

Before the  
**FEDERAL COMMUNICATIONS COMMISSION**  
Washington, D.C. 20554

In the Matter of  
  
Preserving the Open Internet  
  
Broadband Industry Practices

GN Docket No. 09-191

WC Docket No. 07-52

**COMMENTS OF THE  
NATIONAL ASSOCIATION OF TELECOMMUNICATIONS  
OFFICERS AND ADVISORS (“NATOA”) AND THE BENTON FOUNDATION**

by: Ken Fellman  
President

Tonya Rideout  
Acting Executive Director

NATOA  
2121 Eisenhower Avenue  
Suite 401  
Alexandria, VA 22314  
(703) 519-8035  
(703) 997-7080 (fax)

January 14, 2010

**TABLE OF CONTENTS**

I. INTRODUCTION ..... 2

II. PREVIOUS ADVOCACY FOR AN OPEN INTERNET..... 3

III. COMMENTERS SUPPORT CODIFICATION OF A NON-DISCRIMINATION PRINCIPLE AND A TRANSPARENCY PRINCIPLE AND URGES THE COMMISSION TO TAKE ADDITIONAL STEPS TO GUARANTEE AN OPEN INTERNET..... 5

    A. Commenters Support the Commission’s Efforts to Codify a Non-Discrimination Principle, while Recognizing that in Certain Situations Mediation of Packet Transmissions by Network Owners can be Both Desirable and Necessary. .... 6

    B. Commenters Support the Inclusion of a Transparency Element to the Rules. .... 7

    C. The Commission Should Review the Extent to Which Open Access Requirements Could Serve to Deter Discriminatory Practices Intended to Favor Services Offered by Vertically Integrated Operators..... 8

    D. The Commission Should Encourage the Development of High Capacity Networks Such as Fiber to the Premises. .... 8

    E. Managed or Specialized Services that Require Prioritized Transport are Possible So Long as Consumers Have the Choice of Service That Does Not Include Prioritization..... 10

    F. The Commission’s Rules Should Apply to Wireless Providers as Well, As the Future of the Open Internet Cannot Be Protected Absent Extension of these Protections to the Growing Wireless Market..... 11

IV. CONCLUSION..... 12

Before the  
**FEDERAL COMMUNICATIONS COMMISSION**  
Washington, D.C. 20554

In the Matter of  
Preserving the Open Internet  
Broadband Industry Practices

GN Docket No. 09-191

WC Docket No. 07-52

**COMMENTS OF THE  
NATIONAL ASSOCIATION OF TELECOMMUNICATIONS  
OFFICERS AND ADVISORS (“NATOA”) AND THE BENTON FOUNDATION**

The National Association of Telecommunications Officers and Advisors (“NATOA”) and the Benton Foundation (collectively “Commenters”) hereby file these comments in response to the Federal Communication Commission’s (“Commission”) Notice of Proposed Rulemaking in the above-referenced proceeding (FCC 09-93).

NATOA is the national association that represents the communications needs and interests of local governments, and those who advise local governments. NATOA’s membership includes local government officials and staff members from across the nation whose responsibility is to advise and implement telecommunications policy for the nation’s local governments. These responsibilities range from cable franchising, rights-of-way management and government access programming to information technologies and Institutional Network (I-Net) planning and management.

The mission of the Benton Foundation (“Benton”) is to articulate a public interest vision for the digital age and to demonstrate the value of communications for solving social problems.

Benton is a longtime supporter of research on universal service and the potential of high-speed Internet connections for improving Americans' lives.

Commentors welcome this opportunity to comment on an issue of vital importance for ensuring the full propagation of the next generation of the Internet. We applaud the Commission's decision to defend and promote the open nature of the Internet by codifying its existing four Broadband principles.<sup>1</sup> We further support codifying additional principles relating to non-discrimination and full transparency regarding the network management practices of network owners and operators.

## **I. INTRODUCTION**

Commenters believe that network neutrality guarantees are necessary because major private providers have demonstrated their ability and willingness to interfere with communications across endpoints on the network for reasons that are unrelated to legitimate network management needs.<sup>2</sup> In fact, the Commission currently finds itself in litigation with Comcast, the nation's largest cable operator, over Comcast's decision to thwart legal peer to peer transmissions over the Comcast network. In this particularly egregious example Comcast sent packets with RST flags to users to deceive them into thinking that the user, with whom they were

---

<sup>1</sup> The four existing principles are:

1. To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to access the lawful Internet content of their choice.
2. To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.
3. To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to connect their choice of legal devices that do no harm to the network.
4. To encourage broadband deployment and preserve and promote the open and interconnected nature of the Internet, consumers are entitled to competition among network providers, application and service providers, and content providers.

<sup>2</sup> See, e.g. Nate Anderson, "Pearl Jam censored by AT&T, calls for a neutral 'Net,'" *Ars Technica* (Aug. 9, 2007), <http://arstechnica.com/old/content/2007/08/pearl-jam-censored-by-att-calls-for-a-neutral-net.ars>; Susan Crawford, "The big picture: Why the Verizon/NARAL flap matters," *Susan Crawford Blog*, (Sept. 28, 2007), <http://scrawford.blogware.com/blog/archives/2007/9/28/3258382.html>.

communicating, had terminated a session. The fact that Comcast argues that it did nothing illegal and the Commission thus cannot impose any sanctions speaks volumes about why we need strong, enforceable protections.

Without such protections and enforceable penalties, these practices are likely to continue and possibly accelerate as the power of the Internet levels the playing field and allows anyone to innovate and create new services and applications that rival or exceed the offerings from network operators. We are similarly troubled by the many other manipulations and abuses that are possible of which consumers and the Commission may never learn, unlike in the Comcast/Bit-Torrent matter, where at least Comcast's practices have received a public airing. We urge the Commission to continue with its plans to codify principles of network neutrality to forestall the possibility of more widespread abuses in the future.

## **II. PREVIOUS ADVOCACY FOR AN OPEN INTERNET**

Commenters have consistently advocated for the preservation of the openness principles that have made the Internet such an unparalleled success and a key driver of American prosperity and innovation, including at the local level where NATOA's member communities work to enhance community interests. In 2007 NATOA adopted a policy position<sup>3</sup> on network neutrality stating that NATOA supports:

...the effective and efficient use of all communications technologies including voice, video, data and information services over wired and wireless transmission technologies.

Local governments support implementation of Federal, State and Local laws and rules that encourage open and interconnected services and technologies that are universally available to all citizens.

NATOA's policy statement further states that:

In recent years communications providers have suggested that they expect to favor some content and services over others, for commercial, political

---

<sup>3</sup> Attached hereto as Attachment 1.

or other purposes. NATOA's Board does not believe that a communications service provider should be allowed to favor one content provider, service or product over another. All persons purchasing specific communications services or products from a communications provider should receive access without any form of discrimination by the communications provider. This principle of non discriminatory treatment is called "Network Neutrality".

In 2008 NATOA adopted a set of Broadband Principles<sup>4</sup> that we believe should serve to shape the contours of a national broadband strategy for our nation and can articulate a vision of broadband that takes the public interest into account. In those principles, NATOA reaffirmed its commitment to a free and open Internet for all. Specifically, NATOA's Broadband Policy Principle # 6 states:

Network neutrality is vital to the future of the Internet.

It is vital to the future of the Internet that network owners not discriminate in terms of content transport or unnecessarily interfere in communications between end points on the network. Where packet prioritization is necessary network owners must provide similar treatment to all providers of like services. NATOA believes that everyone must have the unabridged freedom to create, post or access any lawful content and services and to attach any devices to the network as long as they do not impair network performance. Many current network traffic management strategies are a function of scarce bandwidth capacity and should not be necessary with high-capacity networks.<sup>5</sup>

In 2009 NATOA again stated its commitment to a free and open Internet in its comments to the Commission regarding the National Broadband Plan.<sup>6</sup> In those comments we affirmed that:

Many new services riding on networks will compete with services offered by the vertically integrated providers. Strong protections against anti-competitive behavior will be required, given that network owners have every economic incentive to favor their own content and services at the expense of their competitors who lease access on their networks.<sup>7</sup>

---

<sup>4</sup> Attached hereto as Attachment 2.

<sup>5</sup> See Attachment 2.

<sup>6</sup> In the Matter of A National Broadband Plan for Our Future, *Comments of NATOA et al*, GN Docket No. 09-51 (filed June 8, 2009) ("Comments of NATOA et al").

<sup>7</sup> *Id.* at 32.

NATOA also stated that:

Industry protests to the contrary, non-discrimination and openness are not new concepts. Rather, they represent established and successful policies without which today's Internet would not have been possible.

In the early days of ARPANET, researchers were able to use the underlying connectivity available through the phone network to transport data packets among connected computers. They had access to the phone networks because the networks were regulated as common carriers. . . subject to open access requirements. The resulting environment was one, in essence, of network "neutrality." The Internet's success arose because anyone could communicate with other network endpoints, unfettered by any unnecessary mediation from the network owner and "without change in the form or content of the information as sent and received." It would not be an exaggeration to say that this made the Internet one of history's great innovations.<sup>8</sup>

Most recently, in October of 2009, NATOA sent a letter to Chairman Julius Genachowski stating its support of this proposed rulemaking.<sup>9</sup>

### **III. COMMENTERS SUPPORT CODIFICATION OF A NON-DISCRIMINATION PRINCIPLE AND A TRANSPARENCY PRINCIPLE AND URGES THE COMMISSION TO TAKE ADDITIONAL STEPS TO GUARANTEE AN OPEN INTERNET.**

NATOA offers additional comments in this proceeding to underscore its belief that without strong and enforceable network neutrality rules the Internet, which has been an engine for tremendous innovation and economic growth, will be subject to artificial constraints caused by arbitrary interference on the part of network owners for purposes unrelated to legitimate network practices. Indeed, without these reasonable protections, the few owners of America's broadband infrastructure will be in a position to pick winners and losers among application and content providers, without the knowledge of American consumers that their choices are being so constrained and manipulated.

---

<sup>8</sup> *Id.* at 34.

<sup>9</sup> Letter from NATOA President Ken Fellman and Acting Executive Director Tonya Rideout to Chairman Julius Genachowski (Oct. 22, 2009) attached hereto as Attachment 3.

**A. Commenters Support the Commission’s Efforts to Codify a Non-Discrimination Principle, while Recognizing that in Certain Situations Mediation of Packet Transmissions by Network Owners can be Both Desirable and Necessary.**

NATOA recognizes that at times there are valid network management practices that may cause some types of transmissions over a network to be moderated. For instance as local governments we know from experience that there must be a way to ensure prioritization of public safety communications during emergencies or catastrophic events. However, we agree with the Commission that these and other examples must be the exceptions to the rule and that any network practices that result in interference of transmissions must be made known and be subject to verification by the Commission that they were legitimate interventions designed to optimize network performance or to advance the public interest. None of these practices should result in an unfair advantage to services offered by a network operator over similar services offered by others with no ownership stake in a network.

NATOA believes the mere threat that an operator can impede the transmission of a new service will have a chilling effect on Internet innovation. Entrepreneurs and startup companies will be reluctant to contribute time and money towards research and development of new applications and services if they have no assurances that their innovations will be provided with the bandwidth or transport terms necessary to ensure that they work as intended. We note that most “killer” applications on the Internet such as e-mail, and the web browser YouTube, were not invented by network owners but by users who had access to the underlying connectivity available to them. Somewhere today someone could be working in a garage on the next Google, Facebook or other service that we cannot envision today—applications that could not only have enormous commercial potential but that could also serve to enhance, support, or transform key aspects of American life such as health-care, environment protection, or economic

competitiveness. Large, established companies like Google and Amazon may be able to afford the pricing terms in a two-tiered Internet, but smaller, more nimble companies that drive Internet innovation and growth may not.

**B. Commenters Support the Inclusion of a Transparency Element to the Rules.**

NATOA supports the Commission's inclusion of a transparency requirement. Given the potential damaging effects on the Internet that could result from unwarranted discrimination in packet transmissions, it is essential that any practices that interfere in transmissions between any endpoints on a network be subject to scrutiny and to independent verification that such a practice was necessary. The Commission, users and other network participants should be able to understand and verify the necessity of practices that tend to degrade the performance of communications over the network. To achieve the desired aims NATOA believes that it is important that an operator's explanation of its network management practices should be in plain English and to the extent possible understandable to the average person. We have witnessed many examples where required explanations are written in arcane language. Consider the required notices from cable operators, banks and credit card companies that purport to explain a consumer's rights to privacy or the terms of services. More often than not the average person is left puzzled by language that even trained lawyers have difficulty interpreting. In our view transparent must mean clear, concise and understandable to the average person.

Additionally the Commission should work with independent engineering firms, standards development bodies, or other non-self-interested institutions to determine what information is required to assess whether any of an operator's network management practices that impeded Internet transmissions were conducted for legitimate purposes as described above. Leaving it solely to network operators to decide what material is relevant for determining the legitimacy of

their network management practices would be absolute neglect of a critical Commission responsibility.

**C. The Commission Should Review the Extent to Which Open Access Requirements Could Serve to Deter Discriminatory Practices Intended to Favor Services Offered by Vertically Integrated Operators.**

Commenters urge the Commission to study the extent to which open access requirements could help facilitate the desired results of fairness, openness and transparency while minimizing the need for complex rules that could be subject to varying interpretations and potentially lead to unintended consequences. The recently published study by the Berkman Center for Internet and Society at Harvard University<sup>10</sup> states that:

Open access policies in other countries have sought to increase levels of competition by lowering entry barriers; they aim to use regulation of telecommunications inputs to improve the efficiency of competition in the consumer market in broadband.<sup>11</sup>

Commenters believe that an environment where multiple service providers compete over a common platform could allow market forces to provide the discipline necessary to curb any attempts by network operators to discriminate in favor of their proprietary services. In a truly competitive environment users will likely choose the services that consistently offer the best performance for the money.

**D. The Commission Should Encourage the Development of High Capacity Networks Such as Fiber to the Premises.**

Commenters note that increasing network speeds would obviate the need for many network management practices. Providers sometimes claim that they must curb the bandwidth provided to some Internet transmissions in order to be fair and equitably allocate scarce bandwidth to all users. In some cases that is true, but it begs the question of what then can be

---

<sup>10</sup> Next Generation Connectivity: A review of broadband Internet transitions and policy from around the world – October 2009 (“Berkman Study”).

<sup>11</sup> Berkman Study at 11.

done to increase the capacity of the network so that more people can engage in more complex applications requiring significantly more bandwidth than is provided today by most broadband networks in the country. The attached graph<sup>12</sup> clearly illustrates the problem. While there is plenty of capacity in long haul fiber lines and in core switching, consumer demand for bandwidth will very soon exceed the capabilities of last mile providers. In some cases this lack of capacity has even led network operators to vilify some of their own customers rather than address the inability of their networks to meet the needs of more advanced users. The term “bandwidth hogs” is a derogatory way of referring to paying users who are only using the bandwidth that was advertised to them. It is important to remember that the congestion is sometimes caused by network operators oversubscribing their networks by selling to more customers than the network can actually support under the assumption that most users will not use the advertised bandwidth. When more consumers use the bandwidth that they purchased, it is unfair and a distraction to call those consumers “hogs” rather than addressing the need for world-class communications networks.

Commenters urge the Commission to recommend strategies in the National Broadband Plan to increase the capacity of today’s networks and put our nation on a path to eliminating the copper last mile connections that continue to be bottlenecks preventing the widespread use and adoption of data intensive applications that have the ability to transform our economy, create jobs and address the increasing entertainment, information and communications needs of our citizens, institutions and governments. The capacity of Fiber to the Home networks will eliminate the need or excuse to throttle many applications.

---

<sup>12</sup> Nemertes Research, “Internet Interrupted, Why Architectural Limitations Will Fracture the ‘Net,” Attached hereto as Attachment 4.

**E. Managed or Specialized Services that Require Prioritized Transport are Possible So Long as Consumers Have the Choice of Service That Does Not Include Prioritization.**

Commenters believe that the Internet should remain fundamentally application neutral as it has been through its tremendous growth to date, an environment in which network traffic is not manipulated on the basis of the particular software or application or service provider originating or receiving the communications, and no traffic receives different priority than any other *unless the prioritization is voluntarily chosen by the consumer* (for example through consumer purchase of a premium or guaranteed tier of service).

Commenters understand that network operators want to be able to guarantee quality of service for some proprietary premium applications. Part of the challenge is how to allocate admittedly scarce bandwidth for such services while ensuring that it does not come at the expense of American consumers and innovators. NATOA believes that the Commission should look at this issue closely with the goal of ensuring that consumers have the chance to choose to purchase such premium, managed services rather than be universally subjected to them.

We know that communications technology is capable of prioritizing users, rather than applications, based on transparent consumer pricing. This application-neutral prioritization enables users who have paid for a higher tier of service to have higher priority and thus potentially encounter less congestion at peak times—without any user necessarily facing limits focused on the use of individual applications. Such an approach would enable carriers to “manage” networks that do not provide sufficient bandwidth, but without compromising consumer choice, transparency, innovation, and the free and open Internet that has become so fundamental to American life, commerce, and civic discourse.

**F. The Commission’s Rules Should Apply to Wireless Providers as Well, As the Future of the Open Internet Cannot Be Protected Absent Extension of these Protections to the Growing Wireless Market.**

The future of the wireless Internet is an essential part of the future of the Internet. While NATOA believes that fiber to the premises is essential to American national interests, we recognize the importance of ubiquitous mobile broadband as a complement to wireline networks, and we recognize the tremendous growth of wireless service in recent years.

If the Commission’s Open Internet rules are not extended to this growing segment of Internet use, the rules will be weakened and undercut by the presence of discrimination and anti-competitive practices on wireless networks. The benefits of the open Internet will be lost to millions of American consumers and to the entrepreneurs and innovators who seek to serve them over wireless platforms.

An open wireless Internet is eminently feasible. Commenters refer the Commission to the technical report submitted by the New America Foundation in this proceeding that describes a conservative, established set of technical processes and principles for achieving “Any Device” and “Any Application” in a wireless environment.<sup>13</sup> We note that robust environments of just this sort exist on both GSM and CDMA wireless platforms in parts of Asia and Europe, demonstrating their technical feasibility. We urge the Commission to reject any argument that “wireless is different.” To the contrary, wireless exists alongside wireline as an essential part of America’s Internet future and the protections the Commission extends to one must also apply to the other.

---

<sup>13</sup> “Any Device and Any Application on Wireless Networks: A Technical Strategy for Evolution.” Andrew Afflerbach, Ph.D., P.E. and Matthew DeHaven. Prepared for the New America Foundation. January 2010. Attached hereto as Attachment 5.

#### **IV. CONCLUSION**

Commenters recognize that certain network management practices may be important to optimize network performance and that some consumers may wish to purchase prioritized services—and some may not. However, the Commission must remain vigilant to ensure that these practices are legitimate and do not have the effect of favoring services offered by network owners at the expense of like services from others with no ownership stake in their networks. As most services today are determined by software and hardware at the edge of the network, the data packets necessary to realize those applications should to the maximum extent possible travel between and among end points with no unnecessary interference from the network owners. No network operator should be able to block or degrade access to websites or sources of information that they may deem contrary to their interests. The Commission’s existing protections of the open Internet should be expanded to include non-discrimination and transparency, and all these protections should be extended to the wireless environment.

Respectfully submitted,

The National Association of Telecommunications Officers and Advisors

Benton Foundation

by: Ken Fellman  
President

Tonya Rideout  
Acting Executive Director

NATOA  
2121 Eisenhower Avenue  
Suite 401  
Alexandria, VA 22314  
(703) 519-8035  
(703) 997-7080 (fax)

## **Attachment 1**

### **NATOA Policy Statement on Network Neutrality**



Board of Directors Policy Statement  
On "Network Neutrality"  
Adopted March 7, 2007

The National Association of Telecommunications Officers and Advisors (NATOA), an organization dedicated to promoting community interests in communications, has reinforced its long standing policy statement regarding the non-discriminatory access by all users to all forms of communications services. NATOA's Board supports the efforts of lawmakers to enact specific legislation that would prevent communications providers from discriminating or prioritizing the transmissions of any communications services or products based on the content or source of such services and products. NATOA's current policy states:

**NATOA Supports:**

- **... the effective and efficient use of all communications technologies including voice, video, data, and information services over wired and wireless transmission technologies.**

**Local governments support implementation of Federal, State and Local laws and rules that encourage open and interconnected services and technologies that are universally available to all citizens.**

In recent years communications providers have suggested that they expect to favor some content and services over others, for commercial, political, or other purposes. NATOA's Board does not believe that a communications provider should be allowed to favor one content provider, service or product over another. All persons purchasing specific communications services or products from a communications provider should receive access without any form of discrimination by the communications provider. This principle of non-discriminatory treatment is called "Net Neutrality."

Communications providers are already compensated for the use of their networks through subscriptions by consumers to their products and services. Communications providers should not be allowed to favor one consumer over another simply by virtue of the consumer's choice of product, service, or website.

**Attachment 2**

**NATOA Broadband Principles**



## **Introduction to NATOA's Broadband Principles**

For centuries, the United States has been a world leader in economic development and social initiatives. From the 19th century railroad systems and the early 20th century electric and telephone networks' expansion, to the post-World War II highway system and airport construction, investments in physical infrastructure have been instrumental in supporting social and economic progress.

Today, the United States is at a critical juncture. Economic and social development increasingly depend on advanced communications infrastructure. However, there is no strategy in place for widespread deployment of next-generation broadband networks. Our failure to take immediate action threatens to relegate our country to second-class status in the broadband age.

The future of broadband is about more than viewing television, surfing the Web and making phone calls. It is about new forms of communication and mass collaboration through the virtually unlimited potential for sharing information, storage capacity, processing power and software made possible through high-capacity bandwidth connections. This collaboration will generate new ideas, accelerate economic development and lead to opportunities for wealth creation, social development and personal expression.

While other industrialized nations have developed strategies for next-generation broadband infrastructure, the United States still lacks a national broadband strategy. The lack of a proactive strategy has effectively ceded control of our broadband destiny solely to the private market without sufficient regard for the public interest or the unique needs of local communities. This approach has not resulted in the investment needed and has failed to realize the many positive externalities created by next-generation broadband networks. The effects of this failure are clearly manifest: fading international rankings for broadband penetration; relatively low bandwidth at high costs; throttling of peer-to-peer communications; and little competition among service providers. Moreover, the future contours of broadband in the U.S. are being defined by a small number of private entities.

NATOA is increasingly concerned that the communities we represent are losing their competitive advantage to communities in Europe and Asia due to the lack of federal and state broadband leadership. This inaction will likely harm the competitive status of local communities with respect to education, healthcare, economic development, standard of living, and the level and quality of civic discourse. Inaction will adversely affect local governments' ability to provide public safety or to create a more sustainable environment for the future.

Local governments have always played an essential role in ensuring that the benefits of communications infrastructure would be available in communities across the United States. Localities will, by necessity and by choice, be part of the solution to our national broadband deficit. To that end, NATOA has adopted its Broadband Principles.



## BROADBAND PRINCIPLES

The National Association of Telecommunications Officers and Advisors (NATOA) supports the development of a National Broadband Strategy consistent with the following principles.

### **1. NATOA calls for the immediate nationwide deployment of advanced broadband networks.**

The United States faces a broadband crisis. Broadband network infrastructure is critical to economic growth. New and emerging applications and services demand more bandwidth than can be delivered by most current domestic networks. The gap between the United States and other industrialized nations is growing wider. Our country is becoming a digital also-ran with serious adverse consequences to our economic competitiveness and quality of life.

The United States has a proud history of deploying electric, telephone and transportation infrastructure to all parts of the country. Now we are challenged again. We are behind and the buildout of advanced broadband networks will take time. We must act now!

### **2. True broadband requires high capacity bandwidth in both directions.**

To grow and enhance economic opportunity, local communities must have access to interactive, open, broadband networks with sufficient capacity to meet the increasing information, communications and entertainment needs of their residents, businesses, institutions and local governments. US competitors in Europe and Asia are building broadband networks that can provide bandwidth of 100 Mbps to 1 Gbps to each premise. Those networks serve as platforms for continuing innovation and allow the delivery of new services and applications that will transform these nations' economies and enhance the quality of life. To remain globally competitive, networks in this country should meet or exceed those standards and be designed so that capacity can be expanded by replacing electronics without having to rebuild the networks.

It is important for America's networks to offer symmetrical, high capacity bandwidth in both directions, as with many of the new networks in Europe and Asia. Ample upstream bandwidth empowers network users to become creators and distributors of content and applications, as well as recipients of services. NATOA believes that the success of Web sites featuring user-provided content, as well as the successes of traditional educational, government and public access television, demonstrate that people can and will become content creators if they are afforded the tools to do so.

### **3. Fiber to the premises is the preferred broadband option.**

Broadband networks use several wire-based and wireless technologies, including: copper and other metal wires; coaxial cable, multimode fiber optics; single-mode fiber optics;

microwaves; Wi-Fi; and WiMax. The transmission bandwidth and reliability characteristics and capabilities of each technology vary based upon many factors, including: the specific technology; the transmission distance and the connecting and terminal equipment being used. Currently, single-mode fiber optic networks are capable of transmitting the most bandwidth with the highest reliability. They show the best potential to handle increasing future demands for higher speeds and greater quantities of information.

NATOA recognizes that it will not be economically feasible to bring fiber optics to all communities in the near term. Where fiber connection is not practical, other technologies, such as high capacity coaxial cable or wireless, may be viable if they achieve the bandwidth levels described above. In the long run however, the goal should be to make fiber to the premises universally available.

Wireless networks are an important part of the broadband picture. Wireless allows mobility, and offers a competitive choice for Internet access with quick and relatively low cost deployment. Wireless will not be a substitute for an all fiber network but will play a complementary role.

#### **4. High capacity broadband connectivity must be affordable and widely accessible.**

An informed citizenry requires knowledge and opportunities for expression. NATOA believes that everyone should be able to access the information and services that high capacity broadband networks will provide. Without reasonable prices and equitable access many of our citizens will not be active participants in the broadband age. Our residents and our society will benefit from wide availability, since the communicative power of the network increases exponentially as more network endpoints are created. High capacity broadband networks can bring to bear the collective ingenuity and enterprise of our citizens to find solutions to the many problems confronting us. NATOA believes that everyone should have access to high capacity networks at reasonable prices.

#### **5. High capacity broadband requires open access networks.**

Fiber optic networks continue to demonstrate economies of scale. This characteristic gives the owner of the fiber platform an unbeatable advantage over other service providers. It is expensive – perhaps prohibitively so - to build multiple fiber networks in one community. Thus the owner of the first and therefore dominant network can set unfair terms and prices for others to use it. On the other hand, multiple service providers who can compete over a common platform will fuel innovation in broadband services, which will benefit local communities and society. Thus structural or regulatory measures must be employed to protect the right to non-discriminatory access to networks for all competing service providers and to forestall unfair business practices by network owners. NATOA recognizes that private developers of new fiber networks must be able to seek a realistic return on investment. This is consistent, however, with providing access on non-discriminatory terms.

## **6. Network neutrality is vital to the future of the Internet.**

It is vital to the future of the Internet that network owners not discriminate in terms of content transport or unnecessarily interfere in communications between end points on the network. Where packet prioritization is necessary network owners must provide similar treatment to all providers of like services. NATOA believes that everyone must have the unbridged freedom to create, post or access any lawful content and services and to attach any devices to the network as long as they do not impair network performance. Many current network traffic management strategies are a function of scarce bandwidth capacity and should not be necessary with high-capacity networks.

## **7. All networks and users have the right and obligation to non –discriminatory interconnection.**

Broadband communications at the local access level can be fast and economical. However, data packets that leave the local access network and traverse the public Internet will flow only as fast as the slowest connections between end points. To facilitate reliable, high-bandwidth, symmetrical, peer-to-peer communications between our communities and to promote the expansion of open access networks, NATOA supports the direct linkage of local broadband fiber network peering points through the use of long haul fiber. All local broadband networks must have the right and obligation to non-discriminatory interconnection with other broadband networks using common, interoperable standards and protocols.

## **8. Local governments must be involved to ensure that local needs and interests are met.**

The desired development of high capacity broadband networks and broadband services will require extensive collaboration among all parties: local communities, regions, state governments, national government, the private sector, interest groups and others. While the U.S. has plenty of broadband capacity in the “long haul” routes, fiber connections rarely reach homes and small businesses. Local governments are central players in ensuring that this “last mile” fiber connection to homes and businesses is achieved. Local elected officials are well positioned to evaluate the infrastructure and economic development tools needed to sustain viability, encourage growth and ensure that the unique needs and specific interests of local communities are addressed. NATOA believes local governments must be recognized as key partners to industry and the states and federal government in broadband development.

## **9. Local governments must be allowed to build and operate broadband networks.**

Local geographic communities share common interests and offer the best opportunity for acceptance and growth of high capacity broadband. The right of local governments to build and operate broadband networks must not be infringed. Public agencies and community-based non-government agencies also need to have equal opportunity to participate through

meaningful investments in communications infrastructure. Communities must have the freedom to meet their unique communications needs. NATOA believes that local governments and the communities they serve must be able to preserve the policy option to own and operate public broadband networks. Any existing prohibitions on local government communications initiatives must be abolished.

**10. A variety of options must be considered to cover deployment costs.**

It is not yet clear which methods of funding deployment are best. Different methods may be preferable in different communities. For example, networks may be financed by private investment, by government investment, by public-private partnerships, by tax incentives, or by other means. None of these approaches should be prohibited by law or burdened by special restrictions (such as laws that forbid cross-subsidy by governments but allow it for private entities).

**Attachment 3**

**NATOA Letter to Chairman Genachowski**



October 22, 2009

Chair Julius Genachowski  
Federal Communications Commission (FCC)  
445 12th Street SW  
Washington, DC 20554

Dear Chair Genachowski:

On behalf of the National Association of Telecommunications Officers and Advisors (NATOA), we write to express our support for the Commission's continued efforts to safeguard the free and prosperous market built on the open Internet.

The open Internet has empowered citizens and local communities by increasing civic participation, facilitating learning, and strengthening neighborhood businesses. Via the Internet, city and state governments can stream council meetings, publish text of resolutions and other official documents, and communicate with their constituents online directly. Students can communicate with their teachers and with one another, and can access immense databases of information, from home, school, and even their neighborhood coffee shop. Through the Internet, small businesses and entrepreneurs can advertise and sell online, and compete with much larger businesses on a level playing field by creating a better product – not by paying for preferential treatment online. The open Internet brings to communities both a stronger economy and a stronger democracy.

For years the FCC has intervened when necessary to preserve the economic and social benefits of the open Internet. As threats to these benefits increase, the time has come to move from incremental actions to clear rules, and we encourage you to continue towards that end. The Commission's existing four principles, plus the proposed principles of nondiscrimination and transparency, should be enacted into rules to establish a clear framework for the open Internet. Such a framework, if developed correctly, will safeguard the benefits of the Internet for local communities, and will foster new opportunities for economic growth and civic engagement.

Attached please find NATOA's formal policy statement on Network Neutrality, adopted in March 2007. We look forward to working with you in developing the proper framework for the open Internet, to preserve its democratic, social, and economic benefits for this and the next generation of citizens.

Sincerely,

A handwritten signature in black ink, appearing to read "Ken Fellman".

Ken Fellman  
NATOA President

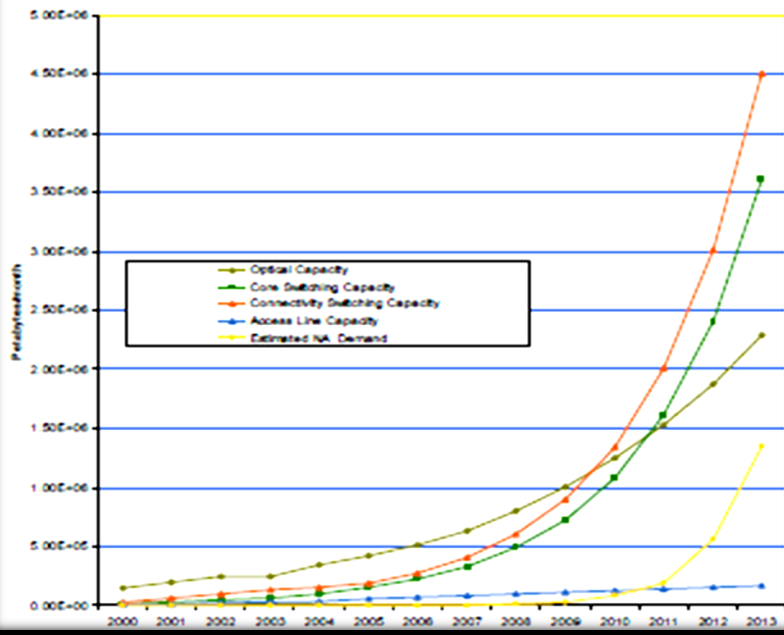
A handwritten signature in black ink, appearing to read "Tonya S. Rideout".

Tonya S. Rideout  
NATOA Acting Executive Director

## **Attachment 4**

**Internet Interrupted, Why Architectural Limitations Will Fracture the 'Net**

North America Capacity vs. Demand - 2008



## **Attachment 5**

# **Any Device and Any Application on Wireless Networks: A Technical Strategy for Evolution**

# **Any Device and Any Application on Wireless Networks: A Technical Strategy for Evolution**

Prepared by  
**Andrew Afflerbach, Ph.D., P.E.  
and Matthew DeHaven**

Prepared for  
**The New America Foundation**



**NEW AMERICA  
FOUNDATION**

**January 13, 2010**



Columbia Telecommunications Corporation • [www.CTCnet.us](http://www.CTCnet.us)  
10613 Concord Street • Kensington, MD 20895 • 301.933.1488

# Table of Contents

<b>1. Executive Summary .....</b>	<b>1</b>
1.1 <i>Scope of This Report .....</i>	<i>1</i>
1.2 <i>The Evolution of Technology Can Enable Openness, If So Directed .....</i>	<i>3</i>
<b>2. Toward A Wireless “Any Device” Environment.....</b>	<b>5</b>
2.1 <i>Existing Carriers Already Prove the Feasibility of Any Device .....</i>	<i>7</i>
2.1.1 <i>A Robust Any Device Environment Exists on the GSM Platform Internationally .....</i>	<i>7</i>
2.1.2 <i>Under FCC Requirements, Verizon Already Implemented Open Development Parameters, a First Step Toward Any Device .....</i>	<i>8</i>
2.1.3 <i>Carriers Already Enable Roaming, a Form of Any Device .....</i>	<i>9</i>
2.1.4 <i>Carriers Already Use Multiband and Multi-Protocol Devices.....</i>	<i>9</i>
2.2 <i>There Exist Multiple Layers of “Any Device” Interoperability—and All Are Not Equal .....</i>	<i>10</i>
2.2.1 <i>Tethering a Device Through a Standard Interface .....</i>	<i>11</i>
2.2.2 <i>Connecting Any Device to Any Single Carrier Network.....</i>	<i>12</i>
2.2.3 <i>Connecting Any Device to Any Network Using a Common Technology Platform .....</i>	<i>12</i>
2.2.4 <i>Connecting Any Device to Any Wireless Network Regardless of Technology Platform.....</i>	<i>15</i>
2.3 <i>The Established Standards-Writing and Certification Processes Provide a Reliable Path Toward Any Device and Resolution of Its Complications .....</i>	<i>16</i>
2.3.1 <i>The Existing Certification Process.....</i>	<i>16</i>
2.3.1.1 <i>Devices Are Independently Certified to Meet Protocol Standards.....</i>	<i>17</i>
2.3.1.2 <i>Devices Are Certified by the FCC to Ensure Licensing Compliance.....</i>	<i>18</i>
2.3.1.3 <i>Devices Are Certified by Individual Carriers to Meet Carrier-Specific Requirements .....</i>	<i>19</i>
2.3.2 <i>The Proposed Certification Process for Any Device .....</i>	<i>19</i>
2.3.3 <i>Evolution to Any Device in a GSM Environment .....</i>	<i>22</i>
2.3.3.1 <i>Enable Network Use Through SIM Cards.....</i>	<i>22</i>
2.3.3.2 <i>Enable Device Unlocking.....</i>	<i>23</i>
2.3.3.3 <i>Develop Non-Discriminatory Technical Requirements. ....</i>	<i>24</i>
2.3.3.4 <i>Allow Non-Discriminatory Carrier Configurations and Updates.....</i>	<i>24</i>
2.3.4 <i>Evolution to Any Device in a CDMA Environment.....</i>	<i>24</i>
2.3.4.1 <i>Bringing the CDMA Any Device Environment to the U.S. ....</i>	<i>25</i>
2.3.4.2 <i>Develop Technical Requirements.....</i>	<i>25</i>
2.3.4.3 <i>Develop Signup Procedures and Incorporate Detachable, Removable User Identity Cards .....</i>	<i>26</i>
2.3.4.4 <i>Allow Non-Discriminatory Carrier Configurations and Updates.....</i>	<i>26</i>
2.3.5 <i>Evolving Roles of Carrier, Device Manufacturer, and User .....</i>	<i>26</i>
2.3.6 <i>Registration and Payment in an Any Device Environment.....</i>	<i>29</i>
2.3.7 <i>Future Technology Evolution in an Any Device Environment.....</i>	<i>30</i>
2.3.7.1 <i>Software-Based Radio .....</i>	<i>30</i>
2.3.7.2 <i>Long Term Evolution (LTE) .....</i>	<i>31</i>
<b>3. Toward a Wireless “Any Application” Environment.....</b>	<b>33</b>
3.1 <i>Network Capacity Is Frequently Insufficient to Support Carriers’ Oversubscription.....</i>	<i>35</i>
3.2 <i>Carriers Face Few Technical Limitations in Traffic Management.....</i>	<i>36</i>
3.3 <i>3G and 4G Wireless Technologies Enable Extensive Management.....</i>	<i>39</i>
3.4 <i>The Technical Consequences of Application-Based Traffic Management Extend Beyond the Individual User’s Experience.....</i>	<i>40</i>
3.5 <i>Defining the Application-Neutral Management Environment.....</i>	<i>41</i>
3.5.1 <i>Wireless Technologies Enable Carriers to Prioritize Users, Rather Than Applications, Based on Transparent Payment Criteria .....</i>	<i>41</i>

3.5.2	The Same Technologies that Enable Discriminatory Prioritization Can Be Used for Transparent Prioritization Based on Non-Discriminatory Criteria.....	42
3.5.3	Wireless Technologies Enable Carriers to Limit Bandwidth Use at Any One Time by Allegedly-Abusive Users .....	43
3.6	<i>Transparency and Verification as Guarantors of Application Neutrality</i> .....	45
3.6.1	Publish Traffic Management Techniques in Lay Language .....	45
3.6.2	Verify Through Periodic Audit of Carrier Equipment Configuration by Sufficiently Expert Parties..	46
3.6.3	Verify Through Technical Investigation of Complaints by Sufficiently Expert Parties .....	46
3.7	<i>The Case for Any Management Diminishes as Spectrum Is Opened and Technologies Evolve</i> .....	48
3.7.1	Expansion into Available Unused Spectrum and White Spaces .....	48
3.7.2	More Advanced and Efficient Wireless Standards .....	49
3.7.3	Segmentation/Sectorization of Service Areas.....	50

## Table of Figures

Figure 1:	The Wired Internet and the PC.....	4
Figure 2:	The Wireless Internet and Devices.....	5
Figure 3:	Tethering a Device to a Mobile Network .....	12
Figure 4:	Use of SIM Card to Obtain Connectivity to Mobile Network.....	13
Figure 5:	Any Device Connectivity to Any Network Using Either GSM or CDMA .....	14
Figure 6:	Any Device Connectivity to Any Wireless Network Regardless of Technology.....	15
Figure 7:	Current U.S. Wireless Device Certification .....	17
Figure 8:	Summary Comparison of Existing and Proposed Certification Processes .....	21
Figure 9:	Functionality of Wireless Device and Detachable SIM .....	23
Figure 10:	Existing Carrier Roles .....	27
Figure 11:	Table of Evolution of Carrier Role in Any Device Environment.....	28
Figure 12:	Capacity Demands of Typical Browsing vs. Streaming Media.....	36
Figure 13:	Priority Queuing.....	37
Figure 14:	Example of Customer Information Table for Transparent Traffic Management .....	45
Figure 15:	Third-Party Traffic Management Validation.....	47
Figure 16:	Table of Frequency Bands for Different Technologies .....	48

## 1. EXECUTIVE SUMMARY

This Report presents the results of an engineering evaluation of some of the issues raised by the Federal Communications Commission's "Open Internet" Notice of Proposed Rulemaking.<sup>1</sup> The Report suggests a strategy entailing a conservative process for evolving from the limitations of current locked and closed wireless device and application environments to a more open future as envisioned by the "any device" and "any application" portions of the Commission's draft Open Internet rules. This Report proposes:

- An Any Device environment made possible through third-party or FCC certification.
- An Any Application environment subject, where necessary, to application-neutral traffic management that is fully transparent and disclosed to customers.

### 1.1 Scope of This Report

The Report was prepared in the winter of 2009-2010 by Andrew Afflerbach, Ph.D., P.E., and Matthew DeHaven of Columbia Telecommunications Corporation (CTC) at the request of the New America Foundation.<sup>2</sup> Specifically, this Report:

1. Describes how technology can evolve and how non-interoperable environments can thereby become interoperable, assuming that industry chooses to evolve—or is mandated to enable such evolution.
2. Describes how the existing certification processes work for wireless devices.
3. Proposes a conservative evolution of certification processes and mandated technological changes to enable Any Device certification independent of carrier approval or veto. Based on the expected schedule of technological advances, this evolution should begin with existing 3G wireless technologies.
4. Notes the clear feasibility of Any Device rules, given that more open practices exist elsewhere in the world, and that even in the U.S. there is some emerging openness with respect to wireless devices, primarily as a result of government requirements and pressure from outside the wireless carrier industry.
5. Describes four different scenarios that are sometimes called Any Device regimes, notes that all are not equal, and notes that "tethering," in particular, is not a true Any Device strategy.

---

<sup>1</sup> FCC Notice of Proposed Rulemaking, 09-93, *In the Matter of Preserving the Open Internet*, GN Docket No. 09-191, and *Broadband Industry Practices*, WC Docket No. 07-52; released October 22, 2009.

<sup>2</sup> With thanks to Shivani Gandhi and Arun Karthikeyan for research and writing assistance.

6. Defines an “Any Device” environment as one in which devices are sold by a range of retailers and resellers, including carrier-affiliated resellers, but the devices are not locked to one network or blocked from other networks. Devices are certified independently of carriers, by a government or third-party entity, and are activated using a standardized methodology, such as by insertion of a detachable card (SIM, R-UIM), or other entirely transferable mechanism that relies on software-based authentication.
7. Defines an “Any Application” environment as fundamentally application neutral: network traffic is not manipulated on the basis of the particular software or application service provider originating or receiving the communications, and no traffic receives different priority than any other unless the prioritization is voluntarily chosen by the consumer (e.g., through the purchase of a premium or guaranteed tier of service). In addition, applications requiring continuous data flows are not necessarily considered harmful to a network, even if they do use extensive capacity, provided they are not unlawful or malicious, such as spam or viruses.
8. Describes how elusive an Any Application environment can be, given that wireless carriers are technically capable of any type of network management, both in the radio frequency (RF) network and in the network core. Absent authority to investigate, it is technically difficult or impossible to determine exactly what type of network traffic management practices are in use, or how traffic is being classified by the network operator for purposes of management—by information source, by user, by application, or by content in application.
9. Proposes scenarios for how a carrier can manage its network in an application-neutral way, according to the above definition, in the event that there may be valid and necessary requirements for proactive management of network traffic. For example, technology enables prioritization of users, rather than applications, based on transparent consumer pricing. This application-neutral prioritization enables users who have paid for a higher tier of service to have higher priority and thus potentially encounter less congestion at peak times—without any user necessarily facing limits focused on the use of individual applications.
10. Notes the importance of transparency of any traffic management practices, and that full disclosure to government and consumers is essential, thereby allowing informed decision-making by customers and, as a result, carrier investment decisions that take into account consumer knowledge of management practices.
11. Discusses technology evolutions (such as opening of previously unused spectrum, new 4G technologies, adaptive antennas, white spaces, and cognitive radios) that will enable more capacity on wireless networks and address concerns about congestion that appear to motivate carrier opposition to Any Application environments.

## 1.2 The Evolution of Technology Can Enable Openness, If So Directed

Recent years have seen rapid advances in the capabilities of Internet technologies and wireless technologies. The Internet has evolved as an open environment, geared toward flexibility and ubiquity. The creators of the Internet did not design the Internet for a particular application, and so it has evolved in unpredictable directions, driven by individuals, corporations, and governments alike. It has grown in capabilities, speed, and availability.

Wireless technologies likewise provide capabilities unheard of 20 years ago. Personal wireless phones are widely available in most countries of the world and are affordable to the majority in the U.S.

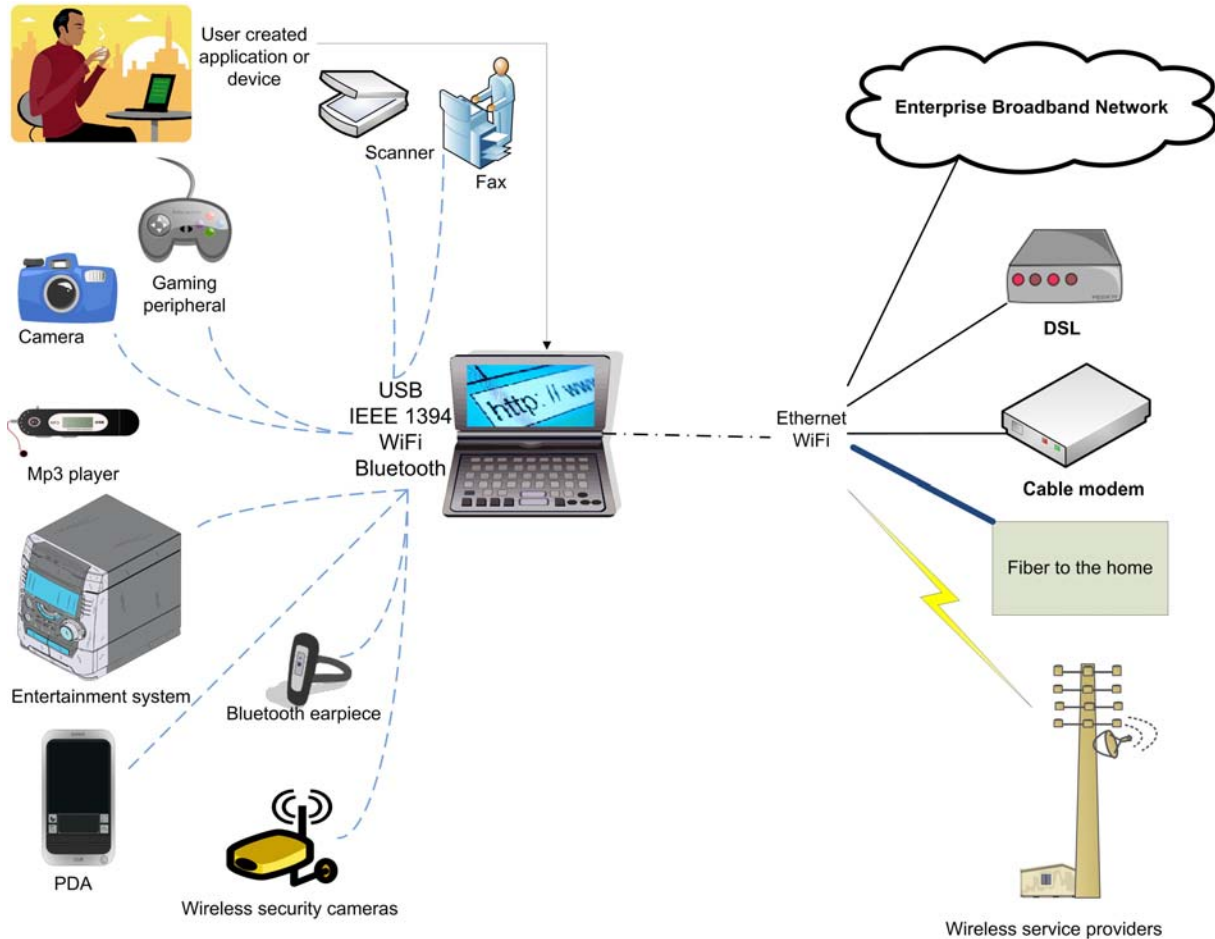
Because it is more mature, the wired Internet has been closer to the Internet ideal. While there are some notable exceptions,<sup>3</sup> users of the wired Internet have enormous flexibility in operating applications on their devices and over their Internet connections. To a large extent, this flexibility results from the evolution of the personal computer, and has been further empowered by the proliferation of low-cost home networking equipment and compatible user devices. Once a marketplace of costly, limited, non-compatible hardware, PCs have made great advances in affordability and flexibility.

Each computer can connect to a huge variety of external devices, operate a wide range of software (with many competing brands for each type of application), and connect to any available service provider available at the customer premises (Figure 1). Through the Internet service provider (ISP), the computer can connect to any available content on the Internet. If the user wishes to change service provider, the user can connect the computer or home network to another service provider through a standard Ethernet, USB, or WiFi interface and will not need to purchase a new computer. If a user wishes to communicate with or share an application with another user on an entirely different type of computer or operating system, the communication and sharing can happen seamlessly.

---

<sup>3</sup> In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications and Broadband Industry Practices Petition of Free Press et al. for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management," 23 FCC Rcd 13028 (2008).

Figure 1: The Wired Internet and the PC



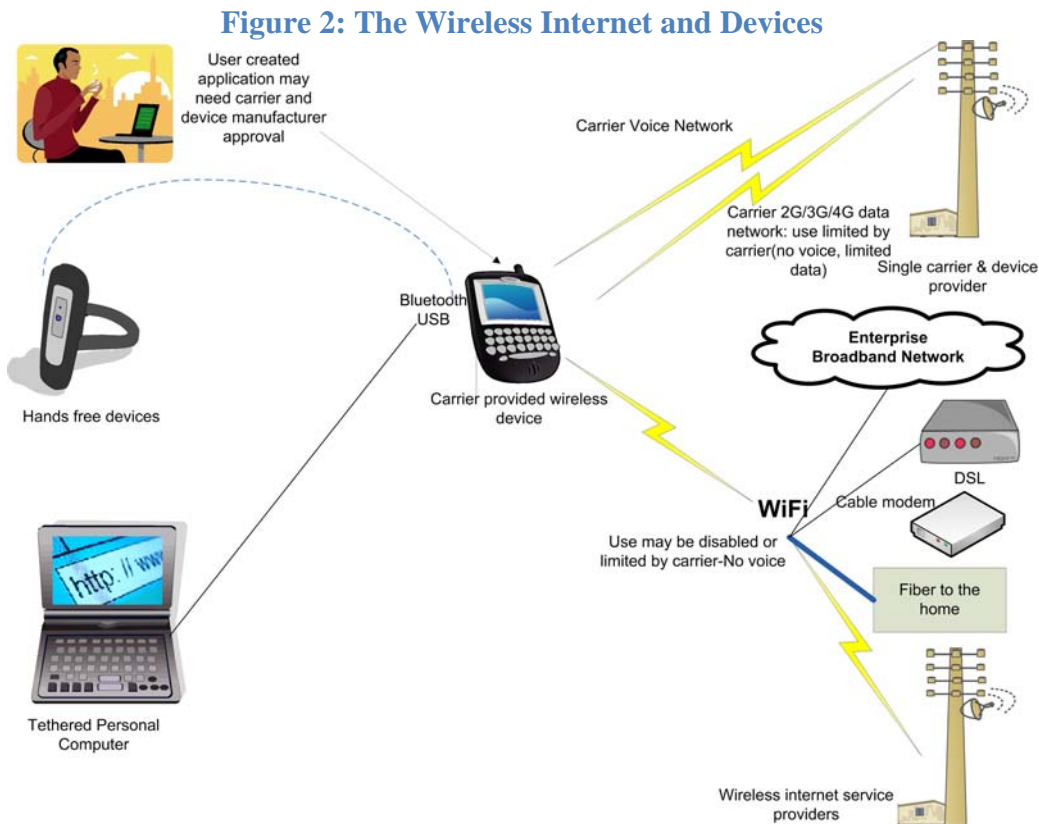
With advances in hardware performance, computers have become more compact and portable. The flexibility of the computer is available in smaller packages, approaching the size of personal digital assistants (PDAs) and smart phone devices.

Many people take the current interoperable computer environment for granted—but until the 1990s the picture was different. Computer manufacturers were separated into separate, siloed groupings (Windows, Macintosh, UNIX) with separate types of incompatible operating systems, applications, and content. Some manufacturers prohibited users from opening their computers or adding non-manufacturer supplied parts. Modems or peripherals were strictly for one type of device, as was software.

**The point is this: technology can evolve, and environments that are closed, exclusive, and non-interoperable can cease to be so.** This Report suggests that the FCC can enable and facilitate technological evolution in the wireless realm through widely-accepted communications industry processes such as standards-writing, certification, and neutrality—and that transparency is essential for technical compliance and verification.

## 2. TOWARD A WIRELESS “ANY DEVICE” ENVIRONMENT

Wireless technologies now provide many of the capabilities that were once available only on fixed, wireline devices. Wireless users can surf the Internet, receive audio and video streams, share photos and video, connect to instant messaging and social networking applications, and obtain a rich range of applications developed by both established and emerging companies and by individuals (Figure 2).



However, the environment around wireless devices differs from that of wireline in critical ways that limits device capability and flexibility. These differences are created through a range of near-universal technology practices among U.S. wireless carriers.<sup>4</sup> Specifically, the carriers, in cooperation with their selected manufacturers:

1. Provide almost all carrier-network wireless devices to consumers.
2. Restrict the types of devices that can operate on their networks.
3. Limit the types of applications that can operate on the devices and on the networks.
4. Limit types of peripherals and outside devices that can connect to approved devices.
5. Limit how devices can connect to WiFi, Bluetooth, and other networks.
6. Restrict how devices can be used on other networks.

<sup>4</sup> These practices are almost universal in the U.S. but not necessarily abroad, as is discussed further below.

To some degree, some of these limitations result from processing speed, miniaturization, and software development; these limitations will decrease or shift as the technologies further mature, assuming that the carriers and manufacturers choose to allow such evolving capabilities on the devices.

To a great degree, however, these limitations are matters of business decisions rather than technology needs, built into the devices by the manufacturers at the direction of their customers, the carriers. In this way, these limitations are not required or fundamental to the relevant wireless technologies—and there exist established industry processes that can, with appropriate direction, enable development and deployment of systems without these limitations.

In the Any Device environment envisioned here:

1. Devices are standardized, manufactured, and configured such that consumer purchase of devices is not *of necessity* part of the same transaction as consumer purchase of wireless service—in other words, there is no technical bar built into the device itself or its certification process that would lock the device to one carrier or network or block its use on any other network.
2. Device developers and others can publicly obtain all needed information to build devices that are able to use the full functionality of the service provider network.
3. Devices are tested and certified by a government or third-party entity to ensure that they comply with industry standards and that they do not create harm to the network.
4. Users can connect their certified devices to any networks matching the technology of the device (GSM,<sup>5</sup> CDMA,<sup>6,7</sup> WiMAX, or LTE<sup>8</sup>), needing only to provide identifying information and means of payment. If the users wish to switch networks, they could do so by switching a small detachable security card with a card from their new carrier.

---

<sup>5</sup> Global System for Mobile Communication (GSM) was first developed in the 1980s and was standardized by the European Telecommunications Standards Institute (ETSI) in the 1990s. Prior to the 1980s, each country used its own specific cellular communication system. In the mid-1980s, several European nations began the process of standardizing digital cellular systems and, in 1992, ETSI was given responsibility for finalizing the technical standards. In the U.S., AT&T, and T-Mobile are the major GSM carriers.

<sup>6</sup> Code Division Multiple Access (CDMA) was developed by Qualcomm and standardized by the Telecommunications Industry Association.

(<http://www.tiaonline.org/standards/technology/cdma2000/cdma2000table.cfm>) in cooperation with the CDMA Development Group (<http://www.cdg.org/>). The initial implementation of GSM and CDMA is known as the second generation (2G) of mobile technology. CDMA is now used by network operators in the U.S., Canada, Asia, and Latin America. In the U.S., Verizon and Sprint Nextel are the major CDMA carriers.

<sup>7</sup> The third generation (3G) of mobile technology represents the evolution of those two protocols. The GSM community developed the GPRS, EDGE, and UMTS technologies, while the CDMA community developed CDMA2000 and EV-DO.

<sup>8</sup> The latest mobile technology development is called fourth generation (4G). It includes WiMAX (an IEEE standard) and Long Term Evolution (LTE), in development by the 3<sup>rd</sup> Generation Partnership Project (3GPP). These technologies are intended to support the need of higher-data-rate applications.

To these ends, this section of this Report offers the following analysis:

1. Notes the existing processes that have resulted in some openness with respect to wireless devices, primarily as a result of government requirements or pressure from outside the incumbent wireless industry.
2. Describes four different scenarios that are sometimes called Any Device regimes, and notes that all are not equal, and that “tethering,” in particular, is not a true Any Device strategy.
3. Makes recommendations regarding certification processes and how they can be used to migrate to an Any Device environment.

## **2.1 Existing Carriers Already Prove the Feasibility of Any Device**

An Any Device environment can be a simple evolution of the existing wireless environment. In some limited ways, the wireless communications industry has adopted some elements of Any Device through pressure of various sorts, including the FCC requirement for an open device environment for a part of the 700 MHz band.

### **2.1.1 A Robust Any Device Environment Exists on the GSM Platform Internationally**

An Any Device approach is hardly alien to the wireless telecommunications industry. An Any Device environment exists in many parts of the world where the GSM technology is dominant, and where government mandates or carrier policies enable consumers to unlock devices so that they can be connected to any compatible GSM network. For example, in Brazil, Denmark, Finland, France, Hong Kong, Italy, and Romania, government regulators limit how long a carrier may lock a device or require that carriers unlock devices upon request at the end of a contract. In Singapore, carriers are not permitted to lock GSM devices. In Belgium, GSM devices are all sold without locks, in compliance with anti-bundling laws. In Britain, Germany, Netherlands, Portugal, and Spain, there is no formal regulatory requirement for device unlocking, but carriers unlock most devices if users have had the devices for a given period or have completed their contracts.

The GSM standards for both the mobile core network and the mobile subscriber device enable interoperability between different vendor equipment and network operators. The development of a common type of Subscriber Identity Module (SIM) card, in particular, provides GSM devices additional flexibility and was one of the main reasons for the popularity of the GSM standard at a time when no other such common standard for digital communication was available.

The SIM card enables interoperability of devices between different GSM service providers. Users remove the SIM cards from their devices and replace them with new SIM cards from a different carrier—thus enabling them to use the same device with service from a new provider.<sup>9</sup>

It is entirely normal for consumers in other countries to connect their GSM telephones to any carrier network simply by obtaining a carrier's SIM card and inserting it into an unlocked telephone. The device does not need to be on an approved list of devices or to have undergone any carrier-specific compliance testing, though it is tested for compliance with the GSM technology standard. This open wireless regime was part of the vision of wireless communications under the GSM model.<sup>10</sup> The proposed Any Device process recommended here draws on this experience, and demonstrates how it can apply to technologies beyond GSM and beyond voice.

### **2.1.2 Under FCC Requirements, Verizon Already Implemented Open Development Parameters, a First Step Toward Any Device**

As part of the latest 700 MHz spectrum auction, the FCC required licensees of the C Block to agree to open device rules.<sup>11</sup> Verizon Wireless plans to use this block for its 4G LTE deployment. To meet the FCC's requirement, Verizon created an Open Development Initiative forum<sup>12</sup> and has published technical specifications for designers and manufacturers to develop network-compliant devices.

Under this initiative, manufacturers comply with the technical specifications and submit their devices to Verizon for compliance testing. Several manufacturers, including Cisco Systems and many smaller companies, have gone through this process and certified devices for use on Verizon's CDMA network.

Relative to past practices, and the practices of other carriers, the initiative provides more public transparency into the requirements of the carrier, which can then be reviewed based on the need for the requirements and the actual harm they might present. In contrast to a true Any Device

---

<sup>9</sup> GSM standards require that all user information on GSM devices be stored on a removable SIM card. The SIM card contains an International Mobile Subscriber Identity number, which enables the carrier to authenticate the subscriber's account. [http://pda.etsi.org/exchangefolder/ts\\_100927v070800p.pdf](http://pda.etsi.org/exchangefolder/ts_100927v070800p.pdf) (accessed January 4, 2010). It also contains a secret key for network authentication and account information for billing purposes and to enable a user's subscribed services. Thus, with GSM devices, subscribers can move all of their services to a new device by switching the SIM card from one mobile device to another. Each GSM device also has a unique International Mobile Equipment Identity number assigned by its manufacturer, which GSM network operators can compare to numbers in an equipment identity register database to check the validity of the mobile device.

<sup>10</sup> ETSI. "TS 100 927 V7.8.0 (2003-09)." Technical Specification (2003).  
[http://pda.etsi.org/exchangefolder/ts\\_100927v070800p.pdf](http://pda.etsi.org/exchangefolder/ts_100927v070800p.pdf) (accessed January 4, 2010).

<sup>11</sup> Second Notice of Proposed Rulemaking, 07-132, *In the Matter of Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150, released August 10, 2007, [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-07-132A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-132A1.pdf) (accessed January 5, 2010).

<sup>12</sup> Verizon Wireless. "Verizon Wireless Open Development Initiative." Website.  
<https://www22.verizon.com/opendev/> (accessed January 4, 2010).

environment, however, the process is entirely in the hands of Verizon Wireless, and requires testing by Verizon in its laboratory, thereby placing significant control and veto power in the hands of the carrier.

### **2.1.3 Carriers Already Enable Roaming, a Form of Any Device**

Roaming is the means by which devices designed to operate on a particular carrier network are also able to operate on other networks (partner networks) that have agreements with the primary carrier. In order to successfully roam, a device must be compatible with the technology type of the network (CDMA or GSM), and the roaming partner must be able to verify that the user is authorized. Both the CDMA and GSM standards specify technically how roaming occurs, and specify the roles of the participating carriers. Most carriers have roaming agreements in order for devices to continue operating outside their service areas, and devices transparently roam as needed.

However, the fact that roaming is possible is not always sufficient to provide full portability of a device from carrier to carrier. As will be discussed below, in the case of CDMA devices, the carrier controls the security keys of the device. When roaming occurs, the roaming network verifies the identity of the device by communicating with the primary carrier but does not itself have access to the key—authentication of the device is always linked to the primary carrier, unless the device has a Removable User Identity Module (R-UIM)<sup>13</sup> card that can be replaced with a card from another carrier.

### **2.1.4 Carriers Already Use Multiband and Multi-Protocol Devices**

U.S. carriers have different spectrum assignments in different parts of the country. As a result, many carriers must use devices that can operate on both the Cellular and PCS bands to provide seamless, ubiquitous coverage to their users. For example, if a carrier operates services in both the 800 MHz and 1900 MHz bands in major metropolitan areas but only uses the 800 MHz band in rural areas, then devices need to operate in both bands to use that carrier network. Dual-band functionality is also necessary if a carrier supports roaming to provide service when customers are using devices outside the carrier's service area.

Cellular networks outside the U.S. operate on different frequency spectrum altogether, so using a phone in Europe, for example, may require at least tri-band capability. Some devices support quad-band frequencies, which operate on every band currently used worldwide and thus allow seamless use of the devices wherever a user may travel.

Some carriers offer “world” devices with electronics and software for operating on both CDMA and GSM networks. These “multi-protocol” devices enable CDMA users in the U.S. to use either CDMA or GSM services in other countries through roaming agreements with other carriers. If

---

<sup>13</sup> R-UIM cards serve similar purposes in CDMA networks in China, India, and Thailand as do SIM cards in GSM networks globally. These cards are not currently used by U.S. CDMA carriers.

the carrier unlocks the device, the user can switch SIM cards and operate the phone on any GSM network, in the U.S. or internationally.

In an Any Device regime, multi-band and multi-protocol devices offer a broader range of technical abilities to make a device portable from one carrier to another. For example, existing “world” devices, if unlocked by the carrier, are capable of operating on the network of any GSM provider (with the appropriate SIM card), plus the primary CDMA carrier and any CDMA roaming partner of that carrier. Future devices incorporating R-UIM would have portability to any GSM or CDMA network with the appropriate R-UIM or SIM card. Devices including LTE and WiMAX would be able to connect to those networks as well.

As software-based devices are introduced, it will be possible to incorporate this functionality in software rather than in separate hardware modules within the device, and potentially the functionality of the detachable card can be performed by software as well.

This type of device would provide the ideal level of interoperability—enabling the manufacturer to offer a single device for any network, and enabling the user to switch from network to network.

## **2.2 There Exist Multiple Layers of “Any Device” Interoperability—and All Are Not Equal**

From a technical standpoint, there exist a range of potential Any Device approaches, but they are not equal or comparable. Most significantly, “tethering” should be distinguished from a full Any Device environment: tethering enables consumers to tether any device to a carrier-approved and -limited device—not to the network—such that the carrier-limited device mediates and limits the capabilities of the tethered device. This “any device” regime is dramatically different in technical effect to an environment in which a consumer has a true choice of attaching Any Device to any current or future service provider, out of the box, as in a wireline environment.

The following describes four distinct Any Device environments, in order of levels of interoperability, beginning with tethering, the least open of all, and ending with an open Any Device environment akin to the one that exists in wireline:

1. Tethering a device through a standard interface
2. Connecting Any Device to any single carrier network
3. Connecting Any Device to any carrier network that uses a common technology such as CDMA or GSM
4. Connecting Any Device to any network regardless of whether the carrier uses CDMA or GSM

### 2.2.1 Tethering a Device Through a Standard Interface

A device can connect to a wireless carrier data network by tethering through a standard interface (Figure 3). An example would be to connect a personal computer through its PC Card or USB or Ethernet interface to a wireless dongle or wireless phone. From a purely technical perspective the user can use any network-capable application on the personal computer. Because the personal computer is connected through a standard interface, neither the computer nor the device need “know” it is on a particular carrier network—the device simply connects through the interface and operates according to the instructions in the software and device drivers.

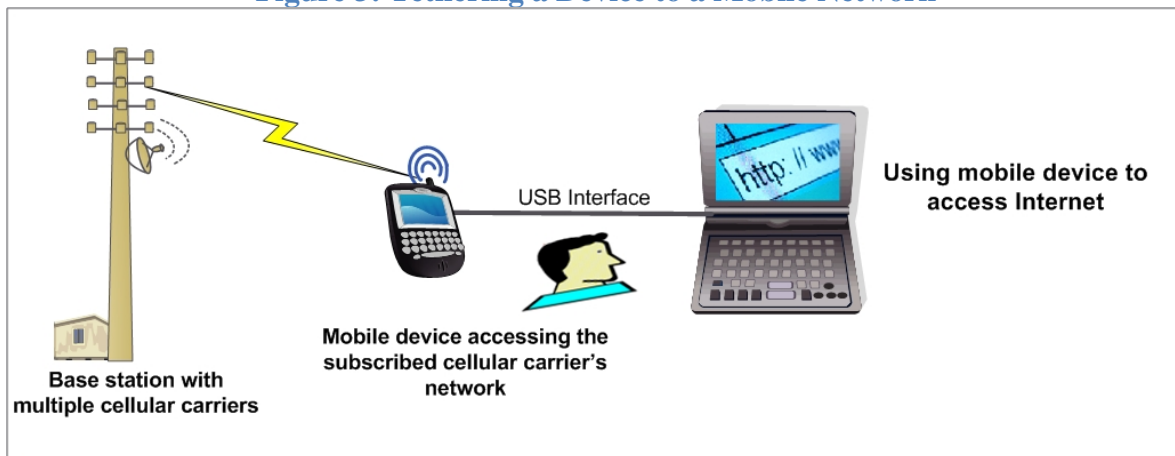
However, tethering is limited because it is costly, inconvenient, and less functional than a single integrated device. As a result, network users relying on tethering are generally receiving an inferior experience to those using an integrated device, and an environment that purported to achieve Any Device through tethering alone would create an unfair disadvantage for non-carrier-provided devices.

The user relying on tethering would not be using “Any Device” but would be required to use a carrier-provided device. The user would need to purchase the device, with a cost ranging from approximately \$50 to hundreds of dollars. Tethering users do not have the easy portability of a single integrated device and may need to separately connect power to the separate device. The user will typically need to install device drivers and make the two devices compatible and synchronize them. The user is subject to the technical limitations of the physical interface of the tethering device and any potential data transmission controls on or impacting the tethering device put in place by the carrier—including incremental buffering delays, intentional traffic blocking, or speed reduction. Some carriers prohibit tethering under the terms of their subscriber agreements.<sup>14</sup>

---

<sup>14</sup> For example, T-Mobile ([http://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr\\_Ftr\\_TermsAndConditions](http://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions), accessed January 4, 2010) and AT&T (<http://www.wireless.att.com/cell-phone-service/legal/plan-terms.jsp#data>, accessed January 4, 2010).

**Figure 3: Tethering a Device to a Mobile Network**



### 2.2.2 Connecting Any Device to Any Single Carrier Network

The next level of interoperability would be for a manufacturer to be able develop a device independently of any service provider and to activate and operate that device on a single service provider network. This does not necessarily confer any ability to operate the same device on multiple networks—for example, a developer would only be able to create a device exclusively for use on the Verizon Wireless network. The device manufacturer would need to comply with applicable industry and government standards. Users of the device would purchase it through a retail outlet, follow a connection/installation procedure, and connect it to the network. The carrier's compatibility requirements and the connection and installation procedures would be available without restriction to the manufacturer and the user, and the device would not need to go through a carrier-run review process. Compatibility requirements would be limited to preventing harm to the network and other users.

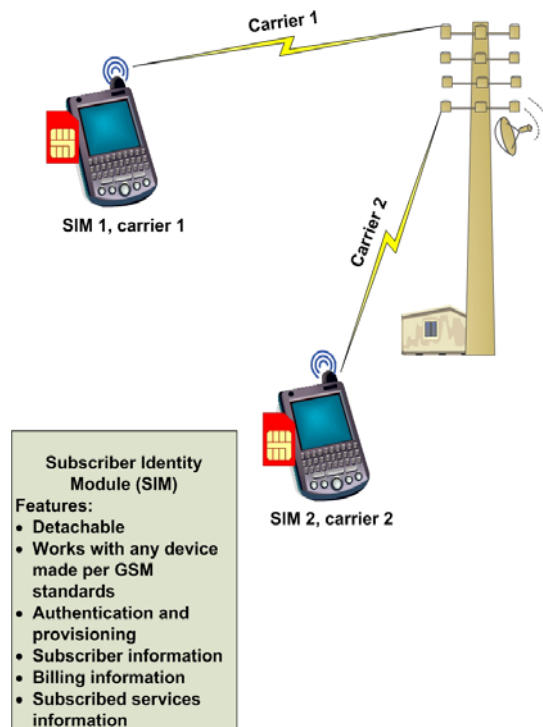
### 2.2.3 Connecting Any Device to Any Network Using a Common Technology Platform

The next level of interoperability would be for a manufacturer to develop a device independently of any service provider and to activate and operate that device on any network using a compatible technology (see Figure 5 and discussion of GSM and CDMA above). The device manufacturer would comply with applicable industry and government standards, and users of the device would purchase it through a retail outlet, follow a connection/installation procedure, and connect to the network. The carriers' compatibility requirements and the connection and installation procedures would be available without restriction to the manufacturer and the user, and the device would not need to go through a carrier-run review process. Compatibility requirements would be limited to preventing harm to the network and other users. The advance

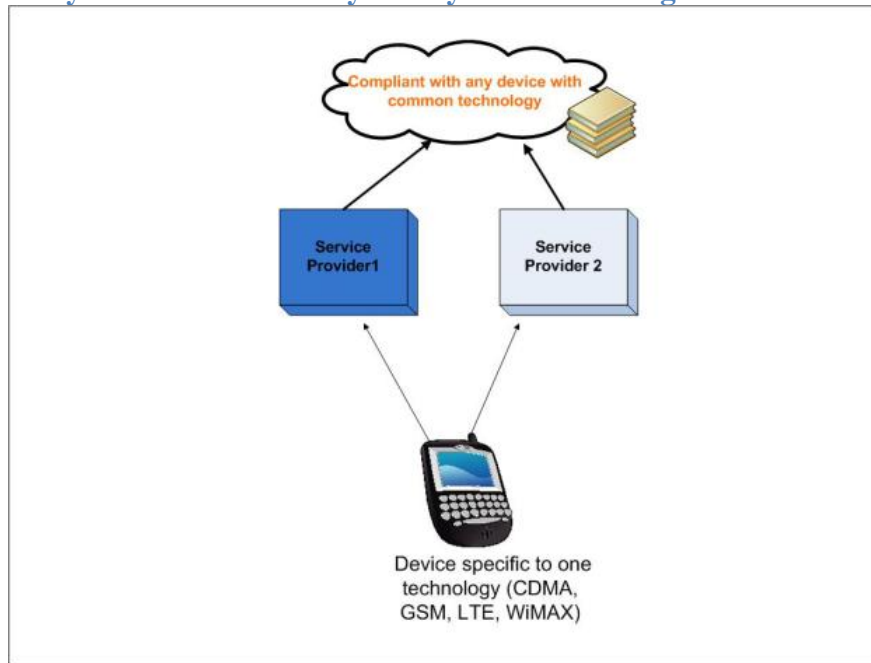
relative to Section 2.2.2 is that the manufacturer could make a single device that operated for a wider range of providers and that could also be portable among multiple service providers—the user would no longer need to obtain a new device to connect to another service provider (although the user would be limited to a service provider that uses a technology type that is supported by the device).

One way to achieve this level of interoperability is to use a small, carrier-specific detachable card inserted the device. The difference between this approach and tethering is that the card is a much less expensive and cumbersome device than the tethering device. It costs only a few dollars, is contained entirely in the form factor of the device, requires no external power or drivers, and does not reduce the speed of the device. If a user wished to connect to a different network, the user would simply obtain a card from that other carrier and switch the card. An example of this approach is the current use of Subscriber Identity Module (SIM) cards in the GSM technology used worldwide, including in approximately half of U.S. carrier-provided wireless devices (Figure 4). Another is the R-UIM (Removable User Identity Module) card used in CDMA networks in China, India, and Thailand (and potentially an option for the other wireless networks in the U.S.).

**Figure 4: Use of SIM Card to Obtain Connectivity to Mobile Network**



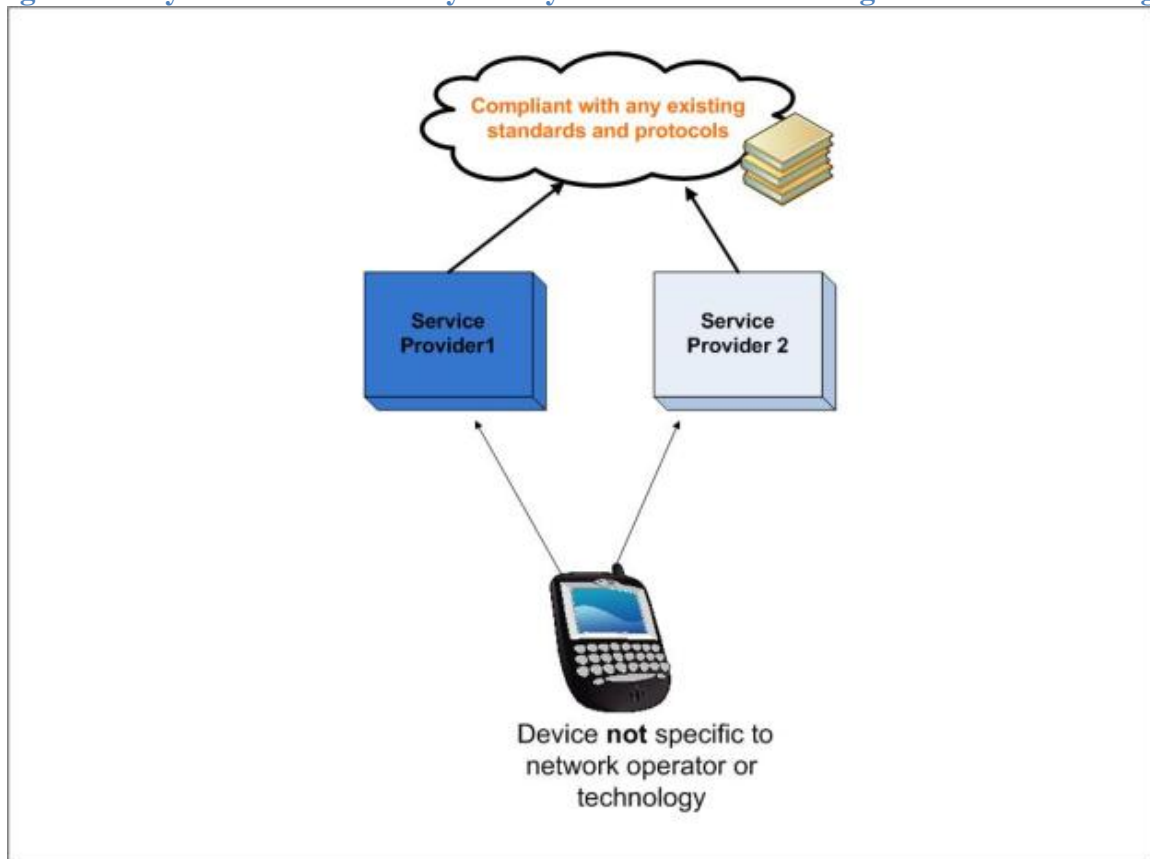
**Figure 5: Any Device Connectivity to Any Network Using Either GSM or CDMA**



### 2.2.4 Connecting Any Device to Any Wireless Network Regardless of Technology Platform

The next logical step would be for a manufacturer to develop a device independently of any service provider, and for that device to activate and operate on any service provider network (Figure 6). This could be accomplished by including software and hardware in the device that is compatible with all of the available technologies and service provider networks. This may be a longer-term objective, but may be more achievable 1) as hardware becomes more miniaturized and less expensive, 2) if Universal Integrated Circuit Card (UICC) devices compatible with both CDMA and GSM are deployed, 3) if devices with multiple slots (for GSM SIM and R-UIM) are available, 4) as software-based radios make compatibility through software more feasible, or 5) if a single technology becomes dominant in the wireless marketplace.

**Figure 6: Any Device Connectivity to Any Wireless Network Regardless of Technology**



## **2.3 The Established Standards-Writing and Certification Processes Provide a Reliable Path Toward Any Device and Resolution of Its Complications**

Enabling evolution of standards entities and processes can result in an Any Device environment in which the device certification process is transparent and independent of any single wireless carrier.

The standards-writing and certification processes have already enabled significant potential device interoperability within technologies, either GSM or CDMA, and can be further utilized to enhance this interoperability. As a result of the standards-writing and certification processes already in existence, any GSM device is technically capable of operating on any GSM network; similarly, any CDMA device has the technical capability to operate on any CDMA network.<sup>15</sup> While the existence of these two different technology platforms is a limit to full interoperability between the two platforms, the existence of standardized technologies can make it possible for a device to operate on several networks within each platform, and creates a framework for creating devices independent of carrier involvement.

### **2.3.1 The Existing Certification Process**

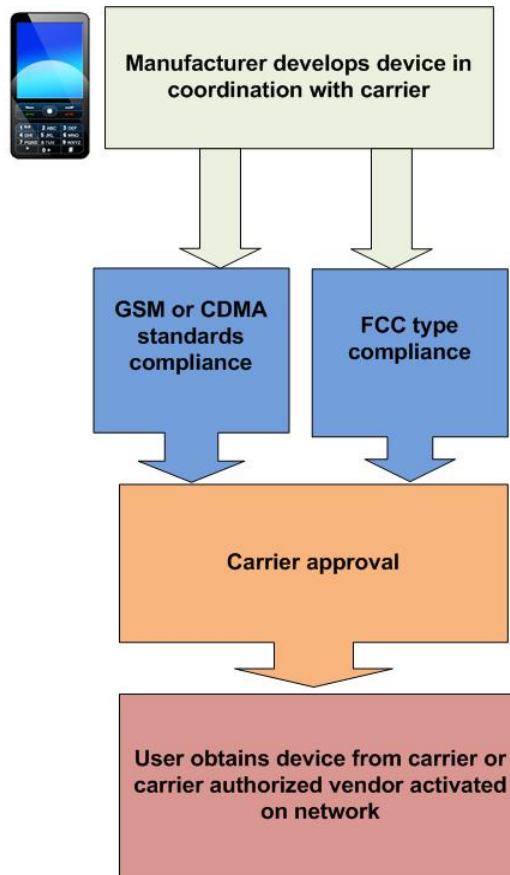
In current U.S. practice, wireless devices are certified on three separate levels (Figure 7):

1. Compliance with industry technology standards
2. Compliance with FCC rules
3. Compliance with carrier requirements

---

<sup>15</sup> Current U.S. CDMA devices have limited portability from one CDMA network to another CDMA network, however, because of the carrier and subscriber identity components built into the devices.

**Figure 7: Current U.S. Wireless Device Certification**



### ***2.3.1.1 Devices Are Independently Certified to Meet Protocol Standards***

First, the device is independently certified as meeting the GSM or CDMA protocol’s standards.

Both GSM and CDMA are mature technologies governed by standards-making bodies. GSM network and device standards<sup>16</sup> are established by the European Telecommunications Standards Institute (ETSI) and Third Generation Partnership Project (3GPP). CDMA standards<sup>17</sup> are established jointly by the Telecommunications Industry Association (TIA) and the CDMA Development Group (CDG).

<sup>16</sup> 3GPP. “TS 151 010-5 V8.3.0 (2009-10).” Technical Specification (2009), [http://pda.etsi.org/pda/copy\\_file.asp?Action\\_type=&Action\\_Nb=&Profile\\_id=N3nr,CVNht\\_nbViYcdvXoXiZoxpnSGc91&Wki\\_Id=V2rcsJRmZu364ACByJ5iF](http://pda.etsi.org/pda/copy_file.asp?Action_type=&Action_Nb=&Profile_id=N3nr,CVNht_nbViYcdvXoXiZoxpnSGc91&Wki_Id=V2rcsJRmZu364ACByJ5iF) (accessed January 4, 2010).

<sup>17</sup> TIA. “ANSI/TIA-98-F-1-2006.” TIA Standard (2006). [http://www.tiaonline.org/standards/technology/cdma2000/documents/tia-98-f-1\\_final\\_for\\_publication.pdf](http://www.tiaonline.org/standards/technology/cdma2000/documents/tia-98-f-1_final_for_publication.pdf) (accessed January 4, 2010).

These industry technology standards encompass a range of specifications and operating processes, including:

1. RF physical-layer behavior, including modulation and non-interference
2. Minimum recommended functional standards for base stations
3. Minimum recommended functional standards for mobile devices
4. Device provisioning and authentication requirements
5. Signaling and network access requirements
6. Optional features, such as locking devices to the operator network

The GSM and CDMA certification organizations are made up of wireless carriers, device manufacturers, and other related parties. Their labs test devices to ensure that they meet all standards for that technology.

GSM devices are certified by PTCRB, an organization that was created by wireless carriers and is administered by CTIA, the industry's trade association.<sup>18</sup> The devices are certified based on the requirements specified in the 3GPP test cases to verify that they operate as expected. Certification is performed in PTCRB-accredited labs. Even a pre-certified module needs to be submitted to PTCRB for a final approval and seal.<sup>19</sup>

CDMA devices are certified by the CDMA Certification Forum (CCF), which ensures that all certified devices are manufactured per the minimum standards specified by the TIA and adhere to the performance, signaling, and application test cases.<sup>20</sup>

### *2.3.1.2 Devices Are Certified by the FCC to Ensure Licensing Compliance*

Second, the device is certified by the FCC. FCC certification currently involves meeting the requirements set forth in the frequency licensing and 911 requirements. The FCC also evaluates devices to ensure that they comply with standards for output power limits, RF emission levels for human safety, and interference.

By means of this existing process, the FCC is already in the business of certifying that devices comply with a range of safety regulations, as well as with the protections the FCC extends to carriers through frequency licensing—protections, from such things as interference, that enable carriers to operate networks in commercially viable and reliable ways.

---

<sup>18</sup> PTCRB. "Welcome to PTCRB." Website. <http://www.ptcrb.com/index.cfm?tab=about> (accessed January 4, 2010).

<sup>19</sup> The 7 layers group. "PTCRB Certification Services." Website. [http://www.7layers.com/PTCRB\\_index.asp](http://www.7layers.com/PTCRB_index.asp) (accessed January 4, 2010).

<sup>20</sup> CDMA Development Group. "CDMA Certification Forum: The Official Test and Certification Forum for All CDMA2000 Devices." Device Test and Certification Fact Sheet (June 2009). [http://www.globalccf.org/CDG\\_Retirement.pdf](http://www.globalccf.org/CDG_Retirement.pdf) (accessed January 11, 2010).

### ***2.3.1.3 Devices Are Certified by Individual Carriers to Meet Carrier-Specific Requirements***

Finally, carriers typically require that each device be certified to meet the wireless carrier's own specific requirements before the carrier accepts the device for operation on its network. Carrier certification involves the specific criteria developed by each individual carrier in its sole discretion. For example, Verizon Wireless specifies details about the handoff criteria between 1xRTT (2G) and 1xEV-DO (3G) and between the specific frequency bands used by Verizon Wireless.<sup>21</sup> The specific criteria are not mandatory industry requirements, but Verizon judges them important to ensure successful handoff between sites. Verizon also requires devices to have a USB port for tethering and device maintenance.

AT&T's Specialty Vertical Device Certification Program requires enhanced network selection (ENS), which enables a device on AT&T's network to identify a site formerly owned by Cingular (with which AT&T merged) as a "home" location, not a roaming network.<sup>22</sup> It also requires use of "a radio module that has been previously certified by AT&T."

Many of these requirements are not extensive or difficult for a manufacturer to address and may simply be specific settings chosen within a standards-compliant device. Some may appear to be more restrictive (for example, the requirement for a "radio module previously certified by AT&T"), and it is not obvious how critical they are to preventing harm on the network, or whether a more flexible approach can be equally workable. In any case, both AT&T and Verizon require testing within their own labs, using carrier-designed test plans, and the carriers have the final word on whether a device is allowed on the network.

### **2.3.2 The Proposed Certification Process for Any Device**

Through additional standards development and resulting certification, required device functionalities can expand to enable third-party-certified devices to operate on carrier networks without carrier-specific certification requirements (see Figure 8). The process will afford device developers access to a full set of requirements for a device that is ready to connect to any provider network. It will specify a publicly available test plan to verify this functionality. All testing will be performed by third parties not affiliated with carriers.

Under this plan, the developer will have access to a full, publicly available standard, incorporating the existing standards and any additional requirements to prevent harm to carrier networks or other users. In this way, the wireless standards will be comparable to the Data over Cable Modem Service Interface Specification (DOCSIS) that enables a customer to buy a

---

<sup>21</sup> Verizon Wireless. "Verizon Wireless Open Development Initiative." Website.

[https://www22.verizon.com/opendev/Forum/developer\\_document\\_archive.aspx](https://www22.verizon.com/opendev/Forum/developer_document_archive.aspx) (accessed January 4, 2010).

<sup>22</sup> AT&T. "Welcome to the AT&T Specialty Vertical Device Certification Program." Fact Sheet (2007). [http://developer.att.com/devcentral/go\\_to\\_market/enterprise\\_software\\_certification/docs/SVD\\_Welcome\\_Kit\\_Electronic\\_Version\\_with\\_Hot\\_Link.pdf](http://developer.att.com/devcentral/go_to_market/enterprise_software_certification/docs/SVD_Welcome_Kit_Electronic_Version_with_Hot_Link.pdf) (accessed January 11, 2010).

DOCSIS cable modem, use it on any cable system, and switch it from system to system.<sup>23</sup> The developer will submit the device for testing by the FCC and by the appropriate third-party entity. As with many cable modem network operators, carriers may still elect to publish a list of compatible devices for which they will provide support (although, strictly speaking, this “support” should not be necessary for a device to be technically compatible with the network). In the case of cable modems, network operator support of particular cable modem models is extensive and does not seem to have hindered the highly competitive development of cable modem user hardware, as the DOCSIS standards are openly available, detailed, and designed to enable backward compatibility between different versions.

Once the device is certified, it will be legal to sell the device and activate it on networks compatible with that device’s wireless technology type. Users will obtain the device at a range of online or traditional retail outlets or on the Internet. The user will activate the device according to publicly available instructions.

On GSM networks, the most straightforward means to activate the device will be to insert a Subscriber Identity Module (SIM) card from the carrier of the user’s choice. SIM cards are already used on all GSM devices.

On CDMA networks, an ideal outcome will be for users to obtain from the carrier and insert into the phone a Removable User Identity Module (R-UIM) card, a removable card used in CDMA networks that holds user identification data and user-input data, much as does the SIM card on GSM networks. R-UIM cards are not currently widely used in the U.S., but are in wide use in China and India.<sup>24</sup>

R-UIMs are not the only conceivable means of achieving Any Device in CDMA, but adopting R-UIMs has several concrete advantages, because they create a clean separation between device and carrier<sup>25</sup> and they are already proven and mass-produced. Adopting R-UIMs can also help carriers avoid a potentially extensive and complex process of determining how to securely share security keys on CDMA devices, as discussed in Section 2.3.4. The separation of device and carrier provides the option for equipment manufacturers and retailers to sell, and users to buy, off-the-shelf devices that are “plug and play” and do not require permission from the carriers, as is the norm for PCs and wireline ISPs.

To reach this process, the government or a third-party entity (potentially the entities developing the existing wireless technology specifications, or the Internet Engineering Task Force (IETF) developing the Internet standards) will need to review the current carrier-specific requirements and 1) evaluate the extent to which these prevent harm to the network and 2) update them to

---

<sup>23</sup> The wireless standard, however, would be tailored to each of the wireless technologies (CDMA, GSM, WiMAX, and LTE).

<sup>24</sup> Samsung India. Samsung Duo Product Description. <http://www.samsungcdma.in/samsung-duo-cdma-mobile-phone.aspx> (accessed January 11, 2010).

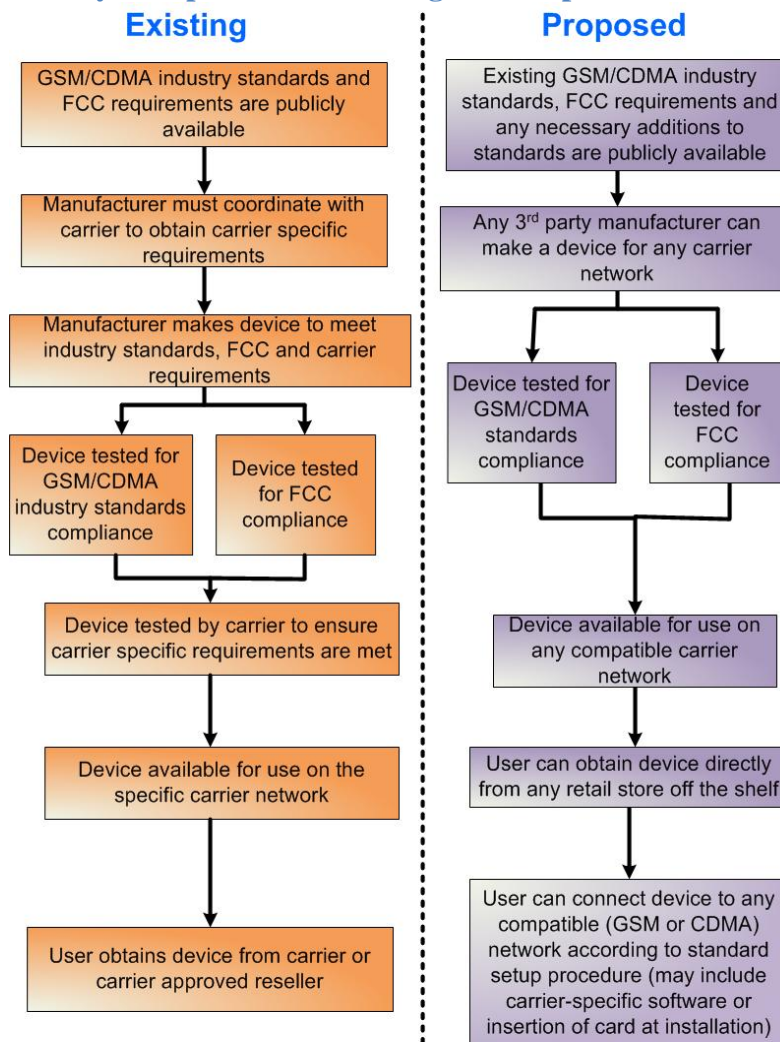
<sup>25</sup> Adopting R-UIMs can also help carriers avoid a potentially extensive and complex process of determining how to securely share security keys on CDMA devices, as discussed in Section 2.3.4.

include any additional requirements that can be justified to prevent harm. If the requirements are not necessary to protect the network from harm, they should be eliminated. The government or third party will also be able to evolve the standards, as called for by changes driven by technological evolution.

Carriers will still have the capability to require particular settings of standards-compliant equipment, such as carrier-specific information about roaming, and these can be incorporated into a firmware or software update at the time of activation or direct entry by the user.

Figure 8 illustrates the existing and proposed certification processes.

**Figure 8: Summary Comparison of Existing and Proposed Certification Processes**



### 2.3.3 Evolution to Any Device in a GSM Environment

Because they have detachable SIM cards, GSM technology devices have the lowest technical barrier to an Any Device regime and therefore the most straightforward path to compliance. If a GSM device is unlocked by the carrier, any functions relating to user identification, billing, and authentication can be switched simply by switching the SIM card to a SIM card from a new carrier.

In the U.S., T-Mobile offers its services to subscribers both through carrier provided devices and through carrier-provided SIM cards. A subscriber with a GSM-capable device can obtain services through T-Mobile, even if the device were purchased from AT&T or from a carrier outside the U.S. According to T-Mobile, roughly one million iPhones already operate on its network, along with many other “grey” devices, and T-Mobile takes steps to accommodate them.<sup>26</sup> As of this writing, AT&T does not offer this type of service.

The GSM standards for both the mobile core network and the mobile subscriber device enable interoperability between different vendor equipment and network operators. The development of a common type of SIM card provides GSM devices additional flexibility and was one of the main reasons for the popularity of the GSM standard at a time when no other such common standard for digital communication was available.

The following practices are recommended to ensure that the Any Device vision of the FCC’s Open Internet NPRM works in a GSM environment:

#### 2.3.3.1 Enable Network Use Through SIM Cards

In the Any Device environment envisioned here, GSM carriers will be able to continue using the same types of devices and networks, with the exception that they also sell their service to their customers through SIM cards, as well as through providing devices. By taking this step, carriers will separate the offering of the device from the offering of the service. All carrier-specific information and functions will be in a physically separate card that can snap in and out and could be moved to a separate device.

Customers should not be allowed to be treated differently based on whether the customer’s device is carrier-provided or customer-provided with a carrier SIM. This would be a change in business processes but would require no new technological change or evolution.

Existing GSM standards require that all user information on GSM devices be stored on a removable SIM card (Figure 9). The SIM card contains an IMSI (International Mobile Subscriber Identity) number, which enables the carrier to authenticate the subscriber’s account.<sup>27</sup> It also contains a secret key for network authentication and account information for billing

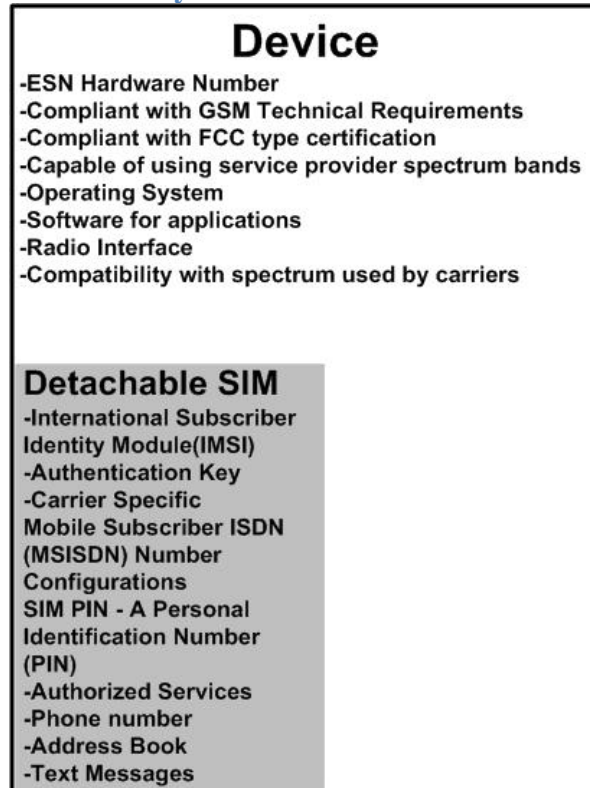
---

<sup>26</sup> T-Mobile engineering staff, in discussion with the New America Foundation and CTC, December 16, 2009.

<sup>27</sup> ETSI. “TS 100 927 V7.8.0 (2003-09).” Technical Specification (2003).  
[http://pda.etsi.org/exchange/etsi/ts\\_100927v070800p.pdf](http://pda.etsi.org/exchange/etsi/ts_100927v070800p.pdf) (accessed January 4, 2010).

purposes and to enable a user's subscribed services. Thus, with GSM devices, subscribers can move all of their services to a new device by switching the SIM card from one mobile device to another. Each GSM device also has a unique International Mobile Equipment Identity (IMEI) number assigned by its manufacturer, which GSM network operators can compare to numbers in an equipment identity register (EIR) database to check the validity of the mobile device.

**Figure 9: Functionality of Wireless Device and Detachable SIM**



Technically speaking, the SIM card enables interoperability of devices between different GSM service providers. Users could then remove the SIM cards from their devices and replace them with new SIM cards from a different carrier—thus enabling them to use the same device with service from a new provider.

### **2.3.3.2 Enable Device Unlocking**

Carriers are technically capable of locking devices such that they cannot be transferred to another carrier. In the GSM world, this practice is also known as SIM-locking. Locking is a competitive tactic that prevents users from switching the device to other carrier by removing the SIM card and replacing it with a SIM from another carrier. It is done by programming the device before it is sold.

Locking of a device is a technical mechanism that is used as a business and sales mechanism; it is not necessary for the functioning of the device and is not related to the authentication/identification function of the SIM card itself.

In the U.S., almost all GSM devices are sold locked. AT&T's current policy is to unlock phones upon request after the contract term is complete, with the exceptions of iPhones, which are never unlocked in the U.S. under AT&T's agreement with Apple, and T-Mobile's general policy is to unlock devices upon request if the user has been a customer for 90 days or more.<sup>28</sup>

Carriers can unlock a device over the air, at a store, or by sending the user a code by email to enter into the device. Once a device is unlocked, the user can insert a different SIM card and be activated as a customer on another carrier network.<sup>29</sup>

### ***2.3.3.3 Develop Non-Discriminatory Technical Requirements.***

Any technical requirements for devices beyond the existing GSM standards required to operate on a network will be purely functional and approved by third-party technical experts in a public forum. They will be public, transparent, and incorporated into an Any Device GSM certification process and testing by a third-party entity. It should be noted that few enhancements should be needed—T-Mobile reports that many “grey” devices, including devices obtained internationally and over one million unlocked iPhones, already operate on its network without causing harm.<sup>30</sup>

### ***2.3.3.4 Allow Non-Discriminatory Carrier Configurations and Updates***

Carriers may add carrier-specific configurations at the time of user activation and may also provide software and firmware updates to customer devices. These may include, but not be limited to, changes to allow devices to use new spectrum, updates in roaming profiles, and updates to software and operating systems. These should provide the same functionality to Any Device GSM customers as to customers with carrier-provided devices.

## **2.3.4 Evolution to Any Device in a CDMA Environment**

Implementing Any Device is more complex with CDMA technology, because the authentication of the device is not detachable from the device as it is with GSM. U.S. CDMA devices do not have a detachable subscriber identity module containing all carrier-specific information. Instead, the manufacturer has supplied the encryption key of the device with the device, and both the key and the device are the property of the carrier.

---

<sup>28</sup> T-Mobile. “Ask T-Mobile: SIM Cards and Unlocking your Phone.” Website. [http://search.t-mobile.com/inquirapp/ui.jsp?ui\\_mode=question&question\\_box=unlock](http://search.t-mobile.com/inquirapp/ui.jsp?ui_mode=question&question_box=unlock) (accessed January 4, 2010).

<sup>29</sup> ETSI. “TS 101 624 V7.0.0 (1999-08).” Technical Specification (1999). [http://pda.etsi.org/exchange/folder/ts\\_101624v070000p.pdf](http://pda.etsi.org/exchange/folder/ts_101624v070000p.pdf) (accessed January 11, 2010).

<sup>30</sup> T-Mobile engineering staff, in discussion with CTC, December 16, 2009.



















































