Network Neutrality in the Wireless World

Tim Wu†

Communications regulators over the next decade will spend increasing time on conflicts between the private interests of telecommunications carriers and the public's interest in a competitive innovation environment centered on the Internet. One area where these issues have been little discussed is the wireless world, of mobile phones and other wireless devices. This paper examines the practices of the wireless industry with an eye toward understanding their influence on innovation and consumer welfare.

In many respects the mobile market is and remains a wonder. Devices that were science fiction thirty years ago are now widely available to consumers. For the last decade, wireless mobile has been an "infant industry" whose practices have attracted some, but limited attention. User penetration has been the primary priority, and all scrutiny has been focused on *intra-industry* practices--namely efforts to prevent switching between carriers. Too little attention have been paid to the effects of wireless industry practices on other industries -- mainly, because of a faith that the oligopoly structure might prevent any practices detrimental to consumers or the nation.

Today, as the industry and platform mature, the wireless industry warrants a new look. In this report, we find a mixed picture. Some of what the wireless industry pursues are policies necessitated by the wireless environment. Yet at the same time we also find the wireless industry -- particularly certain members of it -- pursuing policies that, in the wired world, would be considered outrageous, in some cases illegal, and in other cases simply misguided.

First, this report focuses attention on practices, some better known that others, warrant particular attention:

1. *Network Attachment* -- imposing bars or making difficult building equipment for wireless network;

2. *Phone crippling* -- forcing equipment manufacturers to offer products that with crippled or missing capabilities, most obviously WiFi and

---

† Professor, Columbia Law School. Research assistance provided by Adam Chen and Derek Tang.

Bluetooth, along with phones locked to a single network;

3. *Discriminatory Broadband Services* -- Offering "unlimited" data services, in fact, are limited, and discriminate between applications and also between users;

4. *Application Stall* -- Excessive burdens and conditions on application entry in the wireless application market have stalled what might otherwise be a powerful input into the U.S. economy.

Second, this report rates the carriers. It identifies important variation between the four largest carriers: Cingular, Verizon Wireless, Sprint-Nextel, and T-Mobile. Speaking generally, Verizon Wireless engages in the most restrictive practices across the board, including misrepresentations that may warrant serious attention. Cingular and Sprint are mixed. Finally, T-Mobile is consistently the least restrictive of consumers and application developers. As one consumer representative said to us about transferring photos using Bluetooth, "it's your phone--do what you want with it."

* * *

In Washington D.C., the wireless world is sometimes described as a nirvana for consumers bought on by competition and enlightened government policy. That is true relative to its history. For decades, U.S. policy restricted entry into the mobile market. There is no question that since the 1990s, when the Federal Communications Commission began to auction wireless spectrum suitable for telephones and other devices, wireless telephony finally took off, bringing a dissemination of mobile devices. But now, in the late 00s, the industry is no longer an infant. As mobile platforms mature, and as consumer markets reach saturation, the discriminatory practices of mobile providers have become more obvious and warrant greater scrutiny.

There are in general two principle justifications for the industry's practices. The first is that industry practices should be tolerated as a subsidy to encouraging investments in deployment. That justification may have held more weight in earlier times. Today, however, the penetration rates of cellular phones in the United States and the rest of the wireless world no longer should provide the blanket support for industry practices. A second justification is that the industry's practices are mandated by technological necessity. These claims, similar to the claims made by AT&T for much of the 20th century, must be examined far more closely. [security]

The historic parallel is instructive. Wired voice telephone networks had more or less reached their full potential under AT&T by the 1960s. To

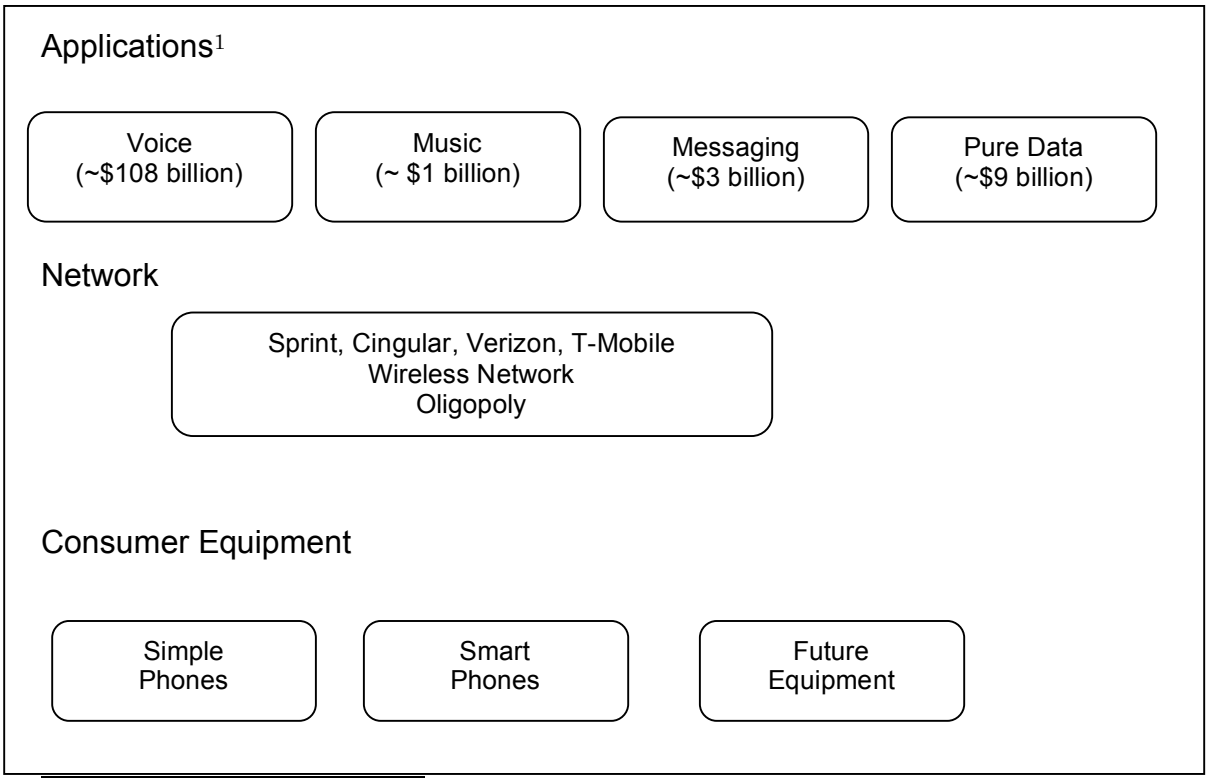
reach the next stage, the most important steps were not technological but deregulatory -- destroying impediments created by AT&T that restricted innovation and competition. To reach the "next stage" in wireless communications, the most important step may be opening the networks to true competitive entry. This paper specifies how that could happen.

One point should be clear. This paper is written from the perspective of what carriers practices are harming consumers or society at large -- and also to raise questions for the carriers themselves. It is not a call for comprehensive regulation or nationalization of the wireless industry. Rather it is intended to shed light on practices that might, for one thing, be dissipated by consumer pressure and competition. The perspective is that regulation, if necessary, should be a last resort.

The discussion is divided into three areas: network attachments, data services, and network applications. First, however, we discuss the economy surrounding wireless devices.

1. Competition Model

The wireless world is a classic example of an information platform economy.



[1] The sources of the revenues in the diagram below are from multiple sources, including eMarketer, September 2006, CTIA-Wireless Association

Today, the dominant discussion of the wireless industry is focused on the degree of competition *between* carriers, and in particular, on price competition. However, little attention has been paid to the effects that carrier practices might have on markets touched by the wireless industry and its spectrum-based oligopoly -- the equipment and application markets, and more generally, society at large.

In this environment, the wireless carriers have an obvious interest: maximization of revenue. Much of the time, maximizing revenue means making the wireless networks and wireless services as useful to consumers as possible. However, sometimes discriminatory practices may maximize the profits of the carrier, but at the expense of the broader economy.

Discrimination is currently limited by law in several ways. When it comes to voice service, the carriers have common carrier duties that require them to allow any American with a phone number to reach any American with a telephone. Discrimination as to voice calling is forbidden. Yet other discriminatory practices are wide-open, and there are numerous gaps between what the carriers will do in pursuit of their interests and what is in the interests of consumers, and the nation as a whole. There are also differences in what might be tolerated in an infant industry, and what ought be allowed in a mature industry.

From this abstract discussion we can identify three classes of behavior that can be expected to persist despite oligopoly price-competition between the carriers.

1. *Industry Threats.* First, even if the wireless industry is competitive within the industry, it may unite to prevent consumers from reaching competitors to the industry *as a whole*. For example, mobile VoIP service may be a threat to the industry as a whole, meaning that it could be in the interests of the carriers to act in near-unison against VoIP and/or WiFi.

A consumer might use the WiFi functionality of the phone when at home, and the "cell" capacities of the phone when on the road. While obviously good for protecting the business model of the existing industry, there is little attractive about wireless carriers blocking VoIP's development. It forfeits potential savings to consumers, and also the innovations that might be centered on mobile VoIP.

2. *Protection of Existing Revenue Streams*. Individual carriers can also be expected to act individually or in unison to block threats to existing

revenue streams, even if doing so makes the product marginally less useful. For example, most telephones could easily obtain ringtones from a multitude of sources -- using the receiver function of the phone itself, using the "Bluetooth" protocol, or through the Internet. However, many carriers have taken steps to make it difficult or sometimes impossible for consumers to install ringtones on their phone, other than by paying the carrier. The ringtone practices are a clear example carriers discriminating to protect existing revenue streams, at a cost both to consumers and potential providers of ringtone content.

3. *Prevention of Potential Revenue Sources.* In some instances, the industry seems interested in preventing the development of business models or revenue streams that rely on its technology and network, yet which it will lack significant control. In other words, the industry sometimes appears to prefer that a new service not exist at all, than develop into a lucrative industry that it cannot control the pricing and conduct of.

For example, given more open mobile development environment, mobile developers might develop all manner of social networking technologies similar to those found on the Web. But the carriers seem hesitant to allow such development to occur, possibly out of the idea that if any such service is to exist, it should be "theirs." At times the industry, or parts of it, seem obsessed with the fear of becoming "a commodity" or "just a pipe." However valid or not, that sentiment sometimes leads to extreme of behavior.

These three basic practices -- protection of the industry, protection of existing revenue streams, and protection of potential future revenue -- are found in most obvious form in the carriers' equipment practices. Yet they have also led carriers to usual practices in the mobile applications world. Fear of competitive threat has led carriers to place overly stringent controls on the applications that they will allow to run or allow to be developed on their platforms, so that only "safe" applications -- namely, those that do not threaten a business model or a revenue stream -- may run on their networks.

The Security Justification

Carriers typically justify more questionable practices not as an effort to preserve present or future revenue streams, but to preserve the "security" of the network. For example, customer representatives for the various companies defended practices as varied as phone locking, whitelisting, or Bluetooth crippling and other practices as necessary for "network security." Often the relationship is tangential at best, and the security risk purely hypothetical.

For example, Verizon Wireless has at times justified crippling Bluetooth on its telephones as a means of preventing "fraud" and virus infections. However, there is no evidence that carriers that do not cripple Bluetooth have had significant problems with either.

The point of this report is not to suggest that there are no security or network health concerns on wireless networks. The point is to ask whether they are fundamentally different from similar concerns on other networks. It is worth recalling that AT&T's classic justification, in the 1950-70s, for its most anti-competitive practices was that it needed complete control of the system to ensure that it functioned effectively and securely. The FCC's answers to those concerns was a statement that AT&T was free to create standards that prevented harmful devices from being used on the network. Similarly, today, we must not accept a blanket claim of "network security" to solve any and all problems.

Will Competition Solve All Problems?

One potential response to the findings of this report is that the oligopoly competition in the industry will prevent any potentially troubling practices. First, troubling practices do exist, which is evidence that competition has not eliminated them. More broadly, the fact that competition pressure can eliminate harmful practices is not a reason not to publicize the practices in the first place. In other words, competition cannot eliminate harmful practices without consumer awareness as to their existence. One of the purposes of this report is to shed light on the differences between carriers, so that competition has more chance of doing its work.

Second, as discussed above, there are some reasons to believe that competition alone may not eliminate some of the troubling practices in the wireless industry. Some of the practices described here are beneficial for an individual company to pursue, yet impose spillovers on adjacent markets, or society at large. Those practices will not necessarily be eliminated by competition alone.

[structure is pricing is not immutable]

* * *

We now turn to a more detailed look at carrier practices. We examine three areas: (1) network attachments, (2) data-service discrimination, and (3) application development.

1. Network Attachments

In the wired world, consumers' freedom to hook up whatever devices they want to has been among the most dramatic and important rights ever established in American technology policy. In 1956, the D.C. Circuit famously ordered that the subscriber has the "right reasonably to use his telephone in ways which are privately beneficial without being publicly detrimental." Through the 1960s and 1970s, the FCC progressively deregulated network attachments – ordering the local phone companies to allow users to connect any devices that complied with a set of basic rules. These principles are usually referred to as the *Carterfone* principles.[2]

In *Carterfone* itself, AT&T had a rule (tariff) that said

> "No equipment, apparatus, circuit, or device not furnished by the telephone company shall be attached to or connected with the facilities furnished by the telephone company, physically, by induction or otherwise."

AT&T relied on this rule to block the use of a device called the *Carterfone* which facilitated communication between a mobile radio and a telephone. The FCC struck down AT&T's rule as "unduly discriminatory." Importantly, the FCC rejected arguments made by AT&T that suggested control over all equipment on the network was necessary for the telephone system to function properly.

The 1968 *Carterfone* right to attach devices to home networks is perhaps the fundamental consumer right in telecom, whose consequences have been of historic scale. The attachment right is broadly celebrated by policy analysts of every ideological persuasion, as both consumer advocates and free market libertarians recognize the *Carterfone* principle as a central tenant of a competitive telecommunications policy. However, as we shall see, AT&T's wireless descendents have shown an interest in resurrecting, one way or another, their pre-*Carterfone* rule.

As a form of anti-discrimination rule, the *Carterfone* principle has had enormous consequences for not only Telecommunications policy, but the history of the United States. Open network attachments gave birth a thriving market in home and business equipment. That led, predictably, to competition in the phone market. But it also led, unpredictably, to other innovations. Those include mass consumer versions of the fax machine, the answering machine, and, perhaps mostly importantly, the modem. The freedom to buy and attach a modem became the anchor of the mass internet

---

[2] See Use of the Carterfone Device in Message Toll Tel. Serv., 13 F.C.C.2d 420 (1968).

adoption of the 1990s, whose effects are still felt today. As one observer put it in 2004, "without *Carterfone,* AT&T would probably be rolling out modems right about now." Arguably, the FCC's rules on network attachments have been its most successful in its history of regulation.

However, these same important freedoms of network attachments have not fully reached the wireless world. Thanks to its recent birth, network attachment in the wireless world is limited in various ways. It is often difficult or sometimes impossible for consumers to decouple their wireless equipment from services from devices provided by the phone company. Consequently, the market for consumer devices is unusual and distorted. It can be difficult or impossible for firms to (as, say the providers of mass fax machine inventors did) enter the market without cooperating with wireless providers. As one equipment developer put it, "if you want to build something, you have to run the gauntlet of business development at the carriers. If they don't like what you're doing, you can't do it."

In the 1960s, of course, Bell offered strong justifications for restricting the free attachment of foreign devices. AT&T, in *Carterfone* argued that "since the telephone companies have the responsibility to establish, operate and improve the telephone system, they must have absolute control over the quality, installation, and maintenance of all parts of the system in order effectively to carry out that responsibility." The principle justification was always the protection of the security and health of the network. Yet over time, those arguments proved unconvincing. Today, the arguments for the continued control of wireless carriers over network attachments is equally unconvincing.

1. Barriers to Network Attachments

We now examine how, technically, the major ways in which wireless carriers limit or make difficult network attachments. In the landline world, the manufacturer of a new telephone or fax machine needs few permissions to sell a new product. So long as the new device complies with basic technical standards, specified mainly in FCC Rule 15 and by private groups like the Underwriters Laboratory, the product can be sold and will work as soon as its plugged in.

It is a mixed picture in the wireless world. As most in the industry know, in the United States, carriers rely on two main, and different main standards -- GSM and CDMA.[3] The CDMA carriers (Verizon, and Sprint

[3] GSM stands for the Global System for Mobile Communications and is the world's most popular standard. CDMA stands for Code Division Multiple Access and is used mainly in the United States and South America. For more on these differences, see [source].

PCS) have different means of restricting network attachment than the GSM carriers (T-Mobile, Cingular, and AT&T). We shall examine each in turn.

Permission-based Entry. For the largest CDMA carrier in the United States, Verizon Wireless, only devices specifically approved by Verizon work on its networks. Verizon, stated differently, acts as the gatekeeper of consumer equipment market entry in manner barred on wired networks since the 1970s.

Technically, how is this accomplished? For CDMA carriers, every device that connects to the network must have approved number – an ESN (electronic serial number, or, more recently, an MEID (mobile equipment ID)). The practice of Verizon Wireless, according to a numerous customer support representatives, is to block telephones that are not sold by Verizon itself.[4] As one Verizon customer representative put it, ""All the phones that work are already in our system."

The technique is to "whitelist" Verizon phones, and by implication blacklist others. Without an approved ID number, telephones not sold by Verizon will not be recognized and cannot be used on the network. This effectively makes Verizon Wireless the gatekeeper of market entry for telephones on their network. It recreates the rule struck down in *Carterfone* -- that no equipment "not furnished by the telephone company" may be used on the network.

The whitelist is not a matter of technological necessity. Sprint PCS is also a CDMA carrier, and its practice is slightly different. Sprint keeps a list of customer ESNs, and bars the use of existing ESNs -- which can be evidence of a "cloned" or stolen telephone. While Sprint "discourages" the use of non-Sprint phones on its network, it does not block the use of phones on its network as Verizon does.

Locked Phones. The GSM wireless providers (Cingular, AT&T Wireless, and T-Mobile) limit the freedom of network attachments using a different means: "locking" cell phones, or making them incapable of operating on any network other than theirs. In the landline world, it is hard to imagine buying a telephone that only worked on one company' phone lines. Outside of communications it would be strange to have a car that worked on some roads but not other. However, most of the equipment sold in the United States today, unless modified, will only work on one network, for reasons that have nothing to do with technological necessity.

---

[4] This was the answer given by Verizon in response to a verbal query on October 5, 2006.

Here's how it works. The GSM Mobile standard envisions a salutary separation between phone and service. For that reason, GSM phones carry a Subscriber Identity Module, or SIM card, designed to make it easy for one phone to be used on various networks, simply by plugging in new SIM cards.

Most if not all of the American GSM phones sold by carriers, however, as of 2006, disable the utility of the SIM system. Equipment is routinely locked to prevent customers from using equipment on more than one network. That is to say, if a consumer purchases a phone that is branded T-Mobile, she cannot insert a new SIM card and begin to use the phone on another network, either in the United States or otherwise. There are two varieties of lock: a "service provider lock" simply prevents the phone from being used on anything but the network of one service provider. A "full lock" prevents the phone from being used with any other SIM card, period.

The original , and still stated justifications for locking phones are to prevent subsidy abuse, ensure customer loyalty, and for "network security." The subsidy concern was that opportunistic firms might buy masses of phones and resell them, or to prevent individuals from buying a subsidized phone and then switching services. Yet today there are widely practiced and much less distortionary means of preventing abuse of subsidies – the contract termination penalties imposed by most cell phone contracts. The security justifications, while relied on my customer support representatives, don't clearly make sense. If a Cingular phone were used, say, on China Telecom's network, it's unclear how that might pose any security risk for Cingular.

Just as it is possible to lock phones, it is possible to unlock them. Typically, unlocking a phone required entering a series of codes, and there are a few companies that specialize in unlocking telephones and reselling them, and others that sell unlocked phones. T-Mobile and Cingular have been careful not to go too far in *absolutely* preventing the unlocking of phones, perhaps for fear of regulation. Both firms appear to have a policy of agreeing to unlock telephones, on request, so long as the phone has been owned for 3 months. However, they maintain a status quo whereby phones are usually locked, absent user expertise or knowledge.

The effects of phone locking are different than Verizon's whitelisting. Phone locking tends to discourage consumers from switching from one carrier to another, since it makes switching carriers also necessitate the purchase of a new phone. However, phone locking does not block the market entrance of phone manufacturers. Companies can still sell phones to T-Mobile customers -- albeit without the advantage of the phone subsidy.

Crippled Phones

As a condition of network access, American wireless carriers require equipment manufacturers to cripple features built into their telephones, or require the American versions of phones to be crippled relative to their European or Asian brethren. Some of the clearest examples are the well-known WiFi and Bluetooth protocols, which are either crippled on American phones or not available.

Bluetooth. Bluetooth is a protocol for short-distance wireless communications. It is designed to be allow up to 8 personal devices to communicate, such as PCs, keyboards, printers, wireless headsets, and so on, and is specified by the IEEE 802.15.1 Personal Area Network Standard. A difference between Bluetooth and technologies like WiFi is that Bluetooth is design to be simpler, and self-configuring. Devices on the network recognize one another and begin to work automatically.

On many American mobile phones with Bluetooth capabilities, the Bluetooth capabilities are crippled. They are typically are limited to recognizing wireless headsets. Other potential uses require "hacking" the telephone's capacities. Hacking is possible, but again, a skill which the vast majority of Americans lack.

In 2004, Verizon Wireless released the Motorola V710 cell phone, advertising "full" Bluetooth capabilities. However all of Bluetooth's file transfer capabilities of the cell phone were crippled. Verizon Wireless stated that the crippling was necessary to prevent "fraud." It later defending the crippling as necessitated by its contracts with various content partners. In January 2005, subscribers filed a class action lawsuit in California. Verizon Wireless settled the lawsuit, and has since more clearly marked its crippling of Bluetooth features. In addition to the V710, Verizon Wireless cripples the Bluetooth capabilities of its other telephones, including Smartphones like the Motorola Q.[5] In addition to Verizon's practices, which are notable, Sprint and Cingular have also, at various times, crippled various Bluetooth capabilities -- particularly on Smartphones like the Treo line.

The crippling of Bluetooth has important spillover effects. Most obviously, it affects the add-on markets for the telephone. For example, a telephone might be configured to communicate with a printer, to print photographs or phone numbers. However, these capacities have not developed, because equipment manufacturers cannot assume that a cell phone will have full Bluetooth capabilities.

[5] http://mark.cdmaforums.com/BT-PHONE.htm

Wi-Fi. Technologically, cellular phones can incorporate WiFi (802.11b) capabilities for a range of potential uses, from making VoIP calls, to accessing the internet more generally, or communicating with other devices. However, most American wireless carriers have strongly resisted the installation of WiFi capabilities in cellular phones. In some cases, they have forced equipment manufacturers to manufacture specialized American versions of telephone that have all WiFi capacities crippled.

The Nokia E62 / E61 is one example. The Nokia e61 cellphone is Nokia's flagship "smartphone" -- widely known as Nokia's "blackberry killer." It was released in Europe in the summer of 2006, to generous reviews. However, in the United States, Cingular will be the exclusive vendor of the e62 -- a crippled version of the e61 that has WiFi and other features removed. In the words of MSN columnist Gary Krakow wrote "What some carriers fear most is the e61's ability to handle VoIP calls when you're near a friendly wireless network. That's why we won't see Wi-fi on the e62."

Similarly, the Motorola Q was launched under a Verizon partnership in the United States in 2006, without Wi-Fi capabilities, and with some Bluetooth crippling. (The phone does has EV-DO capabilities -- Verizon's propriety data network).[6]

As of 2006, there are "pure" WiFi phones being sold in the United States, such as the Netgear SPH101. But these phones do not work on cellular networks on the wireless carriers. They are WiFi phones only -- typically allowing a user to make phone calls using Skype or other VoIP providers.

Of the major carriers, T-Mobile is the only one to experiment with offering consumers hybrid WiFi / Cellular telephones. Since October 2006, in the city of Seattle, T-Mobile has offered a plan whereby consumers can use a hybrid telephone, sold by T-Mobile, in T-Mobile's "hotspots." In addition, also in October 2006, T-Mobile began to make available the "Dash" smartphone, which at this time was the only major WiFi capable smartphone in the United States.

The reasons for blocking WiFi are obvious, and are an example of efforts to protect existing revenue streams at the expense of the consumer. A WiFi phone can make VoIP calls, when in a WiFi network, thereby depriving the cell phone company of potential revenue. In addition, a WiFi capable

---

[6] However, according to some reports in the European media, the European version of the Motorola phone will include Wi-Fi capabilities. (Italy's Cellulare Magazine.)

Smartphone makes a subscription to a proprietary broadband wireless program less necessary. For example, the owner of a Motorola Q with WiFi capabilities might decide not to subscribe to Verizon's EV-DO services.

2. Wireless Broadband Services

Under the general banner of 2.5G, or 3G, or "Third Generation" services, wireless carriers have begun offering various types of data services using their wireless spectrum. These data services are designed to be used both for smart telephones, and personal computers (presumably laptops), through a data-card. As in other areas, GSM and CDMA telephones use different protocols (EVDO (1x Evolution-Data Optimized), EDGE, and HSDPA. While there are important technical differences, we shall refer to all as wireless broadband services.

Verizon, Sprint-Nextel, Cingular and T-Mobile now all offer wireless broadband services. The services compete with commercial WiFi providers who usually offer services in cafes or airports, and free and municipal WiFi. Carrier Wireless Broadband is usually quite slower than WiFi (which has a capacity of 11 mps) yet still relatively fast. The Verizon and Sprint services achieve average speeds between 500-600 kbps, and "burst" speeds of up to 2 mps. The major advantage over WiFi is not speed but coverage -- WiFi networks tend to offered sporadically, by various providers, while EVDO service is available anywhere that the carrier's cell phone network reaches.

However, in a manner similar to early broadband services, Verizon and Cingular offer their services pursuant to discriminatory conditions of various kinds.

Blocks and Bans

Verizon & Cingular's practices are most notable. Verizon widely advertises "unlimited broadband access." (See figure 1). However, in

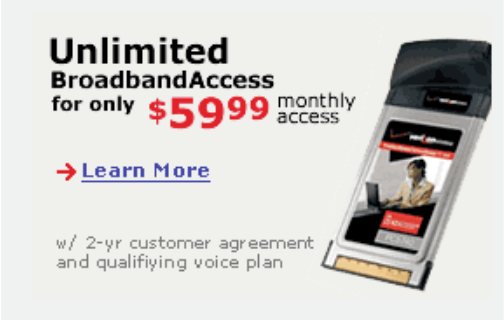


Fig. 2 Verizon EVDO Advertisement

practice, Verizon imposes limits on usage based both on the use of "forbidden" applications and bandwidth limits.

Cingular and Verizon have virtually identical Terms of Service contracts. They ban their users from using their Broadband connections for any purpose other than:

> (i) Internet browsing; (ii) email; and (iii) corporate intranet access (including access to corporate email, customer relationship management, sales force automation, and field service automation applications).

Verizon limits its unlimited brand service as follows:

> Unlimited NationalAccess/BroadbandAccess services cannot be used (1) for uploading, downloading or streaming of movies, music or games, (2) with server devices or with host computer applications, including, but not limited to, Web camera posts or broadcasts, automatic data feeds, Voice over IP (VoIP), automated machine-to-machine connections, or peer-to-peer (P2P) file sharing, or (3) as a substitute or backup for private lines or dedicated data connections.[7]

Cingular states that the following are prohibited uses:

> Prohibited uses include, but are not limited to, using Services: (i) with server devices or with host computer applications, including, without limitation, Web camera posts or broadcasts, continuous jpeg file transfers, automatic data feeds, telemetry applications, automated functions or any other machine-to-machine applications; (ii) as substitute or backup for private lines or dedicated data connections; (iii) for Voice over IP; (iv) in conjunction with WWAN or other applications or devices which aggregate usage from multiple sources prior to transmission; … except for CONTENT formatted in accordance with cingular's CONTENT standards, Unlimited plans cannot be used for uploading, downloading or streaming of video content (e.g. movies, TV), music or games. Furthermore, unlimited plans (except for DataConnect and Blackberry Tethered) cannot be used for any applications that tether the device (through use of, including without limitation, connection kits, other phone/PDA-to-computer accessories, Bluetooth® or any other wireless technology) to laptops, PCs, or other equipment for any purpose.[8]

A computer user who subscribes to Verizon's "unlimited broadband access," for example, is contractually barred from downloading episodes of the

---

[7] Verizon TOS, http://www.verizonwireless.com/b2c/store/controller?item=planFirst&action=viewPlanDetail&catId=409 accessed October 21, 2006.

[8] See Cingular Terms of Service, http://onlinestorez.cingular.com/cell-phone-service/wireless-phone-plans/cell-phone-plans.jsp?WT.svl=2206800007&q_catid=2206800007, accessed October 21, 2006.

television show "Lost" from Apple iTunes. She is barred from downloading user-created content on YouTube, and from using VoIP providers like Skype or Vonage.

How are these rules enforced? First, Verizon or other carriers may be blocking applications that fall outside its list of "permitted" uses. However, no tests of application blocking have been conducted.

Second, over the last two years, numerous people have complained about being shut-down by Verizon for using forbidden applications or too much bandwidth. Reports identify two patterns of termination. In the first, users are notified through letter that they are using too much bandwidth, and asked to call a number. When they call, they are asked whether they are downloading games, or songs. If the answer is "yes, the user is terminated, and may be charged Verizon's $175 termination fee. In a second reported pattern, the appeal stage is skipped: customers who, according to Verizon, use too much bandwidth, are terminated, and charged the termination fee.

An excerpt from one of the letters is below:

We have reviewed your above referenced Verizon Wireless National Access and/or Broadband mobile number with unusually high data activity. After review of the facts, a final determination that the unusually high activity was due to violation of the Unlimited National and/or BroadBand Access Terms and Conditions. Your National and/or Broadband Access service will be disconnected on the referenced number as of 2/21/2006, we regret any inconvenience by this disconnection notice.

T-Mobile and Sprint do not maintain the same restrictions on use. Instead, their terms of service are roughly similar to those of wireline Internet Service Providers, which prohibit illegal activity, reselling of bandwidth, and other harmful activities.

3. Applications

In the words of Michael Mace, an observer of the mobile application world:

"There's a collision coming between the wireless world and the web, and I think it won't be pretty. … The river is the torrent of innovation happening in web apps right now. The dam is the carriers who won't allow that innovation to run freely on their networks. They haven't figured out how

to set up spillways and generators, let along operate them, so the pressure of the water keeps growing as web innovation gets further and further in front of what you can do on the wireless networks."

In the words of another commentator:

"A developing any kind of mobile application is a tarpit. A tarpit of misery, pain and destruction."[9]

Despite the success of more open platforms – particularly the web and the personal computer -- wireless carriers continue to impose extensive conditions and controls the development of applications for their networks. Some is a response to the technical challenges posed by mobile devices and wireless networks. In addition, the variety of platforms and equipment manufacturers creates particular challenges. However, some of the problems can be attributed to the practices of carriers and their approaches to wireless applications.

Open Development Platforms

The personal computer, and internet are a national success story. A major key to the economic success of the personal computer, the internet and the world wide web has been the ability of firms to address large consumer markets directly, without intermediation. Firms like Amazon, eBay, Yahoo and Google began with modest investments and simple web sites. The easy-entry market for applications has led, of course, to a mix of successes and failures. But it has also made the internet and the web a locus of innovation and economic growth that has made a huge contribution to the world.

As we shall see, wireless carriers have taken a different path -- the "Walled Garden" of AOL lineage. They have through a variety of mechanisms controlled what applications may be used on mobile platforms. These next sections explain how those limits work.

A hallmark of the software development environment for personal computers or web applications are (1) permissionless entry, (2) relatively low costs of market entry, and (3) open standards to write to that would work on many platforms.

We need examine how, first, these work together. Today, a web developer can develop a new application without seeking the permission of

[9] http://www.itconversations.com/shows/detail810.html

any carrier, the world wide web, or operating system owner. A new web-site – say www.reddit.com – can be launched without "clearance" from any carrier or owner. Similarly, applications for the major operating systems, Linux, Apple, UNIX and Microsoft Windows -- can be written without the permissions of the companies or authors of those systems.

Second, the costs of developing for these markets, while not zero, have been relatively low. Obviously a developer needs a degree of computer expertise and computer equipment to write a new applications. However, that has not prevented hobbies from becoming multi-national corporations. eBay, for example, was run as a hobby-site before becoming a multi-billion dollar concern. The amount of start-up capital required was sufficiently low that the business could be launched as a part-time job. eBay is an extreme example, but the history of the personal computer and the internet is full of example of low-cost market entry. Microsoft was a tiny concern when it wrote MS-DOS. Yahoo was a graduate-student project. Similar examples are legion.

What contributes to keeping the costs of market entry low are the presence of open standards that are shared across many platforms. Without entering into too much technical detail, presently, a web or computer developer can "write once" and expect their program to work on a reasonable numbers of platforms. A web developer, for example, can expect his or her web site to function on most of the networked computers in the world.

In the wireless world, today, application entry is both permission-based and more expensive than either the computer or internet platforms were or are today. Many factors contribute to making that so.

Difficulties for Developers

The view of many application developers is that the mobile applications market is stalled, or much less active than it might be. Developers describe many reasons, though three are dominant.

First, the sheer number of mobile platforms -- the variety of cell phones, each with varying operating systems, and different implementations of JAVA and BREW, the main development environments. The lack of uniformity raises development costs, as developers need spend considerable resources making sure that even a simple wireless application works on a reasonable portion of the cell phone platforms.

Second, are the carriers; qualification and approval requirements. Each of the carriers have extensive qualification procedures to become a

developer for their cell phone platforms. Becoming a registered developer is expensive, and obviously can impede development by very small and hobbyist developers.

For example, most though not all, of Verizon Wireless's telephones run the BREW development environment, one of two commonly used for mobile telephones. BREW, as implemented, requires an extensive and expensive three-stage process to develop applications. It requires (1) prequalification of both individual developers, (2) a rigorous process of testing for all applications, and (3) individual submission of each application to Verizon for approval and a potential contract.

Developers uniformly say that BREW and JAVA applications must be cleared to bypass the application-locks placed on most phones. While there are reasons to value security on a mobile platform, the process can be sufficiently extensive as to seriously impede development. Developers also complain that minor changes to the product require the initiation of new "clearance" process, impeding the constant improvement which is the hallmark of PC development.

Third, developers complain that carriers and even equipment makers do not make available many of the most useful APIs, or reserve them for some developers over others. In the words of one developer, "If you are a J2ME [JAVA] developer you'd be shocked at the number of capabilities that get locked down for no fucking reason. Serial port access, bluetooth access, location, internet access with encryption, the list goes on…"

A good example are geolocation tools. The GPS capabilities of built into an increasing number of mobile platforms suggest all manner of interesting application possibilities. However, developers report that for many platforms, the appropriate API's for using locational functions are not made available, or made available selectively to developers who are favored or have a good relationship with the carrier. These matters may be addressed, in time, by better standardization, but at present developers report that trying to dolocational capabilities remain a problem.

It is interesting to contrast the present mobile development environment with that of early computer platforms, such as the early Apple II. The Apple II of the late 1970s was, like the mobile phone, a developed platform of limited capabilities. However it gave its users a native development environment (BASIC and Assembler) and had no particular prequalification or approval rules, and thereby became a major platform for innovation. As it stands many mobile platforms have been much less hospitable to innovation than the Apple II.

Part III: Analysis & Recommendations

In the telecommunications policy community, wireless carriers have fallen into a special category for various reasons. First, the industry is comparatively competitive—there are four major competitors in most markets, as compared with the typical local monopoly in cable or telephony, or the duopoly in wireline broadband services. Second, the industry is relatively new, compared, for example, with the personal computer or even the development centered on the world wide web.

Many of the industries' current practices may have been easier to justify when the industry was in its infancy -- as a kind of subsidy to support expensive network deployments. In other words, an *infant industry* argument supported the allowance of the various discriminatory practices undertaken. Yet as the industry matures, some of the distortionary effects of industry practices are becoming more apparent.

Rating the Carriers

Based on the investigation undertaken here, it is easy to rate the carriers on the degree to which they respect Carterfone, network neutrality, and open platform development principles. Broadly speaking, Verizon Wireless scores the worst across every category, while T-Mobile score the best. Cingular and Sprint are somewhere in the middle.

Verizon Wireless

As already documented, Verizon engages in the broadest range of discriminatory, anti-competitive, and misrepresentational behavior. It violates *Carterfone* by blocking unaffiliated network equipment. It imposes what appear to be the most restrictive crippling of telephones in the industry, crippling Bluetooth and blocking WiFi capable phones. Its development environment, BREW, is very strictly limited. Its wireless broadband services, advertised as "unlimited," come with extensive usage limitations, violating core network neutrality principles.

Cingular

Cingular is a GSM carrier, and like T-Mobile, locks its phones to the Cingular network. Cingular's broadband data service is provided with restrictions similar to Verizon's. However, accounts of enforcement are not as common. Cingular's smartphone platform, the Nokia E61, has crippled the WiFi capabilities available in the E62.

Sprint

Sprint is a CMDA carrier, like Verizon, but does not whitelist phones -- it allows unaffiliated CDMA phones to be used on its network. Sprint's Wireless broadband data services are provided with fairly reasonable restrictions, similar to those imposed by dial-up operators. Sprint, however, has led efforts to cripple Bluetooth on various platforms, and generally consented to the blocking of WiFi.

T-Mobile

T-Mobile, like Cingular, locks its telephones, though it allows customers who are aware of what "locking" is to request unlocking after owning their phones for 3 months. T-Mobile seems to offer the least crippled Bluetooth capabilities in the industry. It is also the only carrier, as of October 2006, to have publicly made available WiFi-capable telephones.

Recommendations

1. *Carterfone for Mobile Platforms*

As described above, *Carterfone* was and still is among the most fundamental rule in telecommunications policy -- the "First Amendment" of telecommunications competition. Of the various potential actions, possible, adapting *Carterfone* to the mobile world is likely to have the greatest positive consequences, and the minimum negative side-effects.

In light of existing practices, what *Carterfone* means for the mobile industry is fairly clear. It means two existing carrier practices must stop:

* whitelisting carrier-affiliated telephones, allowing for inter-connection of all compliant network equipment to the network;

* "locking" of GSM equipment to single networks.

These two implementations of *Carterfone,* should be expected, over time, to transform the wireless equipment industry, along the same lines of the fax, answering machine, and PC industries in the 1970s and 1980s.

2. Broadband Wireless Restrictions

Back in the early broadband / Network Neutrality disputes of the early 2000s, discriminatory terms of service and blocking of applications were both

strongly condemned by Chairman Michael Powell and the Federal Communications Commission. These measures were essential to the launch of VoIP companies from Vonage to Skype and even arguably others like YouTube.

[Four freedoms]

Today, regulators should turn the same general scrutiny on the practice of wireless carriers who ban the use of many applications on their networks. As pointed out in the broadband context, such discriminatory bans risk warping application development, by discouraging the use of some applications over others. If the carriers' true goal is managing bandwidth, that ought be made explicit.

Similarly, in the same vein, the daily or monthly bandwidth limits on wireless broadband services should be made clear. Advertising as "unlimited" service, a service that is quite limited, is clearly misleading, regardless of the fine print.

3. Application Development

It is doubtful that government can play any useful role in this area, but it is clear that the mobile application environment is not what it could be. Over-demanding developer qualification requirements, inconsistent operating systems, and overly-restrictive controls on developers have made what might be a flourishing jungle of mobile applications much more of a desert.

This paper suggests that the carriers and equipment manufacturers ought heed the many, many requests from developers to liberate and standardize mobile application development. Some seem to be making efforts to do so. For example, Nextel, before merging with Sprint, made efforts to make widely available its APIs for developers. However, developers generally complain that carriers continue to create various barriers, some passive, and some actors, to the open development of applications for the wireless market.

Conclusion

In many respects the mobile market is and remains a wonder. Devices that were science fiction thirty years ago are now widely available to consumers. But the infancy of the wireless market is now passing, making greater public scrutiny of industry practices more appropriate.

References

[I have conducted numerous interviews, many on background. How can we handle the reference issue?]