Before the

DEPARTMENT OF COMMERCE
Office of the Secretary
National Institute of Standards and Technology
International Trade Administration
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Cybersecurity, Innovation and the Internet Economy	)	Docket No. 100402174-0175-01
	)	
	)	

COMMENTS OF CTIA—The Wireless Association®

I. INTRODUCTION

CTIA—The Wireless Association® ("CTIA"),[1] respectfully submits the following comments in response to the Department of Commerce's Internet Policy Task Force Notice of Inquiry ("NOI") regarding cyber security.[2] CTIA provides these comments to share the wireless industry's perspective and experience regarding cyber security, namely that:

- Strong incentives for protecting against cyber threats already exist in the dynamic wireless ecosystem;
- Network management techniques must remain flexible and focused on the realities of network activity;
- Voluntary industry efforts have been largely successful in establishing practices and techniques for protecting wireless networks; and
- Mobile network operators must be able to effectively manage components at the edge of their networks to prevent cyber threats and avoid interference issues.

The wireless industry is subject to fierce competition, which has created powerful market

[1] CTIA – The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization covers Commercial Mobile Radio Service ("CMRS") providers and manufacturers, including cellular, Advanced Wireless Service, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

[2] *See* Department of Commerce, *Cybersecurity, Innovation and the Internet Economy*, 75 Fed. Reg. 44,216, Notice of Inquiry (July 28, 2010) ("NOI"). Although CTIA recognizes that the NOI's primary focus is on "enhancing the cybersecurity practices of commercial actors, consumers, and citizens outside the [critical infrastructure and key resources] sectors," the NOI touches on several issues of interest to the wireless industry.

incentives for service providers to promote security and safety on their networks. For years, CTIA has administered a variety of programs addressing network security, including steps to secure data stored in networks from disclosure and attack and meeting monthly to discuss trends in illegal data access and other suspicious activities. As the Internet Policy Task Force ("Task Force") makes policy recommendations, it should be mindful of disrupting the strong incentives that already exist for commercial actors and take care not to obstruct the flexibility commercial entities require to appropriately and dynamically protect their customers.

II. COMPETITION AND THE DESIRE TO PROTECT CONSUMERS PROVIDE AMPLE INCENTIVES TO ENSURE AN EFFECTIVE CYBER SECURITY FRAMEWORK.

The NOI asks whether existing incentives are adequate to address the current cyber security risk environment and what initiatives are already under way that have successfully created incentives to make security investments.[3] Robust competition within the wireless industry has created a market imperative to remain constantly vigilant in providing the most effective and innovative cyber security to wireless consumers. Successfully meeting this challenge requires service providers to be both proactive and responsive to changes in cyber threats and/or consumer usage patterns. The wireless industry has bolstered the efforts of individual service providers through the development of industry best practices and participation in other voluntary partnerships focused on addressing cyber security issues. The Task Force should look to this model of voluntary efforts supported by market-based incentives as providing an effective framework for emulation by other industries and sectors.

A. Incentives for Cyber Security Already Exist in the Wireless Marketplace.

The wireless industry serves as a worthy model of a sector that has effectively embraced the need to ensure cyber security because of the substantial market incentives that foster a culture

[3] *Id.*, 75 Fed. Reg. at 44,222.

of innovation and investment. In every aspect of the dynamic wireless ecosystem, competition fuels research and development. It also fuels the need to protect consumers. From the development of cutting-edge devices to the provision of reliable service, the wireless industry ecosystem is constantly striving to deliver a superior product that serves customer demands and interests.

As a result, cyber security is a core aspect of the network management activities of all wireless service providers. Service providers have extensive market incentives to invest in state-of-the-art cyber security measures. Indeed, these service providers recognize that cyber security is a competitive necessity in today's broadband marketplace. With approximately 25% subscriber churn in 2009,[4] network operators compete on every available playing field. In addition to price, network coverage, and devices, reliability and quality of service are key considerations for wireless network operators as they strive to attract and retain subscribers. These market realities create effective incentives for wireless network operators to take cyber security seriously and to constantly stay ahead of the curve – more than any regulatory initiative or government program could hope to accomplish.

Cyber security threats such as spam, viruses, and botnets have the potential to affect wireless networks through unwanted network traffic and malicious code that could damage the network, endanger subscriber data, or otherwise diminish the broadband user experience. Because they are so rare, major wireless broadband security breaches receive significant attention. True mobile broadband is nascent, with carriers providing Third Generation ("3G") services that are competitive with wireline broadband services in many portions of the country

[4] Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, including Commercial Mobile Radio Services, WT Docket No. 09-66, *Fourteenth Report*, FCC 10-81 at 9-10 (rel. May 20, 2010). "Churn" refers to the number of subscriber disconnects relative to the total subscriber base. In the wireless industry, this metric typically represents subscribers changing service providers.

and beginning to deploy Fourth Generation ("4G") wireless broadband services that will, for the first time, replicate (and in some cases surpass) the broadband speeds and experience that many users enjoy on traditional wireline home broadband networks. It is essential that users trust the security of their personal information if adoption of next generation wireless broadband networks is to flourish and if carriers are to see a return on their substantial investments.

Unless service providers actively anticipate and respond to cyber security threats, consumer confidence in those providers will wane, leading to a loss of subscribership and revenue. As such, ensuring network security is extremely vital for wireless network operators, and these activities have become standard components of the services provided. For example, one form of network management that consumers have come to expect and embrace is spam blocking, which wireless carriers provide for both email and text messaging.[5] However, service providers are constantly engaged in a variety of other proactive safeguards, such as monitoring traffic patterns from known origins of malicious code, and tracking the trends and flows on the network ports themselves. These transparent activities, largely provided to subscribers without additional charge, effectively prevent many cyber threats from ever reaching wireless consumers.

B. Network Management Techniques Must Be Flexible and Keyed in to the Realities of Network Activity.

The NOI inquires as to whether government-endorsed minimum performance standards for cyber security are necessary.[6] The greatest challenge in cyber security is that the threats often change more quickly than the techniques used to combat them. Wireless network operators must be prepared for countless varieties of attack. Under these conditions, wireless service

---

[5] *See, e.g.*, *More Good News for Wireless Consumers*, Blog Post of Christopher Guttman-McCabe, Aug 31, 2010 (noting that, despite carriers' aggressive efforts to protect against spam, stronger regulatory enforcement to combat and deter these third party violations of the TCPA and CAN-SPAM Act is necessary), *available at* http://www.ctia.org/blog/index.cfm/2010/8/31/More-Good-News-For-Wireless-Consumers.

[6] NOI, 75 Fed. Reg. at 44,222.

providers and other commercial entities require the flexibility to be innovative and dynamic in their responses to cyber threats. Any government-established fixed standards or practices (even minimum standards as suggested by the NOI) likely would soon be outdated by the swift development of cyber threats and could result in vulnerability rather than an effective safeguard.

The time and compromises inevitable in agency processes of setting government standards risk the obsolescence of those standards and may not facilitate the needed nimble, rapid response and development of new protective cyber security measures. Proactive thinking and dynamic protections are necessary to guard against the evolving cyber threat. Yet, service providers and other commercial entities may be forced to direct resources towards abiding by government-set standards that may hamstring other, more effective initiatives. Equally troubling is the potential for any government-mandated cyber security standards to provide a roadmap to the defenses and vulnerabilities of commercial enterprises that could be exploited by would-be cyber malfeasants. The need for flexibility is particularly acute in the mobile context, where network operators have unique concerns imposed by the temporal and geographic nature of network use in a spectrally-constrained environment. Rather than expending valuable government and private sector resources on developing standards that are likely to be at least partly irrelevant before they are completed, the Task Force should look to endorse more effective approaches to improving cyber security.

Despite the best efforts of service providers, complete protection from every potential cyber threat is not possible. Vulnerabilities exist by virtue of risky user behavior and third party behavior outside the control of wireless service providers. For example, smartphones increasingly include Wi-Fi connectivity that offers users the ability to connect to the Internet wirelessly without utilizing licensed commercial carriers' spectrum. However, when users

choose to connect over unsecured third party wireless networks, commercial wireless service providers have no visibility into or control over the network traffic to which users are exposed. Similarly, the open nature of the Internet and the explosion of applications and introduction of multiple app stores mean that users often have access to third party applications that may contain hidden vulnerabilities or might even be masks for malicious code. In these and many other cases, cyber attacks are preventable if users take appropriate precautions. Ultimately, the best defense, as a supplement to reasonable dynamic network management, is to educate wireless consumers as best as possible about new threats and safe network usage. CTIA and its member companies actively engage in such consumer education campaigns,[7] and this is an area worthy of further investigation to determine the role the Department of Commerce and other governmental bodies could play.

C. Voluntary Industry Efforts Have Been Largely Successful in Establishing Practices and Techniques for Protecting Wireless Networks.

The success of the wireless industry's cyber security practices is best evidenced by the relative lack of major exploits of cyber vulnerabilities on wireless broadband networks to date. When security breaches have occurred, they have largely been addressed quickly, effectively, and transparently. Yet, the wireless industry is not resting on its laurels. Efforts to develop and implement improved cyber security best practices have been ongoing for years within the industry, and continue in earnest. The example of the wireless sector's leadership in voluntary industry efforts and in numerous public-private initiatives should be instructive for the Task Force as it considers the appropriate means for other sectors to bolster their cyber security efforts.

---

[7] *See infra* Section II.C. *See also, e.g.*, Comments of AT&T, Inc., GN Docket Nos. 09-47, 09-51, 09-137 at 40-41 (filed Nov. 12, 2009) (discussing internal programs and external partnerships); Connect Safely, http://www.connectsafely.org/; NetSmartz.org, http://www.netsmartz.org; StaySafeOnline.org, http://www.staysafeonline.org/.

CTIA, as the premier trade association for the wireless industry, has taken a leadership role in organizing industry participation in security-related collaborations. Over the past 15 years, CTIA has administered a variety of programs that deal with different aspects of network security. Wireless carriers manage and maintain the largest private key security systems in the world, and when they established these systems to prevent access fraud in the 1990s, they underwent extensive security audits, then developed the systems, programs and security culture required to secure these keys and other valuable data stored in their networks from disclosure and attack. Carriers developed and shared best practices on password security, access controls, and life-cycle management of security keys. They were early adopters of new and evolving technologies including multi-token authentication credentials, advanced firewalls, intrusion detection systems, and "push" software patching. For over a decade, CTIA has convened a group that monthly discusses trends they observe attackers using in their attempts to steal service, illegally access data, or use social engineering to trick customers or employees. The group reports on suspicious activities and successful strategies to combat these attacks with their carrier counterparts.

Additionally, CTIA has convened a Cyber Security Working Group comprised of members to address key areas of concern in this area. CTIA has designed and administers a Business Continuity/Disaster Recovery program that certifies industry members' response plans in the case critical service interruptions, including in the case of a large-scale cyber attack. The main elements of this program are detailed in an attachment to this filing.[8] Through this program, wireless service providers have integrated cyber security planning into their business practices, assessing potential risks and developing appropriate responses. The wireless industry also has the benefit of detailed best practices that can be customized for each service provider's

[8] *See* Attachment 1.

particular circumstances. For example, the industry participated actively in the work of the Federal Communications Commission's ("FCC") Network Reliability and Interoperability Council ("NRIC"), which issued over 200 recommendations pertaining to cyber security.[9] Furthermore, last year the FCC re-chartered the council as the Communications Security, Reliability, and Interoperability Council ("CSRIC"), which, among other tasks, is reviewing and supplementing the NRIC recommendations to ensure that a set of effective and relevant cyber security best practices are available to all. CTIA and several wireless industry members are actively collaborating with the CSRIC, including members with representation on the CSRIC Working Group 2A dedicated to reviewing the cyber security best practices.

The wireless industry partners with dozens of federal and local governmental agencies and nonprofit organizations to address various aspects of cyber security and network reliability. This participation ranges from assisting the Department of Homeland Security in developing the National Infrastructure Protection Plan ("NIPP"), to working closely with the National Communications System ("NCS") and the United States Computer Emergency Readiness Team ("US-CERT") to share information regarding unusual activities and to fortify communications networks. Industry members also are significant contributors to direct consumer education campaigns such as the National Center for Missing and Exploited Children's NetSmartz.org, the National Cyber Security Alliance's StaySafeOnline.org portals and ConnectSafely.org. These various voluntary efforts have resulted in the development of a broad array of strategies, partnerships, and best practices that work together to ensure, to the greatest extent possible, the security of wireless broadband networks.

[9] *See* "NRIC Best Practices" https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm (last visited Sept. 10, 2010).

CTIA also educates children and teens on maintaining a safe Internet experience through the "Be Smart. Be Fair. Be Safe: Wireless Responsible Use" campaign, as well as complementary initiatives with entities such as Common Sense Media and the Illinois Attorney General's Office. The campaign aims to equip parents and teachers with tools to teach kids about responsible mobile device use, including behavior that could lead to misuse or abuse of a mobile device and user information.[10]

III. MOBILE NETWORK OPERATORS MUST BE ABLE TO EFFECTIVELY MANAGE COMPONENTS AT THE EDGE OF THEIR NETWORKS TO PREVENT CYBER THREATS AND AVOID INTERFERENCE ISSUES.

Even where users act responsibly and all relevant best practices are followed, effective security relies upon wireless service providers retaining the flexibility to manage their entire networks effectively, including the devices attached to those networks. The wireless industry is subject to unique technological and physical constraints that demand particular flexibility and control by the network operator. Because of the interconnected nature of wireless networks, this increased flexibility is essential to successful network operations.

Mobile wireless broadband networks are distinct from traditional wired broadband and even most fixed wireless residential broadband networks in that the network edge extends all the way to the consumer device.[11] In a conventional DSL or cable broadband network, the service provider's Internet access network terminates at the broadband modem. From that point, the user's PC or other device receives the Internet access services through an RJ-45 Ethernet connection to the modem, or perhaps through a Wi-Fi connection to a wireless router, constituting the user's private home network. In this situation, if the user device malfunctions,

[10] *See* http://www.besmartwireless.com/.

[11] For a more detailed discussion of how wireless handsets are part of the overall wireless network, *see* Charles L. Jackson, "Wireless Handsets Are Part of the Network" (Apr. 27, 2007), provided herein as Attachment 2.

the commercial broadband network is protected from harm by the existence of a controlled access point—typically the DSL or cable broadband modem.

By contrast, in the mobile broadband context, there is no such controlled access point between a wireless device and the network on which it operates. The network extends all the way to and includes the user device, which communicates directly with the network infrastructure. Moreover, because mobile broadband networks function in a shared spectrum environment where multiple devices operate over the same frequencies in the same area, a serious malfunction or breach in a single device has the potential to interfere with the operations of multiple other user devices. Indeed, a malfunctioning radio can even interfere with devices operating on competing wireless networks in adjacent spectrum bands. It is for these reasons that in the mobile context, wireless radios are legally licensed to the network operator, not individual users. CTIA has provided detailed information to the FCC concerning the need for adequate network control and management that describes the critical importance of such efforts.[12]

For any cyber security practices to be effective in mobile broadband networks, it is essential that network operators maintain the flexibility to manage their networks to protect against potentially harmful components. Any efforts by the Federal government to limit network operators from effectively managing their networks will greatly inhibit the ability to ensure secure communications on wireless networks.

[12] *See, e.g., In the Matter of Framework for Broadband Internet Service*, Federal Communications Commission GN Docket No. 10-127, Comments of CTIA—The Wireless Association (filed July 15, 2010); *In the Matter of Preserving the Open Internet, Broadband Industry Practices,* Federal Communications Commission GN Docket No. 09-191, WT Docket No. 07-52, Comments of CTIA—The Wireless Association (filed Jan. 14, 2010).

IV. CONCLUSION

Due to the combination of substantial market incentives, dynamic management of networks and business practices, and the success of voluntary collaborative efforts, the wireless industry has developed a constantly evolving core of knowledge, techniques, and best practices that have promoted effective cyber security throughout the industry. Any policy recommendations by the Task Force should seek to preserve the flexibility and independence of the various commercial sectors, and make room for the development of similarly customized and organic strategies, rather than prescribing overly rigid government standards.

Respectfully submitted,

By: */s/ Brian M. Josef*

Brian M. Josef
Director, Regulatory Affairs

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President and General Counsel

CTIA—The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

September 13, 2010

Attachment 1

ELEMENTS OF CTIA – THE WIRELESS ASSOCIATION'S VOLUNTARY BUSINESS CONTINUITY / DISASTER RECOVERY PROGRAM

ELEMENTS OF CTIA – THE WIRELESS ASSOCIATION'S VOLUNTARY BUSINESS CONTINUITY / DISASTER RECOVERY PROGRAM

Requirement 1: Project Initiation and Management

Companies must demonstrate that they have done the following:

Defined objectives

Developed project plan and budget

Defined and recommended process structure and management

Obtained senior management commitment

Requirement 2: Risk Evaluation and Control

Companies must demonstrate that they have done the following:

Identified risks, events, and external surroundings that can adversely affect the company

Evaluated the damage that such risks and events could cause and probability of occurrence

Identified controls and safeguards to prevent or mitigate losses to company

Requirement 3: Business Impact Analysis

Companies must demonstrate that they have done the following:

Identified the critical functions of the organization

Identified the impacts resulting from disruptions and disaster scenarios

Determined recovery priorities and timeline objectives

Requirement 4: Developing Business Continuity Strategies

Companies must demonstrate that they have done the following:

Selected business recovery operating strategies

Assessed risk associated with each optional continuity strategy

Requirement 5: Emergency Response and Operations

Companies must demonstrate that they have done the following:

Developed and implemented procedures for response to situations

Established a process for activation of an Emergency Operations Center

Integrated Disaster Recovery/Business Continuity procedures with Emergency Response procedures

Established Command and Control procedures

Requirement 6: Developing and Implementing Business Continuity Plans

Companies must demonstrate that they have done the following:

Established and implemented Business Continuity and Crisis Management plans

Established procedures to transition from emergency response to crisis management / business continuity

Established a procedure to maintain and update Business Continuity plans

Requirement 7: Awareness and Training Programs

Companies must demonstrate that they have done the following:

Established a process to educate the company regarding business continuity issues and programs

Developed and presented training programs

Requirement 8: Exercise Business Continuity Program

Companies must demonstrate that they have done the following:

Established a process to drill/exercise the Business Continuity / Disaster Recovery program

Organized and completed exercises/drills

Developed and monitored after-action reports and results of exercises

Requirement 9: Public Relations and Crisis Coordination

Companies must demonstrate that they have done the following:

Developed plans to communicate with employees and management

Developed process to communicate, if necessary, with other stakeholders

Requirement 10: Coordination With External Agencies

Companies must demonstrate that they have done the following:

Established applicable procedures and policies for coordinating response with government representatives

Attachment 2

CHARLES L. JACKSON
"WIRELESS HANDSETS ARE PART OF THE NETWORK"

Wireless Handsets Are Part of the Network

Charles L. Jackson
27 April 2007

An earlier version of this report was presented at the 16th ITS Biennial Conference held in Beijing, China, in June 2006. I wish to thank CTIA for support in developing this report.

Table of Contents

1. Overview and Summary

Regulators, competition policy authorities, professed competitors, and class-action plaintiffs have all attacked the joint provision of wireless service and wireless handsets as well as the use of various contractual and technical arrangements that bond a handset to a specific service provider. The arguments raised against these practices often are the usual objections to the tying or bundling of a monopoly product with a competitive product.[1] Many of the discussions of such tying focus on purely economic issues—such as consumer preferences for time payments for equipment purchases.[2]

However, discussions of the wireless industry have failed to examine all dimensions of the handset–network relationship. In particular, discussions of handset tying and bundling have not addressed the extent to which handset capabilities are a substitute for investment in the network. It is well understood that wireless handsets can be regarded as complements to the network. However, it is not generally understood that handset capabilities can also be a substitute for network investment. In practice in today's wireless networks, the handset and the network are not two separate products—as are automobiles and gasoline or shoes and shoe polish—but are aspects of a single product. Most important, purchase of improved equipment by one subscriber can improve service for other subscribers. Handsets are part of the wireless network, and the performance of handsets has substantial static and dynamic efficiency implications for the operation of the network as a whole. Investments in handsets can reduce the investment needed in the rest of the network. Hence, a wireless service provider has strong incentives to control the technology used in handsets in order to create an efficient network as well to manage network evolution. Handset subsidies and various forms of tying and bundling are reasonably efficient tools for such control.

Closely related to efficiency concerns are social concerns. Earlier analyses of handset sales practices have not addressed the extent to which handset supply by service providers is helpful or even necessary for meeting social goals such as supporting

---

[1] Such concerns are raised even though wireless service is not a monopoly.

[2] See, for example, "Bundling, Tying, and Portfolio Effects, Part 2 - Case Studies," DTI Economics Paper No. 1, Barry Nalebuff and David Majerus, February 2003.

emergency services, deterring theft, or providing service to persons with disabilities. In the United States, the FCC has required wireless service providers to meet certain social goals—goals that can only be met if the handsets used on the service provider's networks have specific capabilities. Bundling handsets with wireless service is a simple and efficient mechanism for ensuring that handsets have the technical characteristics needed to meet the regulatory requirements. For example, the incentives for handset theft are substantially reduced if it is difficult or impossible to activate a stolen handset.

This paper reviews wireless network technology and discusses the various ways in which handset capabilities affect overall network efficiency and network evolution. It focuses on the wireless industry in the United States but also considers the general case. It also discusses social concerns, such as support for E911 service and the issue of handset theft. Finally, it considers alternative approaches to ensuring that handsets are efficient matches with the network and offers some concluding thoughts.

1.1. Efficiency

Wireless handsets interact with the network in a fashion quite different from the way that wired telephone handsets do. Unlike the case in wired telephony, in modern wireless telephony the features and quality of the handsets used on the network have a substantial impact on the cost and quality of the wireless service, not only for the individual subscriber but for all consumers. If John uses an inferior wireless phone—even if that inferior phone was state-of-the-art five years ago—he may deny service to Mary who is sitting next to him or may degrade service for other users a mile away. In contrast, if one uses a poor quality wireline handset, it does not degrade one's neighbor's wireline telephone service.[3] In the economist's jargon, poor-quality wireless handsets can easily create substantial negative externalities but poor-quality wireline handsets are extremely

[3] The nature of harms to the network from consumer provided terminal equipment in the wired telephone network was extensively investigated in the early 1970s. The conclusion of those investigations was that, in the vast majority of typical instances, the harms from inferior terminal equipment were imposed on the user of that equipment and on those who wished to call him or her. With a few exceptions, such harms did not impact others using the network. Furthermore, relatively simple protective connecting arrangements or certification of equipment could provide substantial protection against harms to the network. However, in the case of party lines—in which the telephone line is shared as is a wireless link—there are additional potential harms with no easy solution. Consequently, the FCC has never ordered that customer-owned equipment can be connected to party lines. See 47 CFR 68.2(a).

unlikely to do so. Widespread use of inferior handsets would substantially degrade wireless service—such as by increasing the number of coverage holes and dropped calls—or would require a significant increase in the capital plant used by wireless carriers. In either case, consumers—even consumers with superior handsets—would suffer. Wireless carriers have strong incentives to ensure that consumers use handsets that economize on the total costs (capital costs and handset costs combined) of the network.

1.2. Innovation

The wireless industry has seen enormous innovation and technical advancement over the last two decades. Many of these innovations have made the networks more efficient—expanding capacity and avoiding the otherwise rigid limits on capacity imposed by the finite spectrum made available for wireless service. Innovations have also made new service capabilities, including data applications, available to consumers. Implementing such innovations requires interaction between the network and handsets to an extent that is unparalleled in wireline telephony. Seeding the market with handsets providing expanded capabilities is an essential step in fostering the rapid adoption of more efficient or more capable wireless services. Adoption of capacity-expanding innovations would be far slower if carriers did not provide and subsidize handsets supporting new capabilities. Similarly, the adoption of new services would also take longer absent carrier support of handset supply.

The contrast to the wired telephone network is striking. The wired telephone industry adopted a standard interface between telephone instruments and the network no later than 1950. When new technologies, such as electronic central offices or digital loop carrier, were introduced into the telephone network, the new equipment was built to work with the existing wires and telephone instruments. When new telephone equipment was designed, it was built to work with the existing network. The only significant change to the wired telephone interface since 1950 that I am aware of was the introduction of touch-tone dialing. Although extensive innovation occurred both inside the network and in the terminal equipment, the standard interface remained in place for telephone instruments. For example, in the long-distance network microwave replaced copper,

fiber replaced microwave, digital replaced analog, and so on. All the same, a telephone that was new in 1957 can be connected to the network today and will work fine.[4]

1.3. Security

Various security features built into modern wireless handsets make cloning, fraud, and activation of stolen handsets far more difficult than was the case with earlier technologies. In particular, locking a handset to a network makes theft almost pointless. One reason for adopting such features was the request by responsible law enforcement agencies, including the Federal Bureau of Investigation and the British government, that wireless handsets be resistant to cloning and to easy activation after theft or robbery.

1.4. 911, E911, and TTY Support

The FCC imposes several requirements on wireless carriers to support 911 calls. For example, wireless carriers must deliver all 911 calls—even calls placed by nonsubscribers. The FCC also requires wireless carriers (1) to provide the location of wireless callers to 911 to the affected public safety access point (a capacity generally referred to as E911) and (2) to support communications from TTY devices used by the deaf. For many carriers, meeting these two requirements is possible only if handsets contain specific features and meet minimum performance standards. As is more generally true, there is a tradeoff between handset performance and network performance in providing the location information capability. Widespread consumer use of handsets that perform the E911 functions better than industry standards may be necessary for a carrier to meet its legal obligations under the FCC's E911 accuracy requirements.

1.5. Help Desk Support

Wireless carriers provide helpdesk support to their subscribers. Some modern handsets rival a personal computer of a few years ago in complexity and features. Providing helpdesk support to unfamiliar or unknown handsets is difficult and costly.

[4] Ultimately, new technologies that did not use the POTS interface, such as ISDN and DSL were introduced into the loop.

1.6. Summing Up

Multiple technical factors—with the most important probably being the fundamental role of handsets in determining overall system efficiency and capital costs—create strong, efficiency-serving incentives for wireless carriers to control the nature and characteristics of the handsets used by their subscribers.

2. Development of the Modern Wireless Industry

The rapid growth of the wireless industry has created today's wireless economy in which more than 230 million wireless phones are in use in the United States today—slightly more than two wireless phones for every three Americans.

Wireless calls require both a wireless handset and a matching wireless network. Wireless networks consist of cell sites that contain antennas, radios, and communications connections to a switching center where calls are processed and sent on to other subscribers, and a local telephone company or a long-distance company. Figure 1 shows these basic elements of a wireless system.

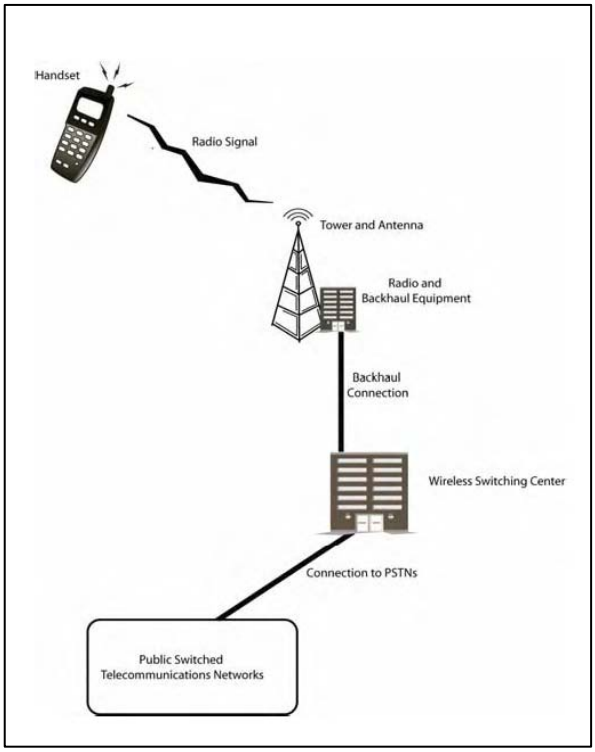

Figure 1. Elements of a Wireless Network

The modern U.S. wireless industry began in the early 1980s with the first cellular systems. These systems used an analog technology, called AMPS, that the FCC required that all cellular operators use. Cellular service turned out to be more popular than most people had forecast. Within a few years, the capacity available on the two cellular licenses was close to exhaustion in some large cities. There were two responses to this pending exhaustion: (1) the industry pressed efforts to develop technologies that could fit more calls into the spectrum available under the existing radio licenses and (2) the FCC looked for additional radio spectrum (radio channel space) that could be made available for wireless services.

Recognizing the need to permit the industry to move to more efficient technology, the FCC dropped its requirement that cellular operators use only the AMPS technology and adopted a policy of "technical flexibility" that allowed cellular carriers to use any radio technology provided it did not create harmful interference.[5] The industry responded by funding the development of new radio technologies that were more spectrally efficient—that is, these technologies enabled carriers to serve more subscribers in the same limited radio spectrum by fitting more calls into a given spectrum block. And, for business reasons, any new technologies also had to be compatible with the existing AMPS service in the sense that cellular operators had to be able to operate mixed systems—part new technology and part the old AMPS technology— during a transition period.[6]

Two system designs denoted TDMA and CDMA were developed to meet these needs.[7] TDMA was the less complex of the two systems and was developed first. CDMA was more complex but promised significantly greater spectrum efficiency. When the technologies entered the market, some cellular carriers chose TDMA, some chose CDMA, and some first chose TDMA and later converted to CDMA. Roughly speaking, TDMA increased the maximum number of subscribers that a cellular system could serve

---

5 Report and Order in Gen. Docket 87-390, 3 FCC Rcd 7033, October 13, 1988.

6 In addition, the FCC required cellular carriers to continue to support analog AMPS users. *See* 47 C.F.R. 22.901.

7 TDMA is the acronym for time-division multiple access; CDMA is the acronym for code-division multiple access. Both these acronyms are misleading in that TDMA and CDMA refer to basic technologies not specific system designs. For example, the GSM system uses TDMA technology.

by a factor of three over the AMPS standard; CDMA (as it was first introduced) increased that number by a factor of six.

As these technologies were being developed to relieve the spectrum shortage, the FCC was working to make more spectrum available for wireless service. As a first step, it made available 10 MHz of additional spectrum by increasing the two original cellular licenses from 20 to 25 MHz each—a 25% increase in capacity.[8] Later, the FCC created a new radio service, called PCS, and allocated 120 MHz (three times the original cellular allocation) of spectrum to the PCS service. PCS carriers were also given technical flexibility to choose the radio system technology that they wished to use. The first PCS system began operating in 1995, and others followed over the next few years.

Wireless was growing outside the United States as well. Initially, several service providers in Europe operated wireless systems using different, incompatible technologies. The incompatibility of these systems created great barriers to using wireless phones as one traveled around Europe. Consequently, in 1987 the European Union directed its member states to clear a common spectrum band for use by a digital cellular service and to move to adopt a single European technical standard.[9]

That standard, now known as GSM, was developed by the European Telecommunications Standards Institution (ETSI).[10] The first GSM systems went into operation in 1992 and GSM quickly became a commercial success.

---

[8] Actually, the 25% increase in spectrum for cellular carriers increased capacity by more than 25% due to trunking efficiencies made possible by having more channels.

[9] "Council Directive 87/372/EEC of 25 June 1987 on the frequency bands to be reserved for the coordinated introduction of public pan-European cellular digital land-based mobile communications in the Community," Council of the European Community. Official Journal L 196, 17/07/1987 P. 0085 - 0086: Council of the European Community, 1987.

[10] The acronym GSM stands for Global Standard for Mobile Communications. Originally, GSM stood for Groupe Spéciale Mobile—the name of a committee formed by the Conférence des Administrations Européenes des Postes et Télécommunications (CEPT). CEPT was the pan-European intergovernmental agency dealing with telephone, wireless, and postal issues. With the massive changes in Europe, including privatization of many communications administrations, the expansion of the EU, and the fall of the Soviet Union, CEPT has been reorganized since the time of the original GSM committee. CEPT's standards activities have been moved to ETSI, and the service providers are no longer members, but the Russian Federation and several other nations that were part of the former Soviet Union are now members. The founding document for GSM, the *GSM Memorandum of Understanding*, was drafted by an official of the British government, and 13 of the 15 signatories were national governments.

As they began to design systems to operate in the new PCS spectrum made available by the FCC, firms could choose from three basic system designs—TDMA, CDMA, and GSM. Naturally enough, firms that were already operating cellular systems using TDMA or CDMA tended to choose to use their current cellular technology on their PCS systems. Recognizing limitations of TDMA, PCS firms that were new entrants to the wireless industry restricted their choices to CDMA and GSM.

Of course, technological progress and market growth did not stop when the PCS systems started operating in 1995. Rapid growth in the demand for wireless service continued to make the capacity constraints of limited spectrum a significant problem for some carriers. Demand for improved data services also prompted innovation. Both the GSM and CDMA sectors responded to these pressures with new technologies. The CDMA camp developed systems with names like IS-95B, 1xRTT, EV-DO, Rev-A, and Rev-B and is developing a new architecture known as UMB.[11] The GSM world used names like GPRS, EDGE, WCDMA, and HSPA for the systems they have deployed; they are currently developing a new system standard known as LTE.[12]

Figure 2 illustrates the family tree of the major wireless standards. Earlier systems are shown at the top; later ones below. The GSM and CDMA timelines are not intended to indicate that systems at the same level were introduced at the exact same date. Similarly, I have not tried to describe all the various quality and service innovations or to describe changes that occurred without a change in the name of the standard. It is important to note that these three technologies—CDMA, GSM, and TDMA—are mutually unintelligible; a CDMA receiver cannot pickup a GSM call and vice versa.[13]

[11] Press Release, "Ultra Mobile Broadband (UMB) Selected to Describe Next Major Advancement in Mobile Communications," CDG, Hong Kong, December 5, 2006.

[12] See http://www.3gpp.org/Highlights/LTE/LTE.htm.

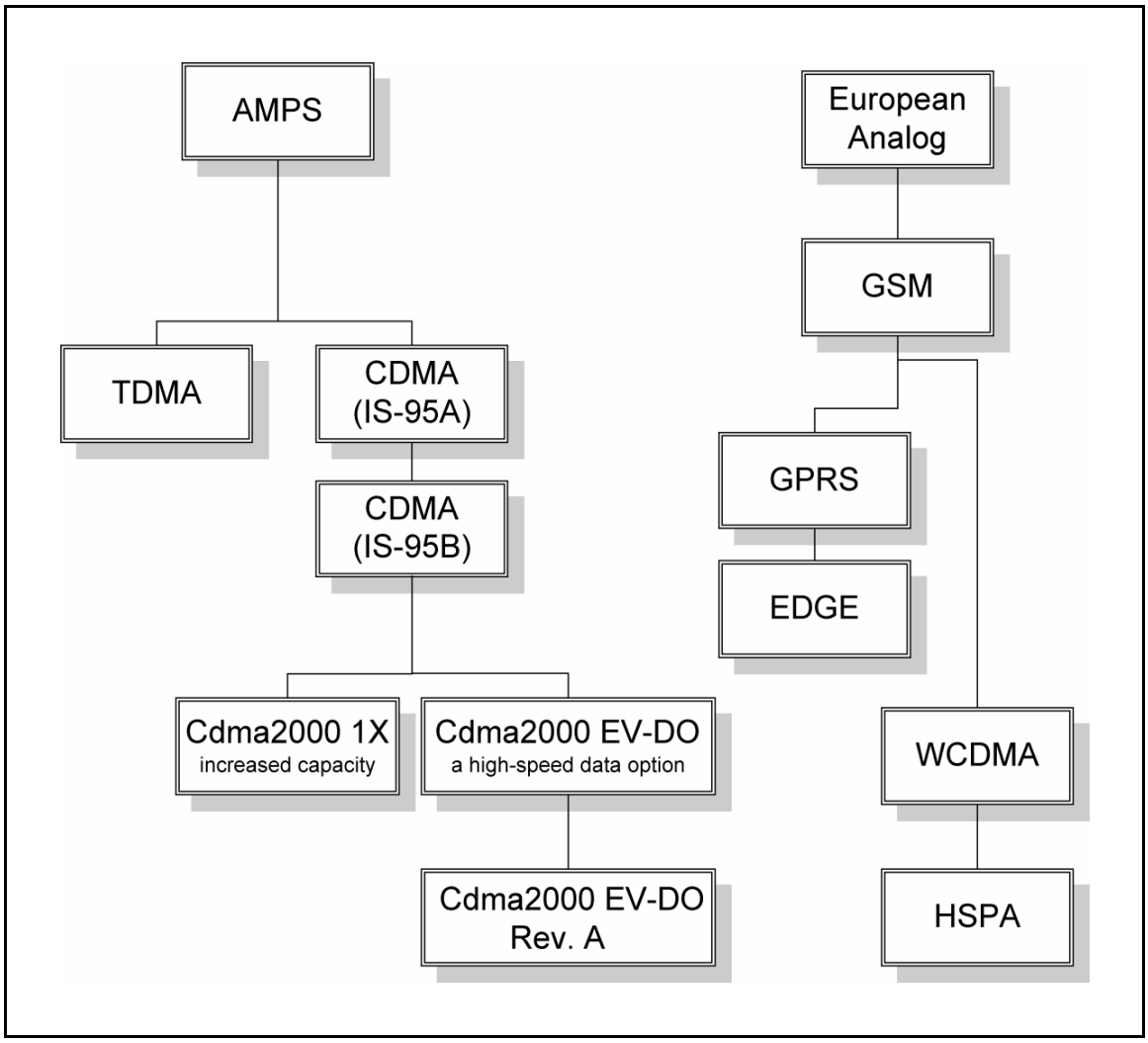

Figure 2. A Family Tree of Wireless Standards

As one moves down the family tree, one repeatedly finds an increase in voice capacity. IS-95 supports 6 to 10 times more subscribers than can AMPS in a given block of spectrum. The later-developed cdma2000 1X can support around twice as many subscribers as can IS-95. Thus, cdma2000 1X is from 12 to 20 times more efficient than AMPS. The early GSM systems were about 3 or 4 times more spectrum efficient than the earlier analog systems—current GSM systems are about 10 times more spectrum

[13] As integrated circuit technology has progressed, it has become possible to build chips that support multiple standards. For example, the QUALCOMM MSM7600 handset chip can communicate using CDMA, GSM, or WCDMA standards.

efficient. WCDMA is perhaps twice as spectrally efficient as later versions of GSM. The issue of spectral efficiency is terribly important to system operators—it determines the ultimate limit on the number of subscribers, and it is closely tied to the number of cell sites required—and thus to total network investment. Because spectral efficiency is so commercially important, it is hard to find objective measures of the capacity increases associated with a specific technology—nevertheless, the substantial growth of capacity over time is undisputed.

Handsets with cdma2000 1X capabilities can also operate on network equipment using the earlier CDMA technology, but the converse is not true—the earlier CDMA handsets cannot communicate using the 1X signals. Consequently, a wireless carrier that wants to exploit the superior efficiency of cdma2000 1X must undertake a complex transition of phasing in cdma2000 1X and phasing out the earlier version of CDMA.

I should note that another important standard wireless standard is used in North America. That is iDEN—the standard that was used by Nextel before the Nextel/Sprint merger and is now used by Sprint. This standard arose from a technical and regulatory history different from the others I have discussed. However, Nextel's network also evolved through generations of technology. That network began as an analog FM system. Later, Nextel expanded capacity by converting to the digital iDEN system. Improvements to iDEN, such as new vocoders, have further expanded capacity and improved quality.

One tool for phasing in new handsets is carrier provision of handsets with the new capabilities—the tying or bundling of handsets with service and carrier prohibitions on activating older technology handsets.

3. Handset Performance and Operating and Capital Costs

All wireless handsets use two shared resources to connect to the switched telephone network. These shared resources are the radio spectrum and the radio base station. So, for the reasons that I explain below, one person's use of a poor-quality wireless handset can impair the wireless service delivered to many others. Indeed, many shortcomings in wireless handsets affect the coverage and capacity of the wireless system. One subscriber's use of a poor-quality handset may cause another subscriber's call to be

blocked or dropped. It would be difficult or impossible for the typical consumer to see that such shortcomings were caused by faults in another subscriber's handset, rather than by faults in the network. At the same time, a consumer may not know or care if his or her handset creates external harms if that handset costs the consumer a few dollars less. That is, a consumer may not make the efficient tradeoff between the external costs created by his or her handset and the lower handset cost.

Wireless carriers are well aware of the tradeoff between handset and network capabilities. A senior manager with responsibility for handsets at Sprint told me, "We [the handset team] meet with network guys every three months just to look for network optimization possibilities."[14] Similarly, a senior manager at Cingular described the process whereby Cingular arrived at its "pretty stringent requirements on RF [radio subsystem] performance" saying "a lot of analysis went into the service calculation."[15] He described Cingular's explicit consideration of the tradeoff between investment in cell sites versus investment in handsets. The categories of handset performance that he mentioned in this context were receiver sensitivity, handset power, and use of the AMR vocoder.

3.1. Handset Attributes that Affect System Capacity

3.1.1. Receiver Sensitivity

The sensitivity of the radio receiver in the consumer handset is a good example of a handset feature that, if impaired, imposes costs on others. In CDMA systems, a base station transmits telephone calls to multiple subscribers using a single complex signal. That signal has fixed maximum power—typically near 20 watts. The base station divides that power among the various subscribers—transmitting to each subscriber at just above the minimum power needed to communicate with that subscriber. Base stations transmit at lower power to subscribers near the base station and at higher power to subscribers who are more distant or who are in hard-to-reach locations—such as deep inside

[14] Telephone conversation, 14 December 2004, Sprint.
[15] Telephone conversation , 15 December 2004, Cingular.

buildings.[16] The base station power assigned to each subscriber varies over time as the subscriber moves to locations with better or poorer reception.

The sensitivity of a handset is defined by the minimum power needed to receive an acceptable signal. Consider two handsets, A and B, identical in all respects except that handset B is less sensitive than handset A—specifically, handset B requires twice as much received power to perform acceptably. A CDMA base station designed to serve 20 simultaneous conversations to type-A handsets could serve only 10 simultaneous conversations to type-B handsets.[17] Looking at the problem another way, such a base station could serve 20 simultaneous conversations to type-B handsets only if those handsets were, on average, located closer to the base station. If one analyzes coverage using a simple and widely accepted model of radio propagation, one finds that a base station that could serve 20 type-A handsets spread over the area within 1 mile from the base station would be able to serve the same number of type-B handsets spread over an area about 30% smaller—the area within only 0.85 miles of the base station.[18] A wireless carrier could compensate for such a reduction in range by installing more base stations—in this case, approximately a 30% increase in base stations would be needed. Base stations, the backhaul equipment needed for each base station, and the termination of backhaul at the wireless switch comprise the bulk of the capital cost in modern wireless systems.[19] A 30% increase in the number of required base stations would, to a first approximation, result in a 30% increase in the capital cost of a wireless system and consequently would significantly increase the cost of wireless service.

---

[16] Handset sensitivity in CDMA systems provides a particularly clear example of a handset feature that, if poorly implemented, reduces the network performance for other subscribers. However, in the GSM standard there are handset options, such as the AMR vocoder and SAIC, that if present and activated, permit a base station to serve more subscribers or subscribers at greater distances from the base station than would be the case otherwise.

[17] This example is simplified. Many CDMA systems are limited by capacity on the reverse (mobile-to-base) link not by forward link capacity. However, were the sensitivity impairments significant, forward-link capacity would become limiting. In the high-speed data service EVDO forward link capacity is often limiting.

[18] The analysis is based on using an inverse fourth-power propagation law. The reduction in spacing is actually by a factor of 0.8409.

[19] "Backhaul" is the transportation of wireless traffic from the cellular station to a mobile switching office from which it can be sent on to its destination.

The factor of two difference in sensitivity between the two handsets discussed above is not an unreasonable difference from the point of view of practical receiver engineering. In late 2004, CTIA, the wireless industry association, filed with the FCC reports of recent tests of PCS handsets performed by independent laboratories. These tests showed, among other things, that the tested handsets were on average, able to pick up signals a factor of two weaker than the weakest signals that could be picked up by a handset just meeting the requirements of the industry standard.[20]

Closely related to sensitivity is the quality of the antenna on a handset. A poor antenna degrades handset performance in much the same way as does reduced sensitivity. Similarly, given that retractable antennas often fail, a service provider requirement that retractable antennas be field replaceable would make it easier for consumers to repair handsets with broken antennas. Easier repair would mean that fewer consumers will have handsets with defective antennas that consume excessive network resources.

3.1.2. Vocoder Performance

Another handset feature that has a major impact on network capacity is the performance of the voice compression subsystem in the handset. This subsystem, known as the voice coder or vocoder, determines how many bits per second are generated to represent a speech signal. Continuing research has resulted in the development of vocoders that perform adequately using fewer bits per second than those originally used in CDMA and GSM. These better vocoders permit more subscribers to be served over a given number of radio channels. Better vocoders expand system capacity and, if better vocoders are sufficiently low cost, the widespread use of better vocoders would lower the total cost of wireless service. Alternatively, better vocoders can be used to deliver better voice quality without requiring increased network capacity. Matching vocoders are needed in handsets and the network—a new vocoder cannot be deployed in either the handset or the network alone.

[20] Test reports of WINLAB and PCTEST attached to the comments of CTIA in Docket ET 00-258, December 8, 2004.

The CDMA standard now includes vocoders called the Enhanced Variable Rate Coder (EVRC) and the Selectable Mode Vocoder (SMR).[21] Because these are variable-rate vocoders, the network can command the handset to reduce the number of bits that are used to encode speech. The widespread use of EVRC and SMR vocoders in consumer handsets gives network operators several valuable options. First, the network operator can expand network capacity in times of emergency or sudden overload, albeit at the cost of reduced voice quality. Second, the network operator can compensate for delays in network expansion, such as might be caused by difficulty obtaining the proper zoning for a new cell site or by extended bad weather. In an area of limited coverage, such as might develop after a brush fire destroyed the equipment at a cell site, the network could command subscriber handsets to reduce the network capacity each handset uses—thereby providing more capacity for others. The industry claims that the SMR vocoder increases system capacity by 34% while delivering the same quality as the EVRC vocoder.

The GSM world has a similar variable rate capability called the adaptive multirate (AMR) vocoder. The AMR vocoder permits a carrier to serve mobiles at greater distance from a cell site or deeper inside office buildings than would otherwise be possible. The outcome is, all other things being equal, that use of the AMR vocoder expands capacity of a GSM system.[22]

A Cingular manager told me, "The transformation from TDMA [to GSM] required less investment in the network than it would have had we not incorporated AMR." He characterized an operating environment without AMR as generating "a huge hit on capacity."[23]

Closely related to the variable rate concept is the discontinuous transmission concept—the engineer's way of referring to handsets that turn off the transmitter when the user is in a conversation and is only listening but not talking. Shutting off the handset transmitter in such situations not only extends battery life but reduces the interference that the

---

[21] See http://www.cdg.org/technology/cdma_technology/vocoder/index.asp.

[22] Nortel claims that use of AMR gives a 100% increase in spectrum efficiency in dense urban deployments. See http://www.nortel.com/solutions/wireless/collateral/nn114180.pdf at p. 2.

[23] Cingular conversation cited above.

handset generates to other users on the system. GSM handsets with discontinuous transmission expand system capacity.

3.1.3. Concluding Thoughts

Receiver sensitivity and vocoder performance are two handset attributes that directly substitute for network investment. Reduced receiver sensitivity reduces the transmission range from base stations—and requires more base stations for equivalent coverage. Vocoders that squeeze a conversation into half as many bits per second double the number of conversations that can fit into a wireless system—or cut in half the electronics required at the base station. Investments in improved receiver sensitivity and vocoder performance are direct substitutes for investment in network physical infrastructure.

3.1.4. Other Handset Attributes that Affect System Capacity

Handset sensitivity is not the only handset characteristic that affects the amount of system resources that a handset will consume.

Tables 1 and 2 list some handset attributes (including receiver sensitivity, which I discuss above) that, if less than optimum, cause the handset to consume excessive system resources and thereby to reduce the wireless system's capacity or coverage. Table 1 considers attributes that affect capacity on the base-to-mobile communications link—what is often called the *downlink path*. Table 2 lists attributes that affect capacity in the reverse direction—the mobile-to-base or uplink path. These lists are not exhaustive—other attributes affect capacity as well—but these lists highlight major capacity-related attributes.

Table 1. Handset Attributes that Consume Base Station Downlink Resources

Attribute	Observations
Receiver sensitivity	A receiver's sensitivity is a measure of the minimum signal strength required to operate effectively. The transmitted power required at the base station is directly related to the sensitivity of the receivers in the handsets.
Immunity to adjacent channel interference	Wireless handsets must distinguish the desired signal from others on nearby frequencies. For example, a Verizon Wireless subscriber may operate her handset near a Sprint base station. When handsets with poor adjacent channel immunity are in the presence of a strong adjacent channel, they require more of the limited downlink power from the base station.
Immunity to co-channel interference	Multi-user detection (MUD) and smart antenna technologies permit radio receiving systems to reduce the impairments caused by interference. Pilot-interference cancellation (PIC) in EV/DO and single-antenna interference cancellation (SAIC) in GSM are such technologies.
Ability to withstand inband overload	This problem is similar to the adjacent channel problem.
Intermodulation	Radio receivers can degrade or fail when multiple unwanted signals are present. The unwanted signals combine, through a process call nonlinearity, to create an interfering signal. A handset that was abnormally prone to intermodulation problems could fail to work properly when being operated near other handsets. A perceptive user might notice that the problem occurs when near other handsets and consider those handsets the source of interference when, in fact, the true cause of the interference arose was the poor performance of the user's own equipment.
Handoff performance	Wireless handsets automatically switch from one cell to another cell as the handset is carried from the service area of one cell to that of a second cell. A handset that does not perform its tasks in the handoff process will require excessive power from one or the other of the base stations.
Out-of-band emissions	Wireless handsets contain both transmitters and receivers. The transmitters in wireless handsets generate relatively strong signals in the band of frequencies used for mobile to base communications. But, handset transmitters also emit weak signals in the bands that are used for communication from the base to the mobile unit. If such unwanted emissions were sufficiently strong, operation of a handset would degrade or prevent operation of other handsets nearby. The FCC's rules for such emissions permit signals a million times stronger than are permitted by the relevant industry standard

Table 2. Handset Attributes that Consume Base Station Uplink Resources

Attribute	Observations
Power control accuracy	CDMA-based wireless systems require that mobile handsets control their transmitted power with great care. Indeed, the highly accurate power control needed for CDMA was once regarded as an insurmountable barrier to the development of practical CDMA systems. If handsets exhibit poor power control, the capacity of the base station is reduced.
Power control range	Handsets that operate near base stations must be able to turn their transmitted signal down so that it does not create excessive interference to the signals of other handsets transmitting to the same base station. One large CDMA carrier requires that handsets be able to reduce the transmitted power to 10 billionths of a watt. A less capable handset would reduce the uplink capacity of a wireless system when it was operated close to a base station.
Modulation quality	If a handset generates a poor quality signal—one that does not clearly separate the ones and zeros transmitted—the handset will have to transmit at a higher power to compensate for the signal quality impairment. But, that handset's higher power will require other handsets to transmit at a higher power as well. Handsets near the edge of the cell, already operating near or at maximum power, will be unable to raise their power high enough to maintain contact with the base station. So such calls will be dropped or never completed.
Frequency accuracy	The effects of poor frequency accuracy in handsets are similar to those caused by poor modulation quality.
Timing accuracy	The effects of poor timing accuracy in handsets are similar to those caused by poor modulation quality.

One should note that the first cellular technology used in the United States, AMPS, did not have as tight a link between handset quality and system capacity as do current systems. Indeed, to a first approximation, in that early technology system capacity was independent of handset quality. Unlike modern CDMA systems that serve multiple subscribers from a single transmitter/receiver pair, those early systems used a separate transmitter and receiver for each conversation. Transmitting more power to one handset did not diminish the power available to other handsets.

Modern wireless handsets often support web browsers and other connections to the Internet. Many of the standard rules for communicating over the Internet were designed

under the assumption that communications capacity was relatively plentiful and inexpensive—consequently, standard Internet communications often contain substantial redundancy. Recognizing that this assumption is not always appropriate, the Internet standards community developed add-on capabilities that permit more efficient use of the communications links at the expense of additional processing in the handset and the network. Probably the most well-known of these is Van Jacobson header compression, but there are several others.[24] Requiring these features in a handset lowers the handset's use of network resources.

3.2. Handset Attributes that Affect Service Quality

Many of the capabilities or attributes of handsets affect not only the efficiency of the network but also the quality of the service delivered to subscribers. For example, a handset with poor sensitivity will lose calls at locations where a phone with better sensitivity could continue the conversation. Similarly, speech delivered by a handset with a poor voice coding subsystem (vocoder implementation) or a low-quality speaker will not sound as good as speech delivered by a higher quality handset.

[24] V. Jacobson, "RFC 1144 - Compressing TCP/IP headers for low-speed serial links," IETF 1990.

Table 3 lists some handset impairments that consumers would find difficult or impossible to separate from network shortcomings.

Table 3. Handset Impairments that Mimic Network Shortcomings

Handset Impairment	Observations
Reduced sensitivity Poor immunity to adjacent channel interference Insufficient ability to withstand inband overload Excessive intermodulation Poor handoff performance	These impairments reduce the handset's ability to receive signals from the base station.
Limited output power Poor modulation quality Reduced frequency accuracy Reduced timing accuracy	These impairments reduce the handset's ability to send signals to the base station.

The entries in Table 3 are based on those in Tables 1 and 2. Note that some of the handset impairments listed in Tables 1 and 2, such as out-of-band emissions, do not have a counterpart in Table 3. That is, some handset impairments that harm other consumers or consume system resources have no direct negative impact on the user of the impaired handset. Table 3 provides examples, not a comprehensive list, of possible impairments in handsets that can affect the quality of the service delivered to the user of that handset.

3.3. Difficulties Distinguishing Poor Handsets from Poor Networks

Consumers are unable to distinguish between many handset limitations (such as poor sensitivity or weak uplink power) and related network limitations (such as poor coverage). The symptoms of these particular network and handset impairments are

exactly the same—dropped calls, regions of poor or no service, and poor voice quality on a call. Because consumers cannot readily distinguish between network weakness and handset shortcomings, consumers with poor handsets may mistakenly blame service providers for the resulting poor service. Wireless carriers concerned with protecting their reputation have an incentive to control the handset used by their subscribers.

Wireless service is a new service—still in the process of rapid technical evolution. Furthermore, because the number of subscribers and their use of the service continue to grow at a rapid rate, wireless service providers are constantly building out and upgrading their networks. The wireless transmission facility—the radio paths to and from the base station—is created, in part, by the handset. Unlike the case in wired telephone service, the consumer cannot replace a handset with different handset in order to test the line. With wireless, the handset and the line are physically integrated—the handset is a fundamental part of the line.

Handsets affect service quality in another way as well. Customers often call their wireless carrier for assistance in configuring their handsets or in dealing with service features. A customer using a handset that the helpdesk staff is not familiar with or does not have information on in their databases would pose unusual and difficult challenges—especially if the customer were trying to use one of the less-common features. As I recount in Section 10 below, experience shows that carriers have encountered substantial difficulties providing support to unfamiliar handsets.

4. A Large Carrier's Handset Qualification Process

The impairments listed above are not just theoretical. Wireless carriers test handsets before approving them for use on their networks. For example, one large carrier disclosed to me their extensive (and expensive) process for testing new handsets. That process consists of four phases plus a preapproval workup by the manufacturer.[25] *Phase I* is parametric testing. The handset is tested in a lab to ensure that it conforms to the industry standard or to the carrier's own standards. For example, the carrier subjects the GPS portion of handsets to a standard that is somewhat more exacting than the industry

[25] Telephone call, 3 November 2004.

standard. I was informed that the carrier, for example, "move[s] the benchmark when we know it is achievable on a routine basis."[26] Handsets are also tested to ensure that they work properly with base station equipment from the carrier's primary suppliers.

Phase II is the testing of the advanced features—such as web browsers, short message service (SMS or text messaging), multimedia messaging service (sending photos from a handset), and measuring data throughput.

Phase III is field interoperability testing. Handsets are operated in the field in the coverage area of base station equipment from each vendor in areas of good coverage and bad. All features are exercised.

Phase IV is selected user testing. Around 30 to 40 handsets are sent to various employees. The employee uses the handset and notes problems and useful features. The handset acceptance team then reviews these staff member comments.

Summing up, this carrier puts substantial effort (and makes its vendors engage in comparable effort) to ensure that the handsets it provides to its subscribers perform properly. The tested attributes include various tests of all of the handset attributes listed in Tables 1 and 2.

5. Network Standards Evolution

As described above, wireless service providers have used multiple standards—AMPS, TDMA, CDMA, iDEN, and GSM—and have had to upgrade their systems as the standards have adopted new features. In several cases, carriers have had to transition their systems from one standard to another.

5.1. AMPS–TDMA–GSM–WCDMA–HSPA Evolution in the United States

Between 1993 and 1996, a U.S. wireless carrier that faced capacity constraints requiring a digital solution had only one choice—TDMA. Consequently, several wireless carriers, most notably SBC and AT&T, adopted the TDMA technology and spent billions of dollars on TDMA network equipment in order to expand capacity and service.

[26] Ibid.

As time passed, it became clear that TDMA would soon turn into a technological dead end. It possessed no clear advantages over the somewhat similar GSM standard or over the CDMA standard. On a global basis, GSM was far more widely used. The legal requirement in the European Union limiting cellular to GSM had, naturally enough, led to widespread use of GSM in Europe. That widespread use helped push the cost of equipment down. Other nations around the world also adopted GSM—in 1997, about 60% of all digital wireless users in the world were using GSM, and there were 70 million GSM users versus 6 million TDMA users.[27] Clearly, the combined effects of economies of scale in handset and infrastructure production along with the much stronger incentives for manufacturers to invest in research and development for GSM gear made it clear that GSM would continue to run away from TDMA.

Given both the similarities between TDMA and GSM and the fact that a multiband GSM handset could be used around the world, it was quite reasonable for wireless firms using TDMA to decide that they would convert their networks to GSM. Certainly, it would have been unreasonable to decide to stay with TDMA indefinitely. Consequently, the major TDMA carriers in the United States decided to transition their networks to GSM.

Obviously, changing a network from one technical standard to a different standard is a difficult and massive activity. At the beginning of the change from TDMA to GSM, service to current customers, with their TDMA-only handsets, has to be maintained, but new customers must be provided with handsets that can operate properly after the switchover is complete. TDMA network infrastructure must be phased out, and GSM network infrastructure phased in. Such changes are made more complicated by the limited radio spectrum available to wireless carriers. In most communities, a wireless carrier would have lacked the radio channels needed to build a complete new GSM system that could be run in parallel with the existing TDMA system. Rather, it would have been necessary to fit the new GSM system into the same spectrum used by the TDMA system. Then, over time the GSM system would have grown and the TDMA

[27] *GSMA Statistics Q2 2004*: GSM Association, 2004.

system would have shrunk. Finally, at some date, perhaps long after the transition had begun, the remaining elements of the TDMA system could be turned off.

The TDMA carriers faced a difficult transition. A key building block in such a transition was a dual-mode phone that could operate under both the TDMA and GSM standards. Such a phone could be sold to new subscribers in TDMA markets. It would immediately allow TDMA subscribers to roam into both GSM and TDMA markets. And, once a significant fraction of subscribers in a TDMA market had such handsets, that market could be partially converted to GSM operation and those subscribers with dual-mode handsets could be switched to the new GSM equipment. When the carrier had sufficient GSM capacity, new subscribers could be provided with GSM-only handsets. In a few more years, when the bulk of subscribers had GSM-capable handsets, the use of the TDMA network could be phased out altogether.

A wireless carrier facing such a transition must put in place a mechanism that ensures that new subscribers buy dual-mode TDMA/GSM handsets. Such handsets would necessarily be more complex and expensive that TDMA-only handsets of comparable capability.[28] During the transition, a carrier would be technically capable of activating a TDMA-only handset. But activating a TDMA-only handset would often create problems for the consumer and the carrier at a later time.

In the United States, the carrier-assisted transition from TDMA to GSM has generally been a success—and has now entered the endgame. In July 2006, Cingular announced that it would impose a fee of $5 per month on subscribers who use the older TDMA and analog handsets.[29] By the time that Cingular made this announcement, more than 90% of their users used GSM handsets.

---

[28] Note that the expense of such dual-mode phones would not only be driven by the additional complexity—it would also be driven by the limited demand because the only customers needing a dual-mode capability would be carriers transitioning from TDMA to GSM.

[29] See "Cingular Adds Surcharge For Old Phones: Monthly Bill to Increase by $5 for Customers without GSM Signal," CBS News, August 1, 2006. Downloaded from http://www.cbsnews.com/stories/2006/08/01/business/main1854442.shtml.

5.2. The General Case

The transition from TDMA to GSM is a case study of a more general problem that is continuously faced by all U.S. wireless carriers—that problem is the need to manage the transition from one generation of technology to the next generation. All cellular carriers had to shift from analog to digital (a process that is not yet quite complete). Today, wireless carriers face the problem of moving from second-generation systems (GSM, CDMA) to third-generation systems (UMTS/WCDMA, cdma2000). And, fourth-generation system designs (LTE, UMB) are on the horizon. Providing customers with a mix of dual-mode handsets is an important tool in such a transition.[30]

Consider a hypothetical network technology upgrade with the following characteristics:

- The new technology doubles the capacity (number of simultaneous calls) that can be served at each cell but does not otherwise affect service—consumers see no difference is call quality, coverage, or any other service feature if they use a new-technology handset.
- The new technology is backwards compatible with the existing network.
    - Old-technology handsets work with new technology cell sites but without the efficiency gain.
    - New-technology handsets work with old technology cell sites.
- The new technology can be installed one cell at a time.
- The new technology requires new handsets.

---

[30] It should be noted that some nations have not permitted wireless carriers to move from one generation of technology to the next within their licensed spectrum. Rather, carriers in a specific band are locked into a specific technology. See http://www.ofcom.org.uk/radiocomms/ifi/licensing/classes/broadband/cellular/celltelinfo.pdf for a statement of the U.K. policy limiting technology in the bands used for GSM. That U.K. policy derives from an E.U. policy directive which is now being questioned. For example, in February 2007 the Commission of the European Communities referred to the restrictions on the GSM bands saying "issues surrounding the introduction of 3rd generation mobile services and the continuing restrictions in the GSM Directive call for action." (CEC COM(2007) 50 at p. 11)

The more rigidly a nation controls the technology used in wireless, the weaker become the arguments for carrier control of handsets used with the carrier's network. At the same time, such rigid controls undercut the innovation process. It should be no surprise that the CDMA technology underlying all 3G system designs was developed under the flexible regulatory regime in the United States. Part of the funding for the original development of CDMA came from Pacific Telesys (PacBell mobile), a wireless carrier that was facing capacity limits in its Los Angeles system. See *Irwin Mark Jacobs Oral History*, Computerworld Honors Program, March 24, 1999 at p. 27. Available at http://www.cwhonors.org/archives/histories/Jacobs.pdf.

This technology will allow a carrier to expand its network without building additional cell sites or purchasing more spectrum. Rather, the carrier can install the new technology in cells that are congested at the busy hour and can migrate the customers who use those cells to new-technology handsets.

But, note that individual consumers have no incentive to buy new-technology handsets—the service delivered to new-technology and old-technology handsets is exactly the same. If it is the case that (1) the adoption of new-technology base stations and handsets is the efficient way to expand network capacity and (2) new-technology handsets are more expensive than old-technology handsets, the efficient network/handset choice will not be made unless the carrier provides an incentive to consumers to use the more efficient handset technology. The usual theory of congestion pricing teaches that service price is one such incentive—the carrier could offer discounts to users who used the new-technology handsets in locations served by new-technology base stations during peak times.[31]

A far simpler approach is for the carrier to subsidize the sale of new-technology handsets to those who are likely to make many calls in the areas served by the new-technology base stations. This allows the carrier to avoid any feeling of unfairness—new and old subscribers pay the same for their calls—but the carrier and its customers reap the benefits of the new technology.[32] Handset subsidies together with the refusal to activate handsets from other sources are effective tools carriers can use to ensure rapid consumer adoption of new-technology handsets.

5.3. Better Quality Voice Connections

The quality of a voice call consists of two major elements—how good the call sounds and how likely it is that the call will suffer an interruption or be dropped by the network. The first generation of CDMA did not improve speech quality significantly over the earlier

---

[31] For an overview of congestion pricing in a communications network see "Pricing congestible network resources," MacKie-Mason, J. K., and Varian, H. R., *IEEE Journal on Selected Areas in Communications,* Sept. 1995, Vol. 13, No. 7, pp. 1141–1149.

[32] Note that, when the new technology reduces network congestion or permits service at lower cost than would otherwise be the case, even the users of the old technology can benefit. That is, a subsidy for

analog AMPS system. CDMA eliminated problems with hearing a second conversation in the background but, in some circumstances, CDMA voice quality was slightly inferior to that of the AMPS system. However, CDMA introduced a new technology, called *soft handoff,* that improved coverage at the edge of cells and substantially reduced the chances that voice quality would be degraded or the call lost as calls were handed off from one base station to another. An improved version of CDMA (known as IS95B) introduced higher-quality voice processing. Some years after the initial deployment of GSM, GSM adopted new vocoders that provide both better speech quality and important coverage and capacity options.

Most such system innovations, for example, improved voice processing, can be put in place only when new handsets embodying the new technology are in use by consumers and when carriers make matching investments in the network. But, consumers have little or no incentive to buy handsets with these capabilities until the matching investment is in place. However, a carrier—concerned about competitiveness and brand value—may wish to subsidize handset capabilities today in order to gain future benefits.

Similarly, introducing a new network service creates a dilemma for the service provider. No one will spend extra money to buy terminals with the capability of using that service until they understand the service and it is available. No single subscriber has the incentive to go first on networked services such as text messaging. Tying, bundling, and handset subsidies are a tool for speeding the adoption of such innovations.[33]

5.4. Handset Evolution and Network Evolution

Although handsets and wireless networks are tightly linked elements of a single system, they have quite different cost characteristics. Handsets are electronic systems—made up of a display, enclosure, battery, keyboard, antenna, and electronics. Such systems can follow the cost/performance curves made possible by Moore's Law. Figure 3 shows the

---

Alice's phone which induces her to adopt more efficient technology can lower the cost of service to Bob or increase the quality of Bob's service.

[33] The classic reference on the adoption of technologies and services with such network effects is "A Theory of Interdependent Demand for a Communications Service," Jeffrey Rohlfs, *Bell Journal of Economics*, The RAND Corporation, vol. 5(1), pages 16-37, Spring.1974. Since then a substantial literature has grown up analyzing such problems.

drop in the cost of a low-end GSM handset from 1995 to 2007. In contrast, wireless networks include major cost elements, most importantly the towers and enclosures at cell sites and the cost of cell-site rental, which do not follow Moore's Law. Data collected by CTIA shows that the cost of wireless network infrastructure has stayed relatively steady over time. Figure 4 shows the capital investment per subscriber in the United States wireless industry for the period 1994 to 2004.[34]

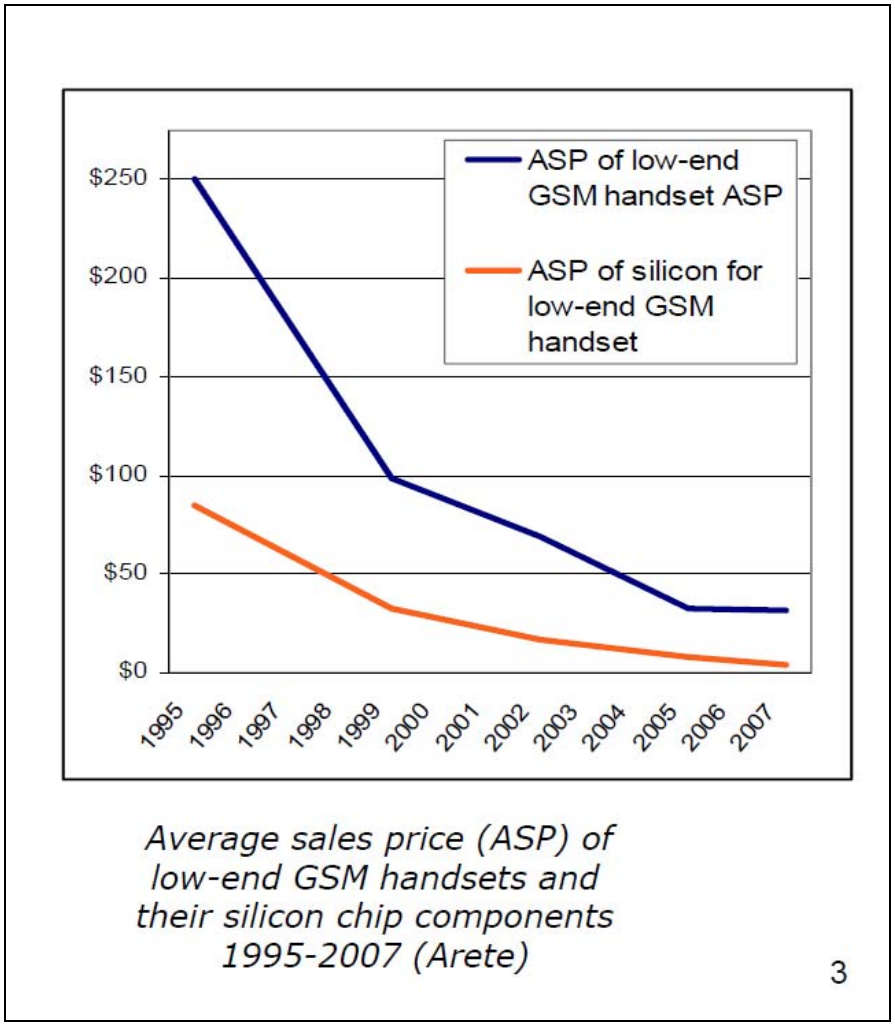

Figure 3. GSM Handset Price Evolution[35]

[34] The data for this chart were taken from Table 81 of *CTIA's Wireless Industry Indices*, Mid-Year 2006 Results, R. F. Roche and J-P Edgette, CTIA, November 2006.

[35] Source, "Benefits of Frequency Harmonization," presentation by Fred Christmas to the ITU Workshop on Market Mechanisms for Spectrum Management, January 2007, Geneva. Available at

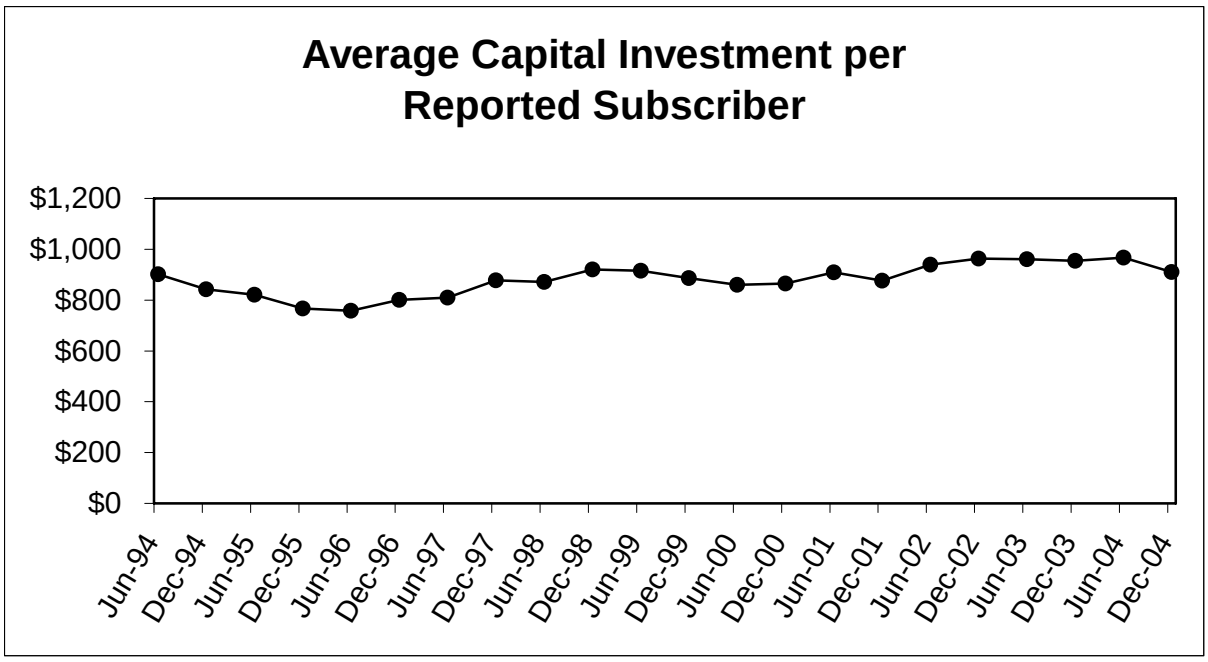

Figure 4. Average Wireless Capital Investment per Subscriber over Time

But, Moore's Law works in two ways in wireless handsets. Improvements in electronics push down the cost of building a handset meeting any given standard. But, such improvements in electronics also make possible the use of more complex signal processing in handsets—thereby permitting more efficient use of the radio channel. Increases in complexity lie at the heart of the spectrum efficiency gains that have occurred as each new standard has been adopted.

Even though the radio electronics in the handset account for only a small portion of the total cost of wireless service, those electronics control the productivity of the parts of the network that do not follow Moore's Law. Evolution of the handset is an essential element in the evolution of wireless service. Efficiency is served when some of the

---

http://www.itu.int/osg/spu/stn/spectrum/workshop_proceedings/Presentations_Abstracts_Speeches_Day_1_Final/ITU%20worshop%20jan%2007%20v2%201+%20FAC%20comments%203.pdf

Moore's Law progress in the handset is used for capacity and quality expansion of the entire network, not just for lower handset costs.

6. Supporting Complex New Service

6.1. The Complexity of Modern Handsets

As wireless handsets become more complex, they begin to rival personal computers in capability and complexity—some handsets have full keyboards, built-in cameras, and voice control options, and can run Microsoft Word and Outlook.

Providing customer support to such complex devices is substantially more difficult than providing comparable support to simpler handsets. Expecting a wireless carrier to be able to provide customer support to unknown wireless handsets is no more reasonable than expecting the help desk at Apple Computer to be able to support Dell and HP computers. Sprint informed me that they work to put in place handsets containing a standardized user interface.[36] Such a standardized interface would simplify consumer difficulties with new handsets, reduce help-desk costs, and might create a differentiated product attached to the Sprint brand name.

An incident related to me by a CDMA carrier illustrates the nature of the difficulties that can be created by such devices.[37] A customer had a Kyocera 3250 handset originally used on ALLTEL's wireless network. The customer brought that handset to one of another carrier's retail outlets, and the handset was activated for use on that carrier's network. The carrier soon discovered that this handset was generating an abnormally large volume of text messages. The information provided to me by the carrier did not explain how the carrier discovered the high traffic volume from this handset—perhaps the carrier noticed an abnormal traffic pattern or perhaps the user complained about an abnormal bill! Investigation showed that the handset had originally been set up to use ALLTEL's "touch-to-talk" service. As part of designing that service on its network, ALLTEL had programmed the handset to regularly send text messages to a computer that provided part of the service. Activating this handset on the other carrier's network created unexpected

[36] Personal communication, April 18, 2007.
[37] Telephone call, November 2004.

side effects that burdened both the subscriber and the new carrier—imposing costs all around.

Wireless web browsers provide a second illustration of the types of problems that are created when handsets optimized for one network are activated on a different network. The senior manager at Cingular told me details of two instances in which problems created by the activation of such outside handsets had come to his attention, the first of which involved the wireless web. There is a standard form of simplified web browsing capabilities optimized for wireless called the wireless application protocol (WAP). Cingular has encountered major problems with the WAP settings on handsets from other networks. In some cases, key IP addresses were embedded in the software and could not be changed under any circumstances. The problem was sufficiently complex and hard to deal with that it was brought to the senior manager responsible for handsets. The costs that such difficulties impose on both the subscriber and the carrier are obvious.

The other matter that manager recounted involved T-Mobile handsets that had been activated on the Cingular network. Because T-Mobile's network operates exclusively on radio channels in the PCS band, most T-Mobile handsets operate only in the PCS band (1900 MHz). In contrast, Cingular's network uses radio channels in both the PCS (1900 MHz) and cellular (850 MHz) bands. Former T-Mobile handsets operating on the Cingular network are restricted to the PCS band (1900 MHz) and incur roaming charges in circumstances in which a typical Cingular handset would not. This occurs because there are areas of the country where Cingular operates on only the cellular band (850 MHz). Thus, Cingular customers who activated T-Mobile handsets that work on PCS band (1900 MHz) are forced to roam when they are in areas where Cingular only offers cellular band (850 MHz) service. Such unexpected roaming charges lead either to customer dissatisfaction or to significant unwanted costs for the carrier—sometimes both. No matter what the final outcome, the mismatch of the T-Mobile handset with the Cingular network imposes costs on both the consumer and Cingular.

These examples show how simple differences in the way that two different networks use the same handset model as well as mismatches between a handset’s capabilities and a

network's capabilities create problems that impose significant costs on subscribers and service providers. Bundling and tying are tools to avoid such costs.

6.2. Meeting the FCC's 911 Rules

The FCC's 911 rules require wireless carriers (1) to provide the location of wireless callers to the public safety agency receiving the 911 call and (2) to permit speech and hearing-impaired persons to use text communications devices, such as the TTYs that are often used by the deaf, to make 911 calls.[38]

The rule requiring such text communication capabilities arose from experience. The analog AMPS system was able to carry the tones generated by TTYs. Unfortunately, the early digital voice coders did not do so. This shortcoming spurred development of the FCC's current rules requiring such capabilities. Carrying such signals required compatible changes in the standards applying to both the network and the handset equipment. Existing handsets could not be easily changed to accommodate TTY signals, but new handsets could be built to support this important capability.

The FCC's 911 rules also require wireless carriers to be able to provide the location of the caller to the E911 public service access point. The regulations impose accuracy requirements on that location information. The FCC permits two alternative approaches to E911 location determination—network based and handset based. The largest CDMA carriers (Verizon Wireless, Sprint) use a handset-based technology, whereas the largest GSM carriers (T-Mobile, Cingular) use a network-based technology. The systems used by Sprint and Verizon Wireless are hybrid systems that combine network information with GPS data from the handsets to derive a location estimate. Higher-quality GPS receivers in consumer handsets reduce the need for network measurement capabilities. Higher-quality network measurement capabilities would reduce the need for handset GPS receiver capabilities.

From a technical point of view, E911 is another example of the tradeoff between network infrastructure and handset investment. Handsets with built-in GPS receivers are more

[38] See 47 CFR 20.18.

expensive than handsets without GPS, but they provide useful location information—information that supplements whatever network measurements are made. I note that one large carrier requires handset manufacturers to provide handsets with GPS receiving capabilities that are better than those specified in the relevant industry standard.[39] Such higher performance handsets could compensate for other elements in the carrier's network design—and would be a factor in allowing the overall system comprised of the base-station radio equipment and the handsets to meet the E911 performance requirements that the FCC has imposed on wireless carriers.

The FCC rules prohibit a wireless carrier that has elected to use a handset-based solution from activating a handset that lacks a GPS receiver.[40] The FCC has made clear that wireless carriers, including resellers, are obligated to ensure that handsets offered to their customers support the relevant E911 location technology.[41]

In their 2004 SEC 10K, Verizon Wireless describes these FCC requirements saying,

> We must also meet separate Enhanced 911 rules that require us to sell new handsets that are capable of providing location information, and also to ensure that, by December 31, 2005, 95% of our "embedded base" of handsets have this capability. We may be required to subsidize the higher costs of Enhanced 911 capable handsets in order to achieve mandated penetration levels among our customers.[42]

Note that these 911 requirements for location capability and TTY compatibility are requirements imposed on the carrier and on the performance of the wireless carrier's service. But the carrier cannot meet these requirements unless the handsets used in its network have the necessary capabilities.

7. Fraud and Other Crimes

Weak security design and incomplete consideration of the various security threats to wireless systems have led to a variety of problems, including fraud, robbery, and widespread eavesdropping on wireless calls.

---

39 Conversation cited above.
40 *See* 47 CFR 20.18(g)(iv).
41 See 47 CFR 20.18(h).
42 Cellco Partnership, SEC Form 10K, March 10, 2004 at p. 15.

7.1. Fraud

Fraud was a major problem in the early days of wireless.[43] The designers of the original first-generation analog wireless system in the United States omitted antifraud controls. Consequently, there were several relatively simple techniques for theft of service. In addition to the loss of revenue to the carriers and the problems created for consumers when fraudulent charges appeared on their bills, such fraud created significant problems for law enforcement because these theft-of-service technologies allowed organized crime to make telephone calls that law enforcement found were impractical or impossible to intercept. A few quotations show the extent of the problem that the susceptibility of AMPS phones to theft of service created for law enforcement. An article in the *United States Attorneys' Bulletin* states,

> *Cloned Cellular Telephones*
> A problem reaching epidemic proportions in South Florida, as well as in many other areas, is that of individuals cloning cellular telephones. Many times those individuals are involved in other illegal activities and the "cloned" phone might be the one you want to intercept. The problem arises where you are intercepting calls over a cellular telephone and, after your interception has begun, the phone usage changes and you believe the target telephone has been cloned. All of a sudden, you are intercepting persons who are not your targets. This may be heralded by a dramatically increased volume of calls. If your targets themselves generate a large volume of calls, or if several targets use the same telephone, the situation can become confusing.[44]

In 1997, the FBI's John Navarrete testified to the House Judiciary Committee,

> First, the cloning problem could be dramatically reduced if cellular telephone manufacturers were required to produce cellular telephones that are not so easily reprogrammable. If one considers the matter, there is no need for cellular telephones to be reprogrammable outside of authorized company service centers. Law abiding cellular telephone users are not constantly reprogramming their cellular telephones nor do they want to; it is only the criminal community that is engaged in this activity.[45]

---

[43] D. G. Park, M. N. Oh, and M. Looi, "A fraud detection method using IS-41C protocols and its application to the third generation wireless systems," IEEE Globcom1998 Conference Proceedings, pp. 1984-1989. D. E. Denning and W. E. Baugh, "Hiding Crimes in Cyberspace," Information, Communication and Society, vol. 2.

[44] *United States Attorneys' Bulletin*, September 1997.

[45] Statement by John Navarrete, Deputy Assistant Director Federal Bureau of Investigation, Sept 11, 1997. House Judiciary Committee.

During the question and answer after his prepared testimony, Mr. Navarrete responded to a question from Crime Subcommittee Chairman McCollum by stating that the technology was available to prevent such behavior. Here are Mr. Navarrete's answer and the follow-up from Chairman McCollum:

> Mr. NAVARRETE. Well, I concur with my colleague and I would like to maybe put—because of the advances in technology, I would like to put the onus maybe on the manufacturers because they are the ones that I think ultimately control it and I think that the technology is there today that we can make these new phones where they could not be cloned.
> Mr. MCCOLLUM. Right. What you are saying is that you believe the phones themselves could be manufactured in a way that they could not be cloned. Does the FBI, Secret Service, of DEA have any scientific studies that would provide a basis for that assertion?
> Mr. NAVARRETE. Yes. We have those studies and, if you like, I can get the information to you.[46]

About the same time, two academics wrote,

> *Cellular Phones and Cloning*
> Drug lords, gangsters, and other criminals regularly use "cloned" cell phones to evade the police. Typically, they buy the phones in bulk and discard them after use. A top Cali cartel manager might use as many as 35 different cell phones a day (Ramo 1996). In one case involving the Colombia cartel, DEA officials discovered an unusual number of calls to Colombia on their phone bills. It turned out that cartel operatives had cloned the DEA's own number! Some cloned phones, called "lifetime phones," hold up to 99 stolen numbers. New numbers can be programmed into the phone from a keypad, allowing the user to switch to a different cloned number for each and every call. With cloning, whether cellular communications are encrypted may have little impact on law enforcement, as they do not even know which numbers to tap.[47]

Thomas A. Constantine, Administrator of the Drug Enforcement Administration, testifying before the Senate on International Organized Crime, stated,

> Colombian drug traffickers continually employ a wide variety of counter-surveillance techniques and other tactics, such as staging fake drug transactions, using telephones they suspect are monitored, limited-time use of cloned cellular telephones (frequently a week or less), limited-time use of pagers (from 2 to 4

---

[46] Ibid.

[47] "Hiding Crimes in Cyberspace," Dorothy E. Denning and William E. Baugh, Jr. July 1999 *Information, Communication and Society*, Vol. 2, No 3, Autumn 1999, also in *Cybercrime*, B. D. Loader and D. Thomas (eds.), Routledge, 1999.

weeks), and the use of calling cards. Colombian organized crime groups continue to show an active interest in acquiring secure communications capabilities.[48]

7.2. Antifraud and Anticloning Options

The lack of security in early wireless handsets created significant problems for both the carriers and law enforcement. However, wireless subscribers strongly prefer security solutions that are user friendly—nobody wants to enter in a password after dialing each call. In the mid- to late 1990s, manufacturers and service providers, working by themselves and working together in industry standards groups, developed a variety of antifraud and anticloning methods that are both effective and reasonably user friendly.

These methods were developed in the context of substantial fraud and law enforcement's concern regarding cloned wireless handsets. Uniform standards were required in order to support roaming services and to permit efficient mass production. Three problems were of significant concern to the industry: (1) preventing cloning, (2) providing simple yet secure service and call authorization, and (3) providing a mechanism to permit handsets to be used only with specific networks. In addition, there was concern about providing secure voice and data communications for users.

Developing good security for wireless has turned out to be a difficult task. Such systems are subject to substantial attacks. The attackers are not just teenage hackers with nothing else to do. The security of a widely used public system is often subject to scrutiny from academics and other security professionals.[49] In 2000, two computer science professors from the Weizmann Institute and one from the University of California published an article describing how to break a major wireless security system.[50] Similarly, in 2002, three IBM researchers, together with a scientist from the Swiss Federal Institute of Technology, published an article titled, "Partitioning Attacks: Or How to Rapidly Clone

---

[48] Statement by Thomas A. Constantine Administrator, Drug Enforcement Administration, Before the Senate Foreign Relations Committee, Subcommittee on the Western Hemisphere, Peace Corps, Narcotics, and Terrorism Regarding International Organized Crime Syndicates and their Impact on the United States, February 26, 1998.

[49] For example, consider the analysis of voting machines by security professionals. See "Analysis of an Electronic Voting System," T. Kohno et al., *IEEE Symposium on Security and Privacy 2004*, IEEE Computer Security Press, 2004.

[50] A. Biryukov, A. Shamir, and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," presented at Fast Software Encryption'00, New York, New York, 2000.

Some GSM Cards."[51] At the same time that academics were studying these systems from the point of view of security engineering, others were attempting to penetrate these systems in order to engage in various forms of illegal behavior.

7.3. SIM Cards

The GSM standard includes a feature called the *subscriber identity module card* (SIM card), which is a small printed circuit card that contains the information specific to the subscriber's account such as the subscriber's phone number and the identification codes needed to access the network. The SIM card can be removed from one handset and inserted into a different handset. A subscription to GSM wireless service is linked to the SIM card, not the handset. If Alice puts her SIM card in Bill's handset and makes a call, Alice is charged for the call. If Carl steals Diane's handset and puts his SIM card in it, Carl can make calls on his account with no further action.

I believe that the concept of the SIM card originated early in the development of the GSM standard at a time when portable handsets were not yet feasible for GSM. In a world without portable wireless phones, such a card would be a useful tool for travelers. For example, a SIM card would permit a traveler to use a wireless phone built into a taxicab or train or to use a wireless payphone as if it were the traveler's own phone. In today's world of portable handsets, the SIM concept offers less value than it would in a world in which wireless phones are built into automobiles.

The experience in Great Britain, where for several years essentially all handsets have been GSM handsets with SIM cards, gives further insight into the role of handset locking and related techniques in crime prevention and law enforcement. By the late 1990s or early 2000, handset robbery had become a significant problem in Great Britain. A 2003 study by the Home Office of robbery in Great Britain contained the text shown below.[52]

---

[51] J. R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely, "Partitioning attacks: or how to rapidly clone some GSM cards," Proceedings. 2002 IEEE Symposium on Security and Privacy, 2002, pp. 31- 41.

[52] J. Smith, "The nature of personal robbery," Home Office Research, Development and Statistics Directorate, London, UK January 2003.

Mobile phones and personal robbery

Mobile phones have become a staple of modern day living and it was perhaps inevitable that they would become an attractive target for theft and personal robbery. A separate report has already been published (Harrington and Mayhew, 2002), which examined the problem of mobile phone theft and robbery, using a combination of police force data and some of the local level BCU data gathered from this research.[26] As the authors point out, unravelling the contribution of mobile phones to robbery is a complicated task.

Figure 5. Quotation from a Home Office Research Study 2003

That study demonstrated that theft of mobile phones was a pervasive problem. Figure 6, also taken from that study, shows that on average 43% of personal robberies in Great Britain involved a mobile phone, with the fraction rising to over 60% in two areas.

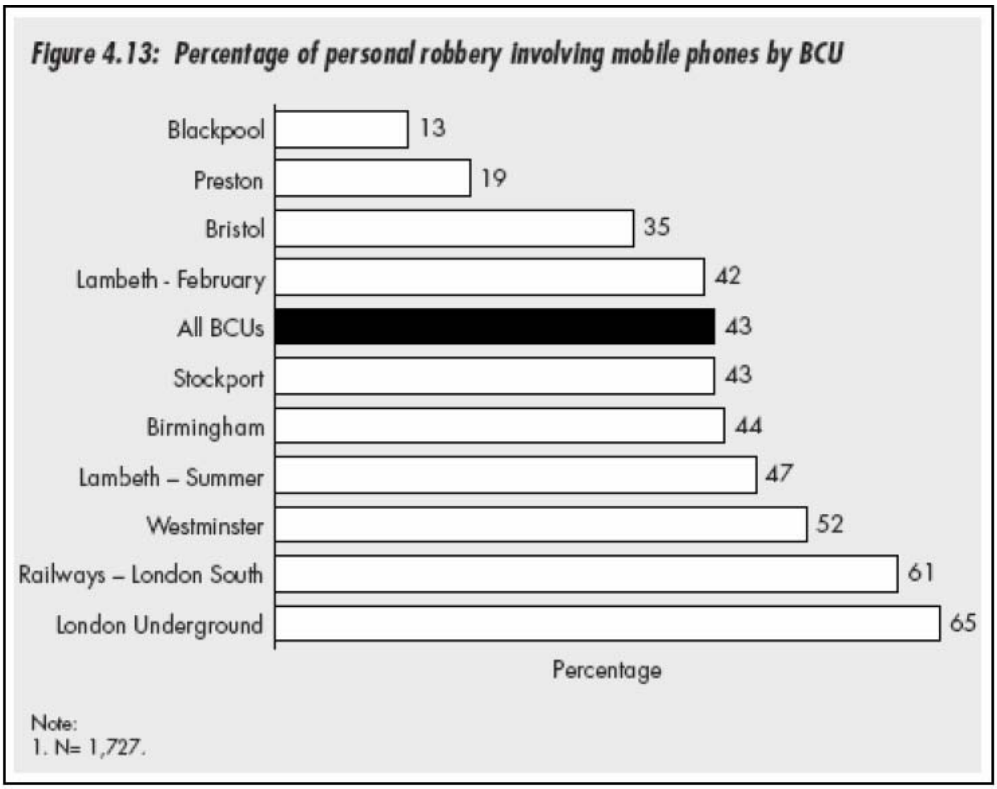

Figure 6. Percent of Robberies Involving Mobile Phones by Basic Command Units (BCU)

The robbers used deadly force in some of these robberies. A BBC story, headlined "Woman Shot for Mobile Phone," recounts one such incident.[53] A 2002 article in *Time*

[53] See http://news.bbc.co.uk/1/hi/england/1738659.stm

Europe overviewed the status of mobile phone theft and resale in several European countries. That story claimed that statistics show that "cell-phone theft is not only rising, it also is becoming more violent."[54]

In 2002, Great Britain enacted the Mobile Telephones (Reprogramming) Act (2002 Chapter 31) to close a loophole in the existing law that allowed the sale of equipment that permitted the easy activation of stolen wireless handsets in the UK.

Programming the phone so that it will work only on a single network or only with a specific SIM card (called a SIM lock) makes it difficult for a thief to pass off stolen property as legitimately acquired. More generally, it is clear that SIM locks are a tool that prevents or make more difficult the sale or reactivation of stolen handsets. An earlier U.K. Home Office study of the mobile phone theft problem noted, "one strategy for thieves is simply to insert a new SIM card. They can be easily and legitimately obtained for about £20, and the Feltham offenders spoke of 'dodgy' markets where they could be picked up for £5 or less."[55] SIM locks deny thieves this strategy.

In the debate in Parliament on the [anti-]Reprogramming Act, MP Michael Fabricant, in response to a question, explained the benefits of SIM locking saying,

> The hon. Gentleman is right to a certain extent. Yes, it would not be possible to take out the SIM card—although if the phone were stolen, the SIM card would be gone, too—and put it in another phone. Instead, owners would have to register with the company the fact that they now had a new phone. However, that is the only thing that they would have to do; they would still have portability. The trade-off would be having to make a telephone call, set against the advantage of its being less likely that one's phone would be nicked. Personally, I think that people would be happy to accept that.[56]

The research for the above part of this subsection was conducted a little more than two years ago. More recent data confirm that handset theft is still a problem in Great Britain. An October 2006 report by the British Ministry of Justice stated

---

54 http://www.time.com/time/europe/magazine/article/0,13005,901020311-214207,00.html

55 P. M. Victoria Harrington, "Mobile phone theft," Home Office Research, Development and Statistics Directorate, London 2001.

56 Hansard 22 Jul 2002: Column 722-3.

> In the UK it is clear that mobile phones are a significant factor in many offences of robbery and theft. Studies suggest that mobile phones are stolen in around half of all robberies and are the only item taken in around 20% of incidents. Young people, especially those of school age, are proportionately more likely to be victims of this type of crime. It is likely that mobile phone crime is increasingly becoming a problem in many other European countries too. The UK police have been contacted by numerous European countries including Poland, Germany, Portugal, France and the Netherlands regarding best practice in tackling mobile phone crime. The approach in the UK, in conjunction with the GSM Association, has been to remove the market for stolen phones, by ensuring that stolen mobiles are blocked and no longer work on UK networks. Many of the handsets that are stolen in the UK, however, are now being trafficked to certain other European countries where they are sold on the black market. It is clear that effective action needs to be taken across Europe to close down these illegal markets.[57]

In contrast, recent statistics from the U.S. Department of Justice indicate that the fraction of all thefts that are handset thefts must be much lower in the United States than in Great Britain—with no more than 8.3% of personal thefts resulting in the loss of "portable electronic, photographic gear."[58] The proportion of all thefts in the United States that are handset thefts can be no more than one-sixth that in Britain. In fact, it is probably significantly less because the statistics for the United States count camera thefts and iPod thefts in the same category as mobile handset thefts. Anyone comparing absolute crime rates in the United States and Great Britain faces difficulties arising from differences in the definitions and the study methods used in the two countries. That said, the national statistics indicate that the rate of personal theft is substantially higher in England and Wales (about 12 in every 1,000 persons being a victim in each year) than in the United States (about 4 in every 1,000).[59] If this three-to-one disparity in rates is correct, then the rate of handset thefts in two countries differs by almost a factor of 20.

---

[57] Report of the Ministry of Justice of Great Britain to the 27th Conference of European Ministers of Justice, MJU-27(2006) 10. Available at http://www.coe.int/t/dg1/legalcooperation/minjust/mju27/MJU-27(2006)10E-UK.pdf.

[58] Criminal Victimization in the United States, 2005 Statistical Tables National Crime Victimization Survey, December 2006, NCJ 215244, at Table 84.

[59] The personal theft rate for England and Wales was taken from *Crime in England and Wales*, Alison Walker et al., Home Office Statistical Bulletin, July 2006 at p. 94. See also Table 6.06. The personal theft rate for the United States was taken from *Criminal Victimization in the United States, 2005 Statistical Tables*, U.S. Department of Justice, NCJ 214244, December 2006. Table 1 of that report shows a robbery rate of 2.6 per thousand persons of age 12 and over. It also shows the rate of purse

A pan-European survey, conducted in 2002 for the European Union, showed that 18% of Europeans felt at risk of being mugged or robbed by someone seeking to steal their handset.[60] The report on that survey stated,

> Across the EU-15, 18% of respondents expected to be at risk over the next year of a mugging or robbery in order to steal a mobile phone. The Greeks, again, headed the poll at 37% followed by the French (30%), the Luxembourgers (28%) and the Portuguese (27%). A pattern is emerging at the other end of the scale with Austrian and German respondents recording scores of 6% and 8% respectively.[61]

Why is handset robbery a radically different problem in Great Britain, indeed in Europe generally, than in the United States? The difference in incentives—it is far easier to resell or reuse a stolen handset in Europe than in the United States—may well be a contributing factor.

7.4. The Effectiveness of Handset Security Tools

Multiple technical standards and multiple radio bands are used to provide wireless service around the world. Some handsets, most notably those conforming to the GSM 900 and GSM 1800 standards, can be used in more than 100 countries. A GSM 900 handset stolen in London can be shipped to Syria or Pakistan and activated there. In contrast, handsets operating on other standards have a far smaller global market. Consequently, the incentives for theft and trade in stolen handsets vary from technology to technology and country to country. Thus, it should not be surprising that some carriers choose to lock handsets to their network and others do not.

To sum up, many of the current tools for wireless handset security were developed in the 1995–2002 timeframe. The economic incentives for evading these security tools are enormous—there are roughly 2.5 billion wireless handsets in the world today worth in the neighborhood of $250 billion, and wireless service generates worldwide revenues of more than one-half trillion dollars annually. The carriers adopted their security policies

---

snatching/pocket picking to be 0.9 per thousand. Combining these numbers gives a total rate of personal theft of 3.4 per thousand.

[60] *Public Safety, Exposure to Drug-Related Problems and Crime,* Report prepared for the European Commission, the European Opinion Research Group, 2003.

and procedures in the context of massive fraud, the threat to human life from handset robberies, and the concern of law enforcement regarding handset cloning.

Today, those security technologies have substantially reduced the incidence of wireless fraud and cloned phones in the United States. Locking handsets to networks and preventing reprogramming is a tool that makes fraud and resale of stolen handsets more difficult. Although such locking is often viewed as merely a tool to protect handset subsidies, it has other important effects.

8. Fundamental Differences Between Wired and Wireless Handsets

Ordinary wired telephones might appear to offer a natural analogy to wireless handsets. However, that is wrong—wireless handsets present a great contrast to traditional telephone service and telephone instruments. Wired telephone service is a familiar, well-established service. Consumers know what quality to expect. Most consumers of wired telephone service take that service from an established carrier that is subject to public utility regulation. The transmission facility, the wires to the home, is separate from the instrument. Just as it is easy to tell the difference between a power failure and a burnt-out light bulb, it is relatively easy to distinguish between problems in the wired network and problems in the wired telephone instrument—one can just unplug the instrument and plug in a second instrument that is known to work well. If the second instrument works when plugged into the problematic network connection, then the problem is in the first instrument. If the second instrument also fails, then the problem is in the network.

One might conclude from the apparent analogy between wired handsets and wireless handsets that wireless handsets can and should be offered completely separately from wireless service, as is the case with wired telephones today. But the analogy, and thus any conclusion based on the analogy, is wrong. As described in some detail above, wireless handsets use shared resources to provide service, and thus one's use of an inferior wireless handset can degrade someone else's ability to get quality service.

---

[61] Ibid at p. 34.

On the landline side, in situations in which there is little or no possibility that use of a handset will interfere with someone else's use of the wired network, consumers can purchase telephone instruments that meet the FCC's Part 68 rules and connect those instruments to the wired telephone network via any standard jack. Home telephone instruments are connected to the larger telephone network by a pair of wires that runs from the home to the telephone company's central office.[62] For most telephone connections, that wire pair is a dedicated resource—used only by that one subscriber. If a subscriber's handset fails, say by shorting out the line or by creating terrible static on the line, only the subscriber's other extensions lose service. The harms created by a substandard instrument flow to the subscriber who purchases and controls that instrument but not to other subscribers.

But even on the landline side, in the case in which the potential for interference exists because of use of a shared resource, no unbundling was ordered by the FCC. Party lines, rare today but once common in residential service, use a single pair of wires to serve two or more subscribers.[63] Thus, only one subscriber on a party line can make a call at any moment, and eavesdropping on the calls of others sharing the same line is easy. In 1981, the FCC initiated an inquiry into the feasibility applying its registration program to telephone instruments connected to party lines.[64] That inquiry concluded that it was not practical to require telephone companies to allow consumers to supply their own telephone instruments for use with party lines.[65] The FCC summed up its analysis saying,

> With as many as eight parties sharing a party line, improperly installed or malfunctioning terminal equipment could affect many more people than just the

---

[62] This account is illustrative of the structure of modern wired telephone networks. Complicating elements, such as the use of remote terminals or load coils, that are inessential to the main point are omitted.

[63] The current FCC terminal equipment interconnection rules read "Except as provided in paragraphs (b) and (c) of this section, the rules and regulations apply to direct connection of all terminal equipment to the public switched telephone network for use in conjunction with all services *other than party line service*s. 47 CFR 68.2(a) emphasis added.

[64] FCC, "CC Docket No. 81-216. Commission invites comments on Notice of Proposed Rule Making amending Telephone Registration Program (Part 68) and institutes an inquiry into standard for business and residential wiring and party line service under Part 68.," 85 FCC 2d 868, 1981.

[65] FCC, "CC Docket No. 81-216. Second Notice of Proposed Rulemaking and Order," 92 FCC 2d 1, 1982.

> user of the equipment. Automatic answering machines, like telephones, would have to be designed to respond only to calls addressing the user of the machine. Otherwise, they would operate whenever any party on the line were called, infringing on that other party's privacy and possibly causing the caller unnecessary billing. Automatic dialers, which present a slightly different but equally significant problem, would require special circuitry to automatically relinquish the line on demand of another party. Such circuitry would be critical in emergency situations. Any damage by any such automatic device to a party other than the user could subject the user and/or manufacturer to considerable financial liability. These risks of third party harm, in addition to those associated with ANI failures and other network related faults, constitute a substantially increased array of potential harms than those generally associated with single party service. Our concern, then, is not only with the feasibility of developing, administering and implementing new rules, but with public safety as well.[66]

The fundamental difference between single-line and party-line phones is that, under most reasonable conditions, failures or impairments in a single-line telephone instrument will harm only the user of that telephone but failures or impairments in party-line instruments can readily harm the others who share that party line.

The mistaken analogy of wireless handsets to ordinary single-line telephones equipment is natural enough. However, such an analogy is deeply flawed, could easily mislead, and should be rejected.

9. Lessons for Competition Policy Analysis

The features and quality of a handset are inextricably intertwined with the quality of the wireless service. If John uses an inferior wireless phone—even if that inferior phone was state-of-the-art 5 years ago—he may deny service to Mary who is sitting next to him or may degrade service for other users within about mile around him. Widespread use of inferior handsets would either substantially degrade wireless service—such as by increasing the number of coverage holes and dropped calls—or would require a substantial increase in the capital plant used by wireless carriers. In either case, consumers would suffer.

---

[66] 92 FCC 2d 37, footnote omitted.

Economists have studied tying and bundling for decades and have identified circumstances in which such bundling serves efficiency and circumstances in which such bundling is anticompetitive and may harm consumers.[67] Most consumers find it convenient that right and left shoes are sold in pairs.[68] However, the usual analyses of tying are inappropriate for wireless handsets. Handsets are both a complement to the network and a *substitute* for network investment.

Arguments that handsets can be competitively supplied—independent of the preferences of the network service supplier—fail to take into account (1) the tradeoff between handset capabilities and network capacity, (2) the co-evolution of the network and the handsets, and (3) the security needs that are served by locking handsets to networks.

9.1. Alternative Approaches to Handset Qualification

Of course, tying is not the only possible mechanism that carriers could use to ensure that their customers use appropriate handsets. Possible alternative strategies include: (1) a list of acceptable handsets, (2) testing consumer-supplied handsets for conformity to the carrier's handset quality standards, (3) pricing network services to reflect a fine-grained measure of the relative network resource consumption of each handset, and (4) government regulation of handset technology to ensure that all handsets in the market were "acceptable." However, each of these alternative strategies poses substantial practical difficulties.

Consider first the difficulties of creating a list of acceptable handsets. Public disclosure of the criteria for making the list could disclose sensitive competitive information—particularly information regarding network engineering, new services, and planned network evolution. A carrier's decision to remove a product from the list could become

---

[67] See Tirole, Jean, "The Analysis of Tying Cases: A Primer" . Competition Policy International, Vol. 1, No. 1, pp. 1-25, Spring 2005 http://ssrn.com/abstract=702641, Carlton , Dennis W. and Waldman, Michael, "How Economics Can Improve Antitrust Doctrine towards Tie-In Sales: Comment on Tirole's 'An Analysis of Tying Cases: A Primer'" . Competition Policy International, Vol. 1, No. 1, pp. 27-40, Spring 2005 http://ssrn.com/abstract=702645

[68] However, the policy of bundling right and left shoes harms some consumers. I know of family with a child whose feet were, due to a birth defect, different sizes. Consequently, purchasing a useful pair of shoes often required purchase of two bundled same-size pairs—one pair to get the shoe for the child's left foot and one pair to get the shoe for the child's right foot.

contentious and the subject of allegations of abuse. Some criteria for making such a list, such as the ease of helpdesk support, are subjective and could also become contentious. And, of course, such a list could itself be regarded as a form of tying.

The second alternative, testing customer-supplied handsets for conformity to the carrier's quality standards, would be impractical. Such testing requires specialized equipment and trained test technicians, and takes hours not seconds. Such testing would impose substantial transactions costs. And, of course, the quality standards and the criteria for determining whether a product meets those standards could easily become contentious.

Pricing network services to reflect handset consumption of network capabilities would require adopting a different pricing model for wireless service—a pricing model that would be far more difficult for consumers to understand than the current pricing models that base prices on minutes of use, time of day, and gross variations in location.[69] Such pricing models would also introduce wide variations in service prices in a fashion beyond user control.[70] Even if such reformed prices were acceptable to consumers and could be shown to serve efficiency, there would still be the potential for contention over the pricing mechanism. One can easily imagine the suppliers of handsets that incurred higher network charges complaining that level or form of such charges were anticompetitive.

To sum up, each of the first three alternative strategies that I identified would impose substantial transactions costs and would be subject to complaints that the particular elements of the implementation of such strategies, such as inclusion on a list of acceptable handsets, were anticompetitive.

The fourth alternative, regulating handset technology, would solve one problem, but at the expense of imposing substantial constraints on the dynamic evolution of the industry. The FCC explicitly abandoned this approach when they adopted their policy of technical flexibility for wireless standards. That policy is regarded by many as an enormous success. In contrast and as noted above, the technical rigidity in the GSM bands in

[69] See Odlyzko, op. cit., for a discussion of consumer preferences for simple pricing structures.

[70] For example, CDMA users located close to a base station would pay less than users at greater distances.

Europe is now regarded as hampering innovation and evolution of the wireless market in Europe.

9.2. Concluding thoughts

The efficiencies of the joint supply of handsets and network services identified here do not appear to have been discussed in the competitive policy arena even though handset tying and bundling has been a contentious issue for about two decades.

The various joint economies between handsets and networks described above should be considered in any competitive policy analysis of the costs and benefits to consumers of handset bundling or tying.

About the Author

Dr. Charles L. Jackson is an electrical engineer who has worked extensively in telecommunications and wireless. He has been both a digital designer and a system programmer. He works as a consultant and is also an adjunct professor of electrical and computer engineering at George Washington University, where he has taught graduate courses on mobile communications, wireless networks and the Internet. Dr. Jackson is a well-know expert on spectrum management and spectrum policy issues. He has consulted for several governments on spectrum policy and radio licensing issues including New Zealand, Panama, Jamaica, United Kingdom, Germany, Latvia, and the United States. He has also consulted for major corporations and industry associations on those issues. He has written extensively on spectrum management and spectrum policy. He was the first to invent combinatorial auctions—formulating them in the context of radio license auctions.

Dr. Jackson is also familiar with spectrum policy issues from inside government—having worked on spectrum issues at both the FCC and for the U.S. Congress.

Dr. Jackson served three terms on the FCC's Technological Advisory Council. He holds two U.S. patents, and has one other patent pending. Dr. Jackson received his PhD from MIT.