied by broadcasters.[33]

While the current supply of unlicensed spectrum has spurred the rapid growth of wireless Internet archipelagos, it is clearly inadequate for scaling-up the system into a wireless grid. In effect, at the current pace of growth the current regime might soon prove inadequate for accommodating new users. Because of favorable propagation characteristics and the availability of inexpensive equipment, the more desirable unlicensed frequencies (i.e., those in the 2.4GHz band) are rapidly becoming congested.

---

[32] Some of the U-NII frequencies in fact overlap with the ISM band, so the net addition was only about 200MHz.

[33] Notice of Inquiry in the Matter of Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band, ET Docket No. 02-380. With the exception of the 2.4GHz band, in other nations the availability of unlicensed spectrum varies considerably (ITU, 2004).

Limitations on transmit power for Wi-Fi equipment (1 Watt in the U.S. case, lower in most other nations) considerably restrict coverage and the opportunities for user experimentation with alternatives architectures such as mesh networks. In many developing nations, those wanting to operate Wi-Fi outside their living room or office still need to obtain a radio license from the regulator (Galperin, 2004a).

The current situation of Wi-Fi is comparable to that of FM radio in the 1930s, cable TV in the 1960s, or computer data networks in the 1970s: as a fledging new technology begins to disrupt the established industry arrangements and challenge economic privileges built into the legal apparatus, incumbents attempt to use regulation to confine the new technology to a niche market or to position it as a appendix to existing ones. Interestingly, incumbent broadband providers have also engaged in some of the same preemptive strategies as their historical counterparts, notably that of refusing interconnection and preventing users from attaching "foreign" devices to the network (these are typically written in service agreements intended to prevent bandwidth sharing). For their part, incumbent wireless telephony providers, many of whom have invested heavily in potentially competing technologies such as 3G , are resisting efforts to make more frequencies available for license-exempt use.

For Wi-Fi networks to reach infrastructure scale, more unlicensed spectrum will need to be made available (preferably below 3GHz), and power levels between licensed and unlicensed devices will need to be rebalanced in favor of low-power users. These reforms, however, will not be easily accomplished. The existing spectrum regime, forged in most nations in the 1920s, has for decades favored centralized networks built upon large investments by a handful of licensees. Over time, this regime has solidified through sunk investments in high-power network equipment and the emergence of interest coalitions aimed at protecting the existing spectrum arrangements. However, a broad political coalition advocating spectrum reforms that would open the door for alternative models of wireless deployment is taking shape. Its key argument is that the current spectrum regime is based on outdated assumptions about spectrum congestion and that progress in radio technology (e.g., software defined radio, smart antennas, cooperative radio networking, etc.) makes possible efficient spectrum sharing by many more low-power devices (Werbach, 2002; Reed, 2002).

Aside from its technical merits (which are yet to be tested outside the labs), the argument faces an uphill battle against powerful spectrum incumbents who are unlikely to surrender their rights without a fight.[34] The most interesting battle in the U.S. context (which is often indicative of those to come elsewhere) centers on the prime frequencies assigned to television services (402MHz in the VHF and UHF bands). While analog television services are notorious for their wasteful use of spectrum, broadcast licensees are on the other hand notorious for their ability to protect their spectrum privileges (Galperin, 2004b). In the past, efforts by entrepreneurs armed with new technologies – such as land mobile radio in the 1980s – to share these bands have met with severe resistance from broadcast trade organizations, which successfully organized to protect the status quo.

The spectrum reform movement is reminiscent of the formative period of broadcast radio, when an eclectic political coalition sought to maintain a balance between large radio networks and small, non-commercial local operators (McChesney, 1993). At the time, the reform coalition lacked major industry allies, given the vertical ties between commercial broadcasters and equipment manufacturers. Today, however, some of the major Internet infrastructure vendors such as Intel and Cisco have thrown their weight in favor of expanding unlicensed bands. Another favorable factor is the growing consensus among academics and policy elites that current spectrum policies are inadequate. This is also important, for as Derthick and Quirk (1985) have shown in the case of the Bell system, changes in the accepted consensus within academia and regulatory elites are often the prologue for wide-scale industry reforms. These are signals that the equilibrium point for the spectrum policies is shifting towards new licensing rules that favor bottom-up deployment, mesh architectures, decentralized network management and other alternatives to the traditional architecture, coordination, and control of wireless networks.

---

[34] Ironically, even the ARRL, an organization originally created to defend the rights of amateurs radio users, has voiced concerns about spectrum sharing with Wi-Fi devices.

5. Conclusion

The deployment of wireless Internet infrastructure stands at an important juncture. So far with Wi-Fi, the unlicensed spectrum experiment has succeeded beyond any regulator's dreams. The immediate result and most significant aspect of this success is the spectacular diffusion of Wi-Fi devices. With tens of millions units sold in just a few years, we now have a critical mass of Wi-Fi radios in the environment. All signs point to the continuation of this trend in the coming few years: Wi-Fi devices are becoming very cheap and embedded in a wide array of consumer devices, from cell-phones to televisions, appliances and cars. Once density reaches a certain threshold, the existing deployment architecture – which we have called the cordless Ethernet – and models of control will need to be revisited, for the system will reach capacity as too many devices compete for scarce resources such as frequencies and backhaul links.

So far however, the wireless grid remains at the embryonic stages of its development. Following Sawhney (2003), we note the sprouting of wireless islands and feeders in homes, campus networks and some community networks. Indeed, all the U.S. public hotspots combined would cover an area just about the size of a small town like Cerritos, CA. We also observe some timid encouragement by the incumbent infrastructure operators, in particular by broadband carriers who see home Wi-Fi networks as a good way to promote cable or DSL services. In this sense, Wi-Fi provides much added convenience and encourages consumers to use more of the old wired networks through their cordless Ethernet, but it doesn't fundamentally challenge the established network's architecture, nor does it introduce a new infrastructure paradigm that could unsettle the existing industry arrangement.

The central question is whether the large, and fast growing, number of Wi-Fi devices could be coordinated differently to create a fundamental challenge to existing networks. We believe we are fast approaching a point where this might happen, because of two related developments. The first is the bottom-up dynamics associated with Wi-Fi deployment, whereby multiple network actors are independently pursuing the deployment of wireless infrastructure. As households, commercial hotspots providers, grassroots community networks, corporations and universities build their own cordless Ethernet archipelagos, the incentives will increase to share resources, reach roaming or peering agreements, and devise new cooperative mechanisms to manage this decentralized wireless infrastructure as a public grid. The possibility to do just that is tied to the second development, the recent emergence of working mesh protocols that can knit together neighboring Wi-Fi devices into a single network. At this point, mesh technology has been worked out for centrally deployed network devices, and much technical work remains to be done for spontaneous mesh networks to become a reality. Nonetheless, as with other technologies, experimentation by users and corporate R&D will eventually result in a workable solution. More challenging, however, will be to create new organizational arrangements to manage the wireless grid, and reform the existing legal regime which confines Wi-Fi to its present role as an appendix to wired networks.

David (2002) has aptly described the Internet as a fortuitous legacy of a modest R&D program which was later adapted and modified by various economic and political actors to perform functions never intended by its original creators. Wi-Fi has similarly emerged from a rather modest experiment in spectrum management that has unexpectedly resulted in the proliferation of local wireless networks in homes, offices, and public spaces. Much like the Internet challenged traditional telecom networks, with this new architecture comes a new distribution of control over wireless networks. However fast new wireless technologies evolve, this will be an evolutionary process whereby various stakeholders, not simply equipment manufacturers and incumbent carriers but also local governments, start-up providers and especially end-users, will interact to shape the technology in different ways. While some battles will be market-driven, other will take place in the courtrooms, in regulatory agencies, and within standards-setting organizations. Having outgrown its original purpose as an appendix to the wired infrastructure, wireless networks now stand at a critical juncture, for they embody technical possibilities of potentially disruptive character, and yet it is in the decisively social realm of economic and political interactions that their future is being cast.

References

Agarwal, A., D. Norman, and A. Gupta (2004). *Wireless grids: Approaches, architectures, and technical challenges*. MIT Sloan School of Management Working Paper 4459-04.

Arthur, B. (1989). Competing technologies, increasing returns, and lock-in by historical events. *The Economic Journal 99*: 116-131.

Auray, N., G. Beauvallet, C. Charbit, and V. Fernandez. (2003). *Wi-Fi: An emerging information society infrastructure*. STAR Issue Report #40, September 2003.

Bar, F., J. Richards, and C. Sandvig. (2002). *The Jeffersonian syndrome: The predictable misperception of the Internet's boon to commerce, politics, and community*. Published?

Benjamin, S. (2003). Spectrum abundance and the choice between private and public control. New York University Law Review 78: 2007-2102.

Benkler, Y. (2002). Some economics of wireless networks. *Harvard Journal of Law and Technology* 16(1): 25-83.

Brock, G. (1981). *The telecommunications industry: The dynamics of market structure*. Cambridge: Harvard University Press.

Chandler, A. (1977). *The visible hand: The managerial revolution in American business*. Cambridge: Harvard University Press.

Cowhey, P., J. Aronson, and J. Richards. (2003). The peculiar evolution of 3G wireless networks: Institutional logic, politics, and property rights. In E. Wilson and W. Drake (eds.)., *Governing global electronic networks*. Cambridge, MA: MIT Press.

David, P. (1985). CLIO and the economics of QWERTY. *American Economic Review* 75: 332--336.

David, P. (2002). The evolving accidental information super-highway. *Oxford Review of Economic Policy* 17(2): 159-187.

Derthick, M., and P. Quirk. (1985). *The politics of deregulation*. Washington, DC: The Brookings Institution.

Douglas, S. (1987). *Inventing American broadcasting, 1899-1922*. Baltimore: John Hopkins Press.

Fischer, C. (1992). *America calling: A social history of the telephone to 1940*. Berkeley: University of California Press.

Galperin, H. (2004a). *Wireless networks and rural development.* Presented at the Latin American Studies Association Conference, Las Vegas, NV, October 7-9, 2004.

Galperin, H. (2004b). *New TV, old politics: The transition to digital TV in the U.S. and Britain*. Cambridge: Cambridge University Press.

Hardin, G. (1968). The tragedy of the commons. *Science* 162:1243-1248.

Horwitz, R. (1989). *The irony of regulatory reform: The deregulation of American telecommunications*. New York: Oxford University Press.

Hughes, T.P. (1983). *Networks of power: Electrification in western society 1880-1930.* Baltimore: John Hopkins Press.

International Telecommunications Union (ITU). 2004. *The portable Internet*. Geneva: ITU.

Joerges, B. (1988). Large technical systems: Concepts and issues. In R. Mayntz and T.P. Hughes (eds.), *The development of large technical systems*. Boulder: Westview Press, pp. 9-36.

Johnston, J., and J.H. Snider. (2003). *Breaking the chains: Unlicensed spectrum as a last-mile broadband solution*. Spectrum Series Working Paper #7, New America Foundation.

Lehr, W., and L. McKnight. (2003). Wireless internet access: 3G vs. WiFi? *Telecommunications Policy* 27(5-6): 351-370.

Lipartito, K. (1989). *The Bell system and regional business: The telephone in the South, 1877-1920*. Baltimore: John Hopkins Press.

McChesney, R. (1993). *Telecommunications, mass media, and democracy: The battle for the control of U.S. broadcasting, 1928-1935*. New York: Oxford University Press.

Nye, D. (1990). *Electrifying America: Social meanings of a new technology*. Cambridge: MIT Press.

Olson, M. (1965). *The logic of collective action*. Cambridge, MA: Harvard University Press.

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. New York: Cambridge University Press

Reed, D. (2002). *Comments for FCC Spectrum Policy Task Force on Spectrum Policy*. ET Docket 02-135.

Rosenberg, N. (1982). *Inside the black box: Technology and economics*. Cambridge: Cambridge University Press.

Sandvig, C. (2003). *Assessing cooperative action in 802.11 networks*. Presented to the 31st Telecommunication Policy Research Conference, Washington D.C.

Satapathy, D., and J. Peha. (1997). Spectrum sharing without licenses: Opportunities and dangers. In G. Rosston and D. Waterman (eds.), *Interconnection and the Internet: Selected papers from the 1996 Telecommunications Research Conference*. Mahwah, NJ: Lawrence Erlbaum, p. 49-75.

Sawhney, H. (2003). Wi-Fi networks and the rerun of the cycle. *Info* 5(6): 25-33.

Werbach, K. (2002). *Open spectrum: The new wireless paradigm*. Spectrum Series Working Paper #6, New America Foundation.