2007

In Pursuit of a Next Generation Network for Public Safety Communications

Philip J. Weiser
University of Colorado Law School

Dale N. Hatfield
Interdisciplinary Telecommunications Program, University of Colorado

IN PURSUIT OF A NEXT GENERATION NETWORK FOR PUBLIC SAFETY COMMUNICATIONS

Philip J. Weiser[†] and Dale N. Hatfield[‡]

I. INTRODUCTION

On April 11-12, 2007, in Washington, D.C., the University of Colorado Law School's Silicon Flatirons Program convened a roundtable on public safety communications ("Roundtable") to tackle the increasingly high-profile and often acrimonious issues surrounding the status of public safety communications in the United States. This Roundtable successfully brought together participants with affiliations spanning a variety of disparate stakeholders and highlighted a series of important issues for policymakers.[1]

Overall, the Roundtable discussion emphasized that technological changes and policy reforms can spur the development of a next generation network

[†] Phil Weiser is a Professor of Law and Telecommunications and Executive Director of the Silicon Flatirons Program at the University of Colorado. This Article results from a two day conference convened by the Silicon Flatirons Program to evaluate solutions for advancing the state of public safety communications. The perspective offered herein is that of the authors—who endeavored to glean insights from the discussion, identify points of rough consensus, and, in general, draw on the discussion from the conference from the standpoint of an informed observer. The authors alone are responsible for the views set forth herein and they should not be attributed to any of the participants in the conference. The authors acknowledge Jill Van Matre, who conducted critical background research and provided valuable feedback on the report, as well as Brad Bernthal, Harlin McEwen, Jon Peha and Bryan Tramont, who provided helpful comments and encouragement. Finally, the authors acknowledge a grant from CTIA—The Wireless Association®, which supported the Roundtable and relevant background research.

[‡] Dale Hatfield is an Adjunct Professor in the Interdisciplinary Telecommunications Program at the University of Colorado.

[1] Participants included leaders in the public safety community, wireless service providers, device manufacturers, engineers, and key scholars. Significantly, those participants are not responsible for the contents of this article, although the relevant participants have approved any statements attributed to them.

("NGN") for public safety communications.[2] Significantly, such a network would facilitate both greater levels of operability and interoperability between networks. Operability refers to the ability of communications systems to function effectively, reliably, and continuously. Interoperability refers to the ability of different first responders to communicate with one another in real-time, whether or not they are using different communications systems. Stated broadly, interoperability signifies "the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary . . . utilizing information technology systems and radio communications systems, and to exchange voice, data, or video with one another . . . in real time, as necessary."[3]

An NGN network will also enable public safety entities to utilize new technologies that will enhance their effectiveness. In particular, such a network will facilitate the adoption of new broadband and Internet-based technologies by public safety agencies. In developing and deploying this network, however, it is important to appreciate, as a number of Roundtable participants emphasized, that policymakers also need to address the immediate need of finding cost-effective solutions to enable interoperability across today's legacy public safety networks. To both promote an NGN as well as manage today's networks effectively, policymakers will need to develop a thoughtful strategic vision and use considerable leadership to put it into practice.

By adopting a new model for promoting public safety communications as part of the auction for 700 MHz spectrum and the assignment of a block of spectrum to a public safety broadband licensee, the Federal Communications Commission ("FCC") has taken an important step toward the development of a nationwide interoperable broadband communications network.[4] To advance

---

[2] As discussed below, the concept of a "next generation network" refers to the architecture used in modern commercial networks, which facilitates convergence—the delivery of video, data, and voice traffic over a single network—through the use of technologies based on the Internet Protocol ("IP").

[3] H.R. REP. NO. 108-796, at 213 (2004) (Conf. Rep.).

[4] *See In re* Service Rules for the 698-746, 747-762 and 777-792 MHz Bands; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Section 68.4(a) of the Commission's Rules Governing Hearing Aid-Compatible Telephones; Biennial Regulatory Review—Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services; Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission's Rules; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band; Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010; Declaratory Ruling on Reporting Requirement under Commission's Part 1 Anti-Collusion Rule, *Second Report and Order*, 22 F.C.C.R. 15,289 (July 31, 2007) [hereinafter Spectrum Auction Rules Order]; *see also In re* Implementing a

this policy effectively, policymakers will need to be realistic about the time and effort needed to implement a fundamental change in public safety communications—particularly under significant technical and financial constraints. Moreover, policymakers must recognize that no system will be perfect, meaning that they will need to make compromises between the ideal level of coverage, reliability, and financial constraints.

From a homeland security perspective, the current operability and interoperability limitations of public safety communications systems are detrimental to national and local emergency response capabilities and risk the lives of both first responders and ordinary citizens. Moreover, these weaknesses of current systems are a day-to-day reality for public safety agencies,[5] who continue to use equipment far less sophisticated than their corporate counterparts. Thus, until progress is made along a new policy direction, antiquated equipment and networks will continue to be used and first responders will continue to be limited by the shortcomings of today's public safety communications infrastructure.

This article reflects a unique combination of the authors' perspectives on an important public policy problem as well as the deliberations of the Roundtable. In general, it attempts to distill the analysis and suggestions presented during the Roundtable's discussion into a coherent description of the challenges facing public safety communications and the near- and long-term solutions for solving these challenges. Part II begins by providing a technological background, including an explanation of the evolution of modern public safety communications systems and their corresponding technological and operational limitations. It also addresses the technological requirements, architecture, and possible constraints associated with an NGN. Part III examines strategies for implementing a next generation architecture. It begins by describing the historical regulatory strategies and then proceeds to analyze possible policy strategies for an NGN, along with the associated challenges and opportunities. Part IV sets forth key concerns for the transition period, including working within the current technological framework, building a sustainable funding base, and establishing clear requirements and standards. Part V offers a short conclusion.

Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band; Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, *Ninth Notice of Proposed Rulemaking*, 21 F.C.C.R. 14,837, ¶¶ 3–4 (Dec. 20, 2006) [hereinafter Ninth NPRM] (noting the Commission's intent to maximize public safety via reserved broadband spectrum).

[5] *See* Jon M. Peha, *Improving Public Safety Communications*, ISSUES SCI. & TECH., Winter 2007, *available at* http://www.issues.org/23.2/peha.html.

II. TECHNOLOGICAL BACKGROUND

In order to fully appreciate the technological choices now facing public safety agencies, it is important to understand: (1) the evolution of public safety communications systems; (2) the technological and operational limitations of such systems; (3) the requirements and architecture associated with a public safety NGN; and (4) the essential considerations that will inform and, in some cases, constrain the development of an NGN designed to meet the needs of public safety in the coming decades. This Part discusses each in turn.

A. The Evolution of Modern Public Safety Communications Systems[6]

1. Technological History

Land Mobile Radio ("LMR") services date back almost a century. The Detroit Police Department engaged in one of the earliest uses of LMR, experimenting with a one-way (base-to-vehicle) system in 1921. These early voice systems used Amplitude Modulation ("AM") located just above the AM broadcast band in the Medium Frequency portion of the radio spectrum. The first license for a mobile transmitter was issued in 1932. Soon thereafter, the first Very High Frequency ("VHF") band came into use and, more recently, radios using the more effective Frequency Modulation ("FM") band were introduced. Over time, increased use of LMR systems by public and private entities led to the opening of another band higher in the VHF region. These two mobile radio bands in the 40 MHz and 150 MHz portion of the VHF range became known as Low Band and High Band respectively.

The early voice systems operating at both Low Band and High Band consisted essentially of a base station transmitter-receiver combination, an antenna tower and antenna, and the individual mobile transmitter-receiver units (transceivers). These early systems operated in the push-to-talk, release-to-listen mode and provided voice dispatch services using a single frequency for both transmitting and receiving. Because of an overall scarcity of frequencies, these channels were often shared with other networks or operators.

With the continuing growth in LMR services, the FCC allotted additional spectrum for public safety uses in the Ultra-High Frequency ("UHF") portion of the radio spectrum. The FCC allocated two frequencies for each channel of communications—one to transmit and one to receive. Providing a pair of fre-

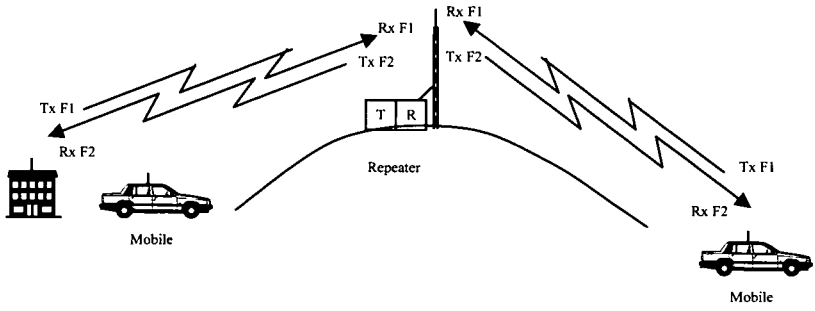
---

[6] Portions of Part II.A are drawn directly from Dale N. Hatfield, *The Technology Basis for Wireless Communications*, *in* THE EMERGING WORLD OF WIRELESS COMMUNICATIONS 49 (1996).

quencies created several advantages, including reduction of the interference between the higher power base stations and the typically much lower power mobile units. Most significantly from a public safety perspective, this architecture allowed for the introduction of repeaters, which can provide greatly increased geographic coverage, especially for mobile-to-mobile and portable-to-portable communications. In most cases, the repeater is installed on a very high tower, building, or mountaintop.

As illustrated in Figure 1, a repeater receives a low-power mobile, portable or base station signal on one frequency and retransmits it at high power on the second frequency of the pair. Due to its advantageous location, the repeater can normally receive and transmit over a wide area. The result is that two low-power mobile or portable units that are located only a few miles apart, but are unable to communicate, can now successfully communicate via the repeater because they are both within its line-of-sight. This arrangement facilitates the rapid voice call setup and group calling among and between a dispatcher and field units.

Figure 1: Conventional Repeater System



Use of conventional dispatch systems grew rapidly throughout the late 1960s, leading the FCC to again make available additional spectrum for public safety LMR systems.[7] In so doing, the FCC sought to encourage the development and deployment of systems that utilized the increasingly scarce radio spectrum on a more efficient basis.[8]

---

[7] *See In re* Amendment of Parts 2, 89, 91, and 93; Geographic Reallocation of UHF TV Channels 14 Through 20 to Land Mobile Radio Services for Use Within the 25 Largest Urbanized Areas of the United States; Petition Filed by the Telecommunications Committee of the National Association of Manufacturers to Permit Use of TV Channels 14 and 15 by Land Mobile Stations in the Los Angeles Area, *First Report and Order*, 23 F.C.C. 2d 325 (May 20, 1970).

[8] *See id.*

One way of improving spectrum efficiency was through the use of "trunking." In contrast to conventional systems, the individual channels in a trunked system are placed into a pool and made available to different groups of users on an on-demand basis. Specifically, a dispatcher or mobile unit desiring to make a call (or transmission) is given a channel to use for the duration of the call, and at the end of the call, the channel is returned to the pool for use by other users. With trunking, a call or transmission can be completed if any of the channels in the pool are idle and, conversely, a call is not blocked or queued unless all channels in the pool are busy.

Without trunking, each dispatcher (base) or mobile unit operates on a single channel that may be shared with other licensees. Thus, a dispatcher desiring to make a call cannot do so if that single channel is busy. In such an instance, the dispatcher cannot complete the call (it is blocked or queued) even though it is very likely that other single channels in the geographic area may be unused at that moment. Finally, users of an untrunked (conventional) single channel cannot make that channel available to users on other channels even if the untrunked channel is not being used.

Systems employing trunking are known as multi-channel trunked systems and one popular form utilizes what is known as centralized trunking.[9] With centralized trunking, status information (busy or idle) on each channel in the pool is maintained in a central controller and one channel from the pool is designated as a control channel. Idle dispatcher and mobile units monitor the control channel. If a unit initiates a call by pushing the push-to-talk button, it sends a signaling message on the control channel to the central controller identifying the called group and requesting a channel from the pool. The central controller identifies an idle channel and responds on the control channel with a signaling message that instructs the calling and called units to tune to the selected idle channel. Units that are not members of the called group continue to monitor the control channel. The conversation can begin when the calling and called units arrive on the selected channel. In a modern multi-channel trunked system, this entire process (the call setup time) occurs in less than one-half second.

Trunking can provide dramatic improvements in spectrum efficiency and performance (in terms of fewer blocked or delayed calls) and offers other important advantages as well, such as the sharing of channels so that individual channels are pooled rather than dedicated to a particular user. Thus, in the mid-1970s, when the FCC allocated additional spectrum in the 800 MHz band for

---

[9] *See generally* SAFECOM, COMPARISONS OF CONVENTIONAL AND TRUNKED SYSTEMS 9 (1999), *available at* http://www.safecomprogram.gov/NR/rdonlyres/F04A685D-5902-4655-BBBB-7251DCDF4693/0/Conventional_Trunked_Radio_Systems_Comparison_Report.pdf.

private LMR (including public safety entities), it authorized not only conventional, single-channel dispatch systems, but also multi-channel trunked systems.[10]

The use of sophisticated signaling and computer logic in the centralized controller of a modern multi-channel trunked system facilitates the inclusion of advanced features that are particularly important in public safety applications. If, for example, the number of calls is very heavy due to emergency conditions, higher-priority calls can be moved to the head of the queue and given the next channel that becomes available. Or, in the alternative, an existing lower-priority call can be preempted by a higher-priority call.

Perhaps the most important aspect to this improvement is that a multi-channel trunked system can provide effective interoperability among all dispatch and mobile units sharing the system. For example, if two jurisdictions have separate, conventional, single-channel systems, they may not be able to communicate with one another in times of emergency. Alternatively, the jurisdictions may be able to communicate only by employing gateways (cross-band repeaters) that require difficult coordination and are inefficient in terms of their use of the radio spectrum. In a multi-channel trunked system, each of the two jurisdictions would have its own separate talk-group or a "virtual network" that is defined in the software residing in the central controller. In times of emergency, units in the two jurisdictions can join pre-formed virtual networks that allow efficient communications between and among the units in both jurisdictions. Of course, such opportunities require ongoing cooperation (multi-agency agreements), such as that necessary to maintain shared access to different databases.[11]

In the early 1990s, the public safety community sought to take advantage of the opportunity to deploy modern multi-channel trunked systems by launching an effort to develop standards that would further facilitate interoperability. This effort evolved into the Project 25 Initiative ("P25"), which utilizes a standardized air interface and standardized signaling messages.[12]

---

[10] *In re* An Inquiry Relative to the Future Use of the Frequency Band 806-960 MHz; and Amendment of Parts 2, 18, 21, 73, 74, 89, 91, and 93 of the Rules Relative to Operations in the Land Mobile Service Between 806 and 906 MHz, *Second Report and Order*, 46 F.C.C. 2d 752, ¶¶ 16–17 (May 1, 1974).

[11] The degree of cooperation among agencies required and the complexity of the administrative issues involved (e.g., in keeping multiple databases operational and current) in these multi-agency agreements should not be underestimated.

[12] *See* Telecomms. Indus. Ass'n, *Project 25, Public Safety Communications Interoperability—Frequently Asked Questions Available on TIA Web Site,* PULSEONLINE, Oct. 2004, http://pulse.tiaonline.org/article.cfm?id=2057.

2. Relevant Regulatory Background

In 1995, the FCC, in concert with the National Telecommunications and Information Administration ("NTIA"), established the Public Safety Wireless Advisory Committee ("PSWAC") to assess the public safety communications needs through the year 2010. In 1996, the PSWAC released a report, which concluded that 97.5 MHz of new public safety spectrum would be needed by 2010, including 25 MHz by 2001.[13]

As a result of the PSWAC report, Congress directed the FCC to allocate 24 MHz of spectrum between 746 and 806 MHz to public safety agencies.[14] In particular, this spectrum will be recovered from television broadcast channels 60-69 as a result of the implementation of digital television ("DTV").[15] In its rules governing the uses of that spectrum, the FCC specified that UHF television channels 63, 64, 68, and 69 would be designated for public safety.[16] Moreover, the FCC concluded in 1998 that one-half of the new spectrum (12 MHz) would be made available for public safety narrowband voice channels and the remaining 12 MHz for wideband data channels.[17] Finally, to recommend rules for the use of the new 24 MHz of spectrum in the 700 MHz band, the FCC created the Public Safety National Coordinating Committee ("NCC").[18]

To date, the FCC's effort to accommodate the growth of private LMR systems has resulted in public safety allocations spread over five different bands. In particular, public safety agencies use spectrum in Low Band VHF, High Band VHF, UHF, 800 MHz, and 700 MHz.[19] Unfortunately, this fragmentation exacerbates interoperability problems and reduces the ability of vendors to achieve economies of scale. Moreover, there are differences in performance

---

[13] PUB. SAFETY WIRELESS ADVISORY COMM., FINAL REPORT OF THE PUBLIC SAFETY WIRELESS COMMITTEE 3 (1996), *available at* http://pswac.ntia.doc.gov/pubsafe/publications/PSWAC_Al.pdf.

[14] Balanced Budget Act of 1997, Pub. L. No. 105-33, 111 Stat. 251.

[15] *In re* Reallocation of Television Channels 60-69, the 746-806 MHz Band, *Report and Order*, 12 F.C.C.R. 22,953, ¶¶ 2–6 (Dec. 31, 1997).

[16] *Id.* ¶ 12.

[17] *In re* Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010; Establishment of Rules and Requirements for Priority Access Service, *First Report and Order and Third Notice of Proposed Rulemaking*, 14 F.C.C.R. 152, ¶ 43 (Aug. 6, 1998).

[18] *Id.* ¶ 7.

[19] The FCC recently allocated an additional 50 MHz of spectrum for public safety use in the 4.9 GHz band. *See In re* 4.9 GHz Band Transferred from Federal Government Use, *Memorandum Opinion and Order and Third Report and Order*, 18 F.C.C.R. 9152, ¶ 16 (Apr. 23, 2003). Based on the current technology, the 4.9 GHz band is unsuitable for highly mobile use and thus is not discussed herein.

among the bands because of radio propagation variations associated with the five bands. Consider, for example, that a jurisdiction in an urban area may prefer a modern digital multi-channel trunked system at 800 MHz when the need for maximum capacity is great and shorter ranges can be accommodated. By contrast, a jurisdiction in a rural area may prefer a High Band VHF analog conventional system because capacity is not a significant issue, but maximum coverage from a single site is of paramount importance.[20]

The FCC has traditionally licensed private land mobile radio systems, including those used by public safety, on a local, site-by-site basis.[21] While there may be important benefits associated with such a licensing scheme, it tends to exacerbate the fragmentation. In addition, conventional public safety channels are typically shared with other public safety users. Without the more disciplined approach to channel access provided by a trunked system, there are powerful incentives for local public safety agencies to acquire and retain their own channels, even if they are not heavily used. In the absence of a multi-channel trunked system serving multiple agencies or in the face of a refusal by an individual agency to join such a system (because a conventional analog system is more economical), opportunities for interoperability, greater spectrum efficiency, and larger economies of scale are lost.

In a further attempt to accommodate the growth in private land mobile radio use, the FCC has embarked upon a lengthy proceeding to create additional individual channels by decreasing the width of each voice channel from 25 kHz (the current width) to 12.5 kHz, and perhaps eventually to 6.25 kHz.[22] This channel splitting requirement applies to both public safety and industrial licensees in the popular VHF and UHF private land mobile radio bands.[23] Un-

---

[20] This is due to the fact that VHF signals travel further than 800 MHz signals in rural areas. However, there is more spectrum available at 800 MHz than VHF. Since rural areas do not need as much capacity as urban areas, it is possible to reduce the number of base stations because the signal will travel farther. Thus, VHF is optimal for rural areas. By contrast, greater capacity is needed in urban areas. These areas require more channels, more frequency reuse, and, ultimately, more base stations. Greater frequency reuse means that signals do not have to travel as far. Therefore, 800 MHz tends to be optimal in urban areas. Rural areas forced to use 800 MHz would require more base stations, and, ultimately, a significant increase in cost.

[21] *See generally* 47 C.F.R. pt. 90 (covering private land mobile radio services regulation and licensing).

[22] *See In re* Implementation of Sections 309(j) and 337 of the Communications Act of 1934 as Amended; Promotion of Spectrum Efficient Technologies on Certain Part 90 Frequencies, *Third Memorandum Opinion and Order, Third Further Notice of Proposed Rule Making and Order*, 19 F.C.C.R. 25,045, ¶ 2 (Dec. 20, 2004).

[23] The NTIA has adopted a similar requirement for federal government land mobile radio users. NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, UNDERSTANDING FCC NARROWBANDING REQUIREMENTS (2007), *available at* http://www.ncjrs.gov/pdffiles1/nij/217865.pdf.

fortunately, "[i]n an ironic twist of lagging policy, at the same time that users are trying to explain their need for wideband and broadband channels to the FCC, the most heavily used bands in operation are subject to narrowbanding."[24] Thus, the narrowband requirement, in the face of industry trends to move to wider channels (1.25 - 5.00 MHz), may actually further exacerbate interoperability problems and lead to further losses in terms of economies of scale.

3. Modern Dispatch Oriented Services for Data, Image, and Video

In addition to public safety voice- and dispatch-oriented wireless communications systems, there exist more advanced systems that are capable of handling data, image, and video traffic. Before advanced data and multimedia capabilities can play a critical role in public safety communications, however, agencies will need to adopt new systems while transitioning away from their old ones. Using today's narrowband (25 kHz) systems (with their low-speed two-way data communications capabilities), first responders can send brief, text-based inquiries regarding a vehicle or suspect directly to the National Crime Information Center or other databases maintained by state or local agencies. Such systems cannot provide, however, the broadband data capabilities of an NGN, which will enable high quality images (mug shots) and video clips (scenes from a natural disaster location) to be sent between and among public safety units.

Despite the potential benefits of advanced data communication features, speed and reliability in critical tactical situations (such as whether to shoot or not) remain of significant importance. Thus, while access to building plans and video coverage at a scene may be extremely useful, public safety officials cannot take the time to create and read data communications while pursuing a fleeing suspect, for example. In such situations, nothing can replace voice communications with rapid call setup and group calling. As such, these mission-critical capabilities must be maintained as part of public safety communications.

In short, rapid voice call setup and group calling is the *sine qua non* of modern public safety voice communications. For ordinary telephone (landline or wireless) conversations, by contrast, very rapid call setup is not an issue, as it may take tens of seconds for the called telephone to ring and to be answered. Because speed is an essential issue in mission-critical public safety operations,

---

[24] NANCY JESUALE & BERNARD C. EYDT, A POLICY PROPOSAL TO ENABLE COGNITIVE RADIO FOR PUBLIC SAFETY AND INDUSTRY IN THE LAND MOBILE RADIO BANDS 5 (Feb. 3, 2007), *available at* http://www.netcityengineering.com/PID354224.pdf.

modern systems achieve call setup times of one-half second or less. Moreover, unlike ordinary voice telephony, a dispatch system allows all members of a talk group to receive the transmissions from all other members of that talk-group.[25] In particular, calls to individual units and broadcast calls to all units are possible when using such a system.

Along with fast call setup times and group calling capability, modern dispatch systems also provide a number of other important functionalities. First, agencies may often need to set up multiple talk groups and to change group membership on a dynamic basis to reflect changing operational and tactical needs.[26] Second, another important capability of modern dispatch systems is a handset feature known as "talk-around," which enables two mobile or portable units to communicate directly with one another even in the absence of the network infrastructure.[27] This provides a limited form of failsafe capability in the event that centralized base station or trunking facilities are out of service, or if the two units are out of range of those facilities. The talk-around capability can also be used to off-load local communications from a heavily-loaded wide area system. Notably, ordinary wireless telephony services do not offer this capability as no direct, "infrastructureless," peer-to-peer communications are possible using such systems.

A third important feature of modern dispatch systems is that they allow call requests to be queued when all channels are busy. This is in contrast to the ordinary telephone network, which results in an "all trunks are busy" signal to the user. Because messages are typically much shorter in a multi-channel dispatch system, a channel is more likely to become available in a short time and there is thus less of a need to immediately return a busy signal. Moreover, the queuing and associated call processing used by modern dispatch networks can provide priority access (with multiple priority levels) and, in particularly critical situations, can allow the preemption of calls in progress. Indeed, more

---

[25] Note that group calling is possible in an ordinary voice telephony system by establishing a conference call through a conference bridge, but that it is not a substitute for the group calling utilized by public safety.

[26] With respect to talk groups, an additional feature called "late entry" allows a unit that has just been turned on, or is manually switched from one talk group to another, to join a conversation already in progress. That is, the late entry does not need to receive the original signaling message that was used to connect the talk group on a particular conversation channel.

[27] Talk-around functionality was an area stressed by many of the Roundtable participants. In particular, Vice Chair of the National Public Safety Telecommunications Council, Harlin McEwen, emphasized its importance, noting that the key issue of reliability should never be compromised to achieve economies of scale. Moreover, Stephen Meer, Co-Founder and CTO of Intrado Inc., made the point that although talk-around is used as a fallback mechanism in modern systems, capacity issues often preclude its effectiveness in emergency scenarios.

modern systems offer encryption of public safety communications to provide greater levels of privacy for sensitive communications.

Finally, to improve or tailor radio system coverage in a given geographic area, modern dispatch systems employ two additional techniques. First, modern systems are capable of operating in the "simulcast mode," in which an additional transmitter is placed in an area needing additional coverage. This additional transmitter simultaneously emits the same signal sent from the main transmitter and on the same band. Normally, such a transmitter would cause severe interference in the geographic area where the signals overlap. However, by carefully controlling the characteristics of the signals (in terms of carrier frequency and phase or timing), this interference can be minimized. Simulcasting requires that the main and simulcast sites be connected using a microwave radio link or leased fixed line, but it provides the benefit of allowing the transmitter or "talk-out" coverage to be optimized without requiring an additional frequency.

The second technique deals with the opposite issue—"talk-back" range. Because of their lower power (and associated battery-life issues) and less efficient antennas, the talk-back range of portable, handheld radios is sometimes less than the talk-out range of its associated base station. To compensate for this reduced range in critical areas, remote receivers are often employed in these places. These remote receivers are, in turn, connected back to the base station by a fixed link. When multiple remote receivers are employed, the signal from the remote receiver with the best reception of the signal from the portable is selected. In this situation, the remote receivers are referred to as "voting receivers." In combination, simulcasting and remote receivers often overcome coverage gaps in critical areas.

B. Limitations of Modern Public Safety Systems

As discussed above, early generations of public safety networks focused on voice communications, used conventional (i.e., non-trunked) single channel repeaters, used push-to-talk access, and worked in the narrowband, analog transmission mode. By contrast, later generations continued to focus on voice communications, used trunked repeaters, used push-to-talk access, and worked with digital signaling, but continued to use narrowband, analog transmission for the conversation channels. The current generation of public safety systems (i.e., P25) still focuses on voice communications, but provides circuit switched and packet switched data access that is limited in data rate by the narrowband channels employed. In an advance over their predecessors, they use trunked repeaters with push-to-talk voice access and employ all-digital transmission in narrowband channels. Table 1 depicts the differing attributes of these systems.

Table 1: Technology of Public Safety Networks Over Time

	Early Generation Public Safety Network	*Later Generation Public Safety Network*	*Current State of Art Public Safety Network*
Type of communications emphasized?	Voice communications	Voice communications	Voice communications with some data
Conventional vs. trunked architecture?	Conventional single channel repeaters	Trunked repeaters	Trunked repeaters
Access method?	Push-to-talk access	Push-to-talk access	Push-to-talk access
Analog vs. digital transmission?	Analog transmission	Analog transmission (but with digital signaling)	All digital transmission
Narrowband vs. broadband?	Narrowband	Narrowband	Narrowband

In contrast to the commercial cellular market, the market for state-of-the-art public safety communications equipment (i.e., P25 systems) is much smaller, more concentrated, and less competitive. Notably, public safety systems are designed to provide maximum coverage from each site, thus facilitating simultaneous communications with individual talk-group users spread over a wide area. In engineering terms, these are referred to as "noise limited systems" and the large coverage areas they produce minimize the number of base stations required to communicate with widely dispersed units, thereby reducing the associated fixed infrastructure costs.

Commercial cellular systems have evolved over three generations.[28] First generation systems were voice-oriented, used analog transmission in narrowband (30 kHz channels), and employed circuit switching. In the United States, this generation was exemplified by the Advanced Mobile Phone System standard.[29] Second generation systems were also voice oriented, but offered some data capabilities; they were all digital, but still employed circuit switching. Examples of such systems included GSM, CDMA, iDEN, and, in the United States, TDMA. In contrast, third generation systems can seamlessly handle

[28] *See generally* ANDREA GOLDSMITH, WIRELESS COMMUNICATIONS 11–13 (2005).

[29] JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 277 (2005).

voice, data, image, and video traffic, employ packet-oriented switching, and operate in wideband channels (1.25 MHz), allowing high data rate transmissions roughly comparable to the speeds achievable by early generation wireline DSL and cable modem services. Examples of these systems include WCDMA and CDMA 2000. Moreover, because of the highly competitive environment, the availability of wider channels, and the large manufacturing volumes associated with these systems, the capabilities of such systems continue to increase. In particular, the handsets associated with these systems continue to evolve, supporting not only voice, but also data, image, and video or multimedia applications.

The contrast between the third generation cellular systems and the third generation public safety systems highlights the opportunities for improving the latter. To be sure, the current (and third) generation of public safety systems (P25) does a laudable job of meeting the requirements of rapid voice call setup and group calling among geographically dispersed users. However, aspects of its technical architecture—including the use of narrowband channels—essentially preclude such systems from evolving into broadband networks. This means that systems premised on P25 technology are not capable of evolving so that they can seamlessly handle voice, data, image, and video traffic on a common platform (as is happening in the commercial cellular environment). Certainly, public safety organizations recognize the pressing need for such broadband capabilities, but they have yet to develop a strategy for modernizing their current platforms.[30]

While not a technical limitation *per se*, the market for specialized multichannel trunked systems is itself limited by the small size of the public safety market and by the relatively small purchases made by individual agencies at any given time. This, in turn, limits economies of scale and reduces competitive pressures because fewer suppliers can be supported. Reflecting the advantages of the commercial cellular equipment ecosystem, "a cell phone with voice, video, and data capability costs about seven times less than a public safety digital portable radio that cannot even take a digital photo, much less send it to another person."[31]

---

[30] *Hearing on Oversight of the Nat'l Telecomm. Info. Admin. and Innovations in Interoperability Before the Subcomm. On Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong. (2007) (written testimony of Harlin R. McEwen, Chairman, Commc'ns & Tech. Comm., Int'l Ass'n of Chiefs of Police) [hereinafter Testimony of Harlin R. McEwen], *available at* http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.032207.McEwen-testimony.pdf.

[31] Robert Rouleau, *Connecting Data Networks*, MISSION CRITICAL COMM., Aug. 2006, at 98, 102.

Because the public safety communications infrastructure is premised on the use of narrowband channels and specialized multi-channel trunked systems, the public safety community cannot directly adopt the commercial cellular technology into the existing public safety bands. As a result, the public safety community cannot benefit from economies of scale, competition among vendors, and research and development expenditures associated with the commercial cellular marketplace. Consequently, as one observer noted:

> [T]he public safety user community is two orders of magnitude smaller than the commercial user base. As a result, R&D investments in commercial wireless technologies dwarf those made in public safety wireless technologies. In addition, the large size of the commercial wireless market fosters greater levels of competition between vendors of network infrastructure, user devices, and applications.[32]

According to a recent article, a substantial fraction of all public safety systems still use the same narrowband, analog FM, conventional (untrunked) systems in the VHF and UHF bands that have existed for decades.[33] In contrast to users of P25 infrastructure, public safety users of conventional, analog FM systems are able to take advantage of a competitive market that reflects a broad array of users for such equipment, including both domestic and international suppliers working to serve the industrial, transport, maritime, government, and amateur venues. The resulting lower prices, coupled with the propagation advantages associated with the VHF and UHF bands, greatly reduce the incentives for public safety agencies (especially outside the larger urban areas) to deploy modern multi-channel trunked systems, thereby aggravating interoperability problems.

The interoperability limitations of public safety infrastructure stem from three principal factors. First, as noted above, the use of different technologies at the state, local, and federal levels of government, ranging from legacy FM conventional systems to proprietary analog and digital multi-channel trunked systems to modern standardized P25 digital multi-channel trunked systems, make interoperability between networks difficult to achieve. Second, as discussed above, the historical developments that led to public safety systems being licensed in five separate spectrum bands spanning a range from 25 MHz to 866 MHz also complicate any interoperability solution. Finally, the long-standing policy of licensing public safety radio systems on a local level (indeed, on a channel-by-channel, site-by-site basis) creates a tradition of local autonomy and sometimes raises barriers to cooperation.

---

[32] Krishna Balachandran et al., *Mobile Responder Communication Networks for Public Safety*, IEEE COMM. MAG., Jan. 2006, at 56.

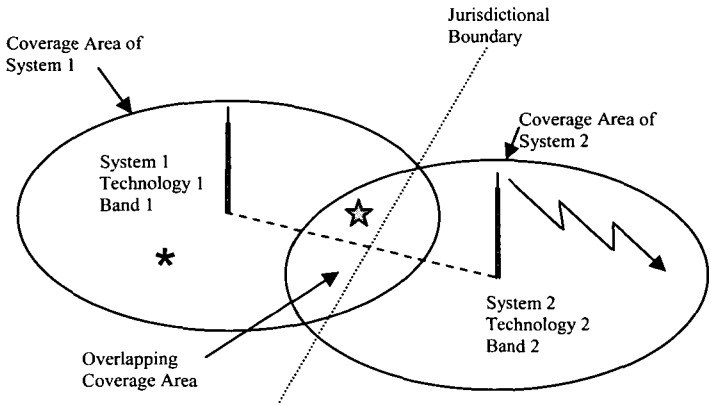
[33] JESUALE & EYDT, *supra* note 24, at 3.

1. Interoperability Solutions

The lack of interoperability between public safety communications systems became a national tragedy on 9/11 when first responders were not able to communicate with one another. Responding to this failing, policymakers have pushed a variety of proposals. In reviewing the possible options, it is useful to distinguish between three parts of a telecommunications network—(1) the end-user devices; (2) the local access portion of the network; and (3) the wide area or core portion of the network—because solutions can be implemented at any of these points.

In a traditional commercial cellular network, the end-user devices are ordinary cell phones; the access portion of the network includes the base stations and microwave or other links for connecting the base stations to the Mobile Switching Center ("MSC"); and the wide area portion of the network includes the facilities used to interconnect the MSCs to each other and to the public switched telephone network. In a modern P25 public safety system, the end-user devices are mobile and portable radios built to the P25 standard; the access network includes the P25 base stations plus microwave or other links (telephone company provided leased lines) to connect the base stations to the centralized P25 switch controller. In addition, if it is a network covering a large geographic area, the wide area portion includes the facilities for interconnecting multiple switch controller nodes.

Figure 2: Interoperability Solutions[34]



[34] Figure 2 is adapted from a slide in a presentation entitled "Interoperability, Public Safety and Homeland Security" by Steve Sharkey, Director of Spectrum and Standards Strategy at Motorola, presented at the Law Seminars International Conference on Spectrum Rights and Management, Washington, D.C., Sept. 19, 2006.

Figure 2 provides one perspective on available interoperability solutions. The circle on the left represents the coverage area of Public Safety System 1, which is operating in band 1 and using access technology 1. For example, Public Safety System 1 could be operating a multi-channel, P25 trunked system digital access network in the 800 MHz band. The circle on the right depicts the coverage area of Public Safety System 2, which is operating in band 2 and using access technology 2. This system could be operating in the UHF (450 MHz) band using conventional analog FM repeaters as the access technology. (Note that there is some overlap between the two systems.)

To appreciate the nature of the interoperability issue, consider what options there are in the event of a large emergency at a location within the overlapping coverage area (marked with a star in Figure 2). For the sake of the example, assume that the incident is within the jurisdiction of the agency operating Public Safety System 1, but it is of such a nature that it requires assistance from mobile units in Public Safety System 2. Consequently, a successful response to the event will require that the end-user devices used in Public Safety System 2 communicate with the end-user devices used in Public Safety System 1.

Conceptually, interoperability between Public Safety System 1 and Public Safety System 2 can be achieved in three different ways: end-user device solutions, access network solutions, and network-based solutions. First, the arriving mobile unit from Public Safety System 2 could utilize a multi-band, multi-mode radio (or a software defined radio equivalent) capable of operating on the access network of Public Safety System 1. This exemplifies an end-user device solution. Such solutions are still developing and, at present, are not used to any substantial degree because of their higher cost, greater weight, and lower battery life. Moreover, the complexity of such solutions increases dramatically as the number of modes and bands increase.

Second, although difficult in practice, the access network in Public Safety System 1 could be reconfigured (using software defined radio technology, for example) to work with the end-user device from Public Safety System 2 without any changes to that end-user device (except perhaps for a change in channels within band 2). This solution, even if not practicable using today's technology, represents an access network solution.

Third, in this area of overlapping coverage, Public Safety System 1 units are able to maintain contact with their switch controller and Public Safety System 2 units are likewise able to maintain contact with their switch controller. As a result, the wide area or core network connection between the two switch controller nodes (shown as a dotted line in Figure 2) could be used with certain functionality within the two nodes to interconnect or provide a "gateway" between the two systems. This is an example of a network-based solution. If the

two switch controllers use a common standard (e.g., P25), such interconnection is relatively straightforward.

In evaluating the appeal of a gateway solution, it is important to realize that it, too, has a notable limitation. In particular, it is important to note that while gateway solutions allow conversations on a channel in one system to be heard on a channel in a second system and *vice versa*, such a solution requires two channels to be effective—one on each system. If the traffic is relatively light on the combined channels, spectrum is wasted because a single channel could otherwise handle all of the traffic. But where the traffic on the combined channels is heavy, overload and unsatisfactory performance may occur when the two channels are bridged. In short, gateways in general are not always spectrum efficient and, unless other steps are taken, the use of gateway solutions may decrease performance under heavy traffic loads.

The analysis of the appropriate interoperability solution changes if the emergency occurs is inside the coverage area of Public Safety System 1, but outside the coverage area of Public Safety System 2 (marked with an asterisk in Figure 2). The first two types of solutions—the end-user device solution and the access network solution—would still work to provide interoperability. The network-based solutions, by contrast, would not work because the mobile units associated with Public Safety System 2 are out of the range of their switch controller. In some emergency situations, however, a local, temporary repeater that is compatible with the mobile units associated with Public Safety System 2 can be located in the vicinity of the incident. If such a repeater could be installed, the gateway solution could then be used to bridge the channels together to provide temporary interoperability.[35]

The above discussion highlights why the lack of interoperability of today's public safety systems is not easily rectified. To be sure, narrowband interoperability issues for local first responder personnel would be minimized if every public safety agency used a P25 system operating in the 700 MHz or 800 MHz band. Such a strategy would reduce the complexity of achieving interoperability, even if the P25 systems operated in different bands, because it would facilitate the core network-based gateway solution. Indeed, this is the dominant strategy now being used by many states, which are seeking to deploy state-

[35] Interoperability problems between two jurisdictions can be minimized by increasing the amount of coverage overlap between the two systems. Indeed, under existing conditions, there are incentives for different agencies to create overlapping coverage to facilitate interoperability in situations requiring mutual aid. However, extending coverage in this way, for the sole purpose of facilitating interoperability in emergencies, can be spectrum inefficient because it reduces the amount of frequency reuse that can be obtained in public safety spectrum allocations and allotments. *See* Jon M. Peha, *How America's Fragmented Approach to Public Safety Wastes Money and Spectrum*, 31 TELECOMM. POL'Y 605 (2007).

wide, multi-channel trunked systems that address interoperability and reduce the reliance on fragmented, localized systems. Such a strategy comes at a high cost, however, as the P25 narrowband technology cannot support broadband applications and prevents public safety agencies from leveraging commercial broadband developments.

The principal short-term alternative to the use of P25 systems is a reliance on gateway or network-based solutions. These solutions, while appealing as strategies to solve interoperability problems at a lower cost than the P25 model, have drawbacks and are thus not an efficient or effective long-term solution. These drawbacks include: (1) spectrum inefficiency—taking two or more channels when one would do; (2) the possibility of a decrease in voice quality in translating from one technology or standard to another; and (3) the requirement that both sets of mobile units have access to their respective systems—which may not always be the case, especially in rural and remote areas. In such a situation—in which the mobile units are outside of their coverage range—the talk-around function becomes essential. If unavailable, a repeater or mobile satellite system may need to be employed, which could be achieved through a multi-function, multi-band, end-user device.

C. Requirements and Other Ingredients for a Next Generation Public Safety Network

1. A High Level View

Telecommunications networks worldwide are evolving toward a converged, broadband, Internet Protocol ("IP")-based network-of-networks model. This NGN architecture envisions the development and deployment of networks that are capable of supporting voice, data, image, and video applications (including multimedia services) over individual or multiple types of infrastructures.[36] In essence, an NGN for public safety is envisioned as part of this evolution.

Under an NGN perspective, the future of public safety networks would be IP-based. In particular, the IP layer of the IP protocol suite defines the manner in which a packet of information is organized and structured and then routed on a packet-switched basis over various transmission media. A packet of information is a collection of bits including voice, data, image, or video content.

---

[36] *See* TIA TECHNICAL COMMITTEE, NEXT-GENERATION NETWORKS FOCUS GROUP, CONVERGING NGN TECHNICAL FRAMEWORK—TIA PRINCIPLES AND ISSUES 1–3 (2006), *available at* http://docbox.etsi.org/workshop/gsc11/GSC11_GTSC4/gsc11_gtsc4_31%20TIA%20TCNG NFG%20Technical%20Framework_Principles%20and%20Issues.doc.

By way of analogy, a packet of information can be viewed as akin to the standardized shipping containers used in the transportation industry. A standardized container facilitates the shipping and handling of a wide range of goods such as television sets, clothing, and industrial goods on a wide range of transportation infrastructure platforms, including ships, barges, railroad flatcars, and trucks. Similarly, an IP packet can handle the whole range of information types on a wide range of transmission media, including copper wire, fiber optic cable, or wireless.

To appreciate the power of IP-based technology, consider how it supports the transmission of a typical emergency message. In such a network, any standardized packet of voice content can originate in an officer's handset, travel over a wireless access network connection and a core network connection (over an optical fiber cable), reach a wired access network (copper or fiber), and connect to a console used by a public safety dispatcher. For systems or devices that are not IP-based, gateways can be provided that take the end-user information content (and associated signaling messages on the non-IP side) and convert them to ensure compatibility with the IP-based network on the other side and *vice versa*. To continue the transportation analogy, this would be similar to unpacking a container of television sets and specially repacking them for transportation in an aircraft incapable of handling the standardized container.

While an IP-based network can efficiently support traffic of varying urgencies and importance, the system must be designed to prioritize and manage the traffic accordingly. This is necessary to ensure that, in the case of mission-critical public safety voice communications, the packets of signaling information and content are delivered in a reliable and timely way, whether the underlying platform is operated on a private or commercial basis. The technical approaches to achieve this are known, although they are not available in all of today's off-the-shelf IP-based products.

2. Specific Public Safety Requirements and Associated Principles

There are two basic scenarios under which the public safety mission-critical voice communications needs could be met in the future. In the first scenario, mission-critical voice communications (and low-speed data services) would be maintained on traditional multi-channel trunked systems optimized for such communications (e.g., P25 systems) while the next generation, common user broadband network would be used to meet advanced broadband data, image, and video communications requirements. In the other scenario, the mission-critical voice communications traffic would be carried on the converged public safety NGN along with the advanced data services, once that network proved

that it could meet voice-dispatch requirements. Of the two options, the preferable one is to carry voice, data, image, and video traffic on a fully converged network because economies of scale can be captured, spectrum efficiency improved, and the need for gateways reduced. Thus, requirements for public safety's mission-critical voice communications must be included in the initial specifications for the public safety NGN. These needs include the rapid call setup and group calling capabilities representative of modern narrowband public safety systems, as well as the other features including multiple talk-groups, talk-around capabilities, multi-level priority access, preemption, and end-to-end encryption for privacy and security.

Beyond the traditional voice dispatch requirements, a public safety NGN system must support a wide range of "data services" (i.e., applications). Such services would include support for real-time voice connections to the public switched telephone network, e-mail and text messaging, high resolution still image and streaming video transmission, Internet/Intranet access to databases, and telemetry transmissions. During the Roundtable discussions, however, participants noted that certain bandwidth-intensive applications, such as streaming video from fixed locations could be off-loaded to other networks, including broadband networks operating in the 4.9 GHz public safety band or other commercial networks.

Out of practical necessity, existing public safety narrowband systems will need to remain in place as critical components of the public safety communications infrastructure for decades to come. Nonetheless, the core of the NGN public safety system, coupled with appropriate gateways, can and should be used to achieve interoperability between the dispatch and other narrowband services provided on the access networks associated with the new NGN system and the dispatch and narrowband data services provided on legacy (e.g., P25) systems. Indeed, IP-based solutions for facilitating interoperability are already being offered by vendors such as Cisco, Twisted Pair, and CoCo Communications. These solutions have already demonstrated, in deployments such as the one in Dallas's Love Field, that they can enable interoperability in a relatively inexpensive fashion.[37]

As the Roundtable participants emphasized, an NGN for public safety could allow local agencies to create virtual networks within the larger physical network. In particular, a local jurisdiction could establish its own talk groups and operate what would otherwise appear as a separate private network during non-emergency times, while seamlessly interoperating with other, larger groups of users in emergency situations. Importantly, this would provide diverse agen-

[37] *See* Jim McKay, *Instant Interoperability*, GOV'T TECH., Jan. 19, 2007, *available* at http://www.govtech.com/gt/articles/103426.

cies with much of the local control that has historically been associated with the less interoperable and less spectrum-efficient dedicated private systems.

On all accounts, rights management technologies are a critical component in the operation and management of an NGN for public safety. Rights management in this context involves, for example, determining who can be assigned to a particular talk group in a particular situation, who makes that decision, and how it is accomplished technically. Similar questions arise in determining who is permitted to place "offnet" calls through the ordinary telephone network (i.e., the Public Switched Telephone Network or "PSTN"), whose calls have priority, and who can preempt calls already in progress.

In terms of the broad principles to guide the development of an NGN for public safety, Roundtable participants discussed a series of key issues. In particular, they emphasized the importance of reliability, security, openness, modularity, extensibility, and reliance on commercial, broadly supported standards. While the importance of the first two (reliability and security) is self-evident in the public safety environment, the latter four (openness, modularity, extensibility, and reliance on commercial standards) deserve some elaboration.

Openness refers to standards that are available for use by all and freely available without undue restrictions on their use. Modularity refers to the decomposition of complex hardware or software systems into smaller subsystems that interact with each other through well-defined interfaces. Modularity (or layering, in the protocol sense) coupled with open, standardized interfaces ensures the potential of continued innovation because it facilitates the introduction of new technologies, and allows new applications to develop and deploy without disturbing other subsystems.

Extensibility refers to the ability of a system or subsystem to be extended or customized to provide new capabilities. An example of a system that is not extensible is one that does not scale well—that is, its performance in some important dimension decreases if new functionality is added. Because of rapid changes in technology and the increasingly complex demands placed upon public safety agencies, these goals of openness, modularity, and extensibility are particularly important.

Finally, given the probability of continuing budgetary constraints at all levels of government and the considerable resources currently devoted by the private sector to the development of commercial wireless networks, it behooves public safety agencies to rely, wherever possible, on broadly supported commercial standards—provided they satisfy essential requirements such as security and reliability considerations.

D. Essential Considerations in the Development of the Next Generation Public Safety Network

During the Roundtable, the participants raised a number of practical considerations that will impact the deployment of an NGN for public safety. These practical considerations include four central points: (1) the network's available coverage; (2) the network's capacity; (3) the network's cost; and (4) the need to interconnect the network with other networks.[38]

As a practical matter, wireless communications networks by their very nature will always suffer from some gaps in coverage. Reliable radio coverage in an urban area can be extended through a variety of specialized techniques such as bi-directional amplifiers, pico-cells, and distributed antenna systems into many buildings. But at some point, cost constraints prevent coverage from being extended into very remote locations such as the third sub-basement of a major bank building. As many Roundtable participants noted, unless new methods for providing indoor coverage emerge, requiring ubiquitous indoor coverage could significantly increase the cost of a network. Moreover, despite the costs, it may still be impossible to gain the necessary access to private property to extend coverage or to test coverage, even if it is externally provided to the building.

Another significant limitation is the impracticability of extending coverage to geographically remote areas using a terrestrial network. Even though mobile satellites can provide coverage to such areas, that coverage does not extend to places where satellites are invisible (in a radio sense). Stated another way, obtaining the last few percentage points of geographic coverage becomes prohibitively expensive in any radio-based system designed to cover a wide geographic area. Combining this consideration with the highly variable nature of radio propagation necessitates a great care in contractually specifying coverage requirements over a large geographic area. Consequently, some local tailoring of coverage will always be required to ensure that reliable coverage of particularly critical locations is provided.

As a practical matter, it is likewise impossible to build a physical or virtual public safety network with sufficient capacity to handle all communications needs—both essential and non-essential—in all locations during a major crisis. As in the case of radio coverage, reducing the blocking probability (or waiting time in a system where calls are queued) associated with gaining access to a radio channel to extremely low values under extreme load conditions becomes

[38] These principal considerations assume, as a basic precondition, that the relevant network is built to meet public safety's essential requirements, including rapid call set-up time, group calling, hardened infrastructure, and back-up power.

prohibitively expensive. As such, priority schemes, load sharing arrangements, and methods of eliminating non-essential traffic (when the network is in high demand) represent crucial components of any NGN public safety system. Participants noted that in cases of both coverage and capacity, emergency performance can be enhanced if the end-user device is capable of accessing more than one network. For example, a multi-mode, multi-band handset could first try a local P25 public safety network, then a terrestrial commercial broadband network, and finally a nationwide mobile satellite network in order to complete a voice call.[39]

Finally, practical necessity concerns dictate that a public safety NGN must be able to interconnect with other networks both routinely and in times of crisis. At a basic level, a public safety NGN must interconnect with the ordinary PSTN to allow, for example, an official with access to an ordinary telephone to communicate with public safety personnel at the scene of an emergency. At a more advanced level, it must also interconnect with a private LMR system utilized by, for example, an electric power utility with personnel attempting to restore critical infrastructure facilities at the scene of an emergency. The Roundtable participants noted that the trend of networks to migrate toward use of the IP suite of protocols should further facilitate such interconnection.

III. POLICY STRATEGIES FOR A NEXT GENERATION NETWORK

During the Roundtable, the participants emphasized that emerging technologies, particularly those facilitated by IP-based broadband networks, can provide all emergency responders with effective and interoperable access to information and communications. The participants also highlighted that a major reorientation of government policy, as well as a fundamental paradigm shift in public safety's approach to their communications needs, will be necessary to facilitate a transition to this next generation architecture. This Part begins by discussing the traditional policy approach and then evaluates strategies to migrate toward an NGN for public safety.

A. The Traditional Policy Paradigm

Only twenty-five years ago, the primary users of wireless LMR technology were public safety agencies and those who used dispatch networks. At that

---

[39] J. Brad Bernthal, Timothy X Brown, Dale N. Hatfield, Douglas C. Sicker, Peter A. Tenhula & Philip J. Weiser, *Trends and Precedents Favoring a Regulatory Embrace of Smart Radio Technologies*, *in* IEEE INT'L SYMP. ON NEW FRONTIERS IN DYNAMIC SPECTRUM ACCESS NETWORKS 9–10 (2007).

time, it was difficult to imagine the emergence of widely adopted wireless telephone service, never mind wireless broadband access. Indeed, at the time of the 1984 AT&T divestiture that broke up the Bell System, AT&T's CEO indicated little to no interest in keeping the newly issued licenses to provide commercial mobile radio service.[40] After all, AT&T's McKinsey and Company-commissioned study indicated that only one million subscribers would adopt wireless services by 2000.[41] Ultimately, this judgment was only off by a factor of one hundred.[42]

The FCC's paradigm for issuing licenses to operate wireless networks for public safety agencies focused on particular local agencies. In the 1980s, it was accepted wisdom that such networks should be operated on a local basis. Even commercial wireless services were viewed as local-based services and licenses were issued to local firms. Over time, however, the logic supporting local autonomy of network infrastructure deteriorated. Because the local networks were often assembled using very expensive and proprietary equipment (on account of limited economies of scale), they are often unable to interoperate with one another.

Policymakers generally provided local agencies with unconstrained autonomy to use their spectrum licenses to operate local networks as they saw fit. Indeed, until a recent proceeding governing spectrum dedicated to public safety in the 700 MHz band,[43] the conventional wisdom was to dedicate all blocks of spectrum for public safety to local agencies, with limited interagency cooperation requirements.[44] Similarly, grants to achieve interoperability goals are often provided directly to local agencies, assuming that such agencies would find strategies for cooperating effectively with one another.

Given the traditional paradigm's focus on local networks, spectrum assignments were generally made on a more *ad hoc* basis, with little focus on facilitating an NGN architecture. For example, public safety agencies received assignments in local VHF and UHF bands, in the 700 and 800 MHz bands and in the 4.9 GHz band with little or no concern with whether such assignments fa-

---

[40] Christopher Rhoads, *AT&T Inventions Fueled Tech Boom, And Its Own Fall*, WALL ST. J., Feb. 2, 2005, at A1.

[41] *Id.*

[42] *Id.*

[43] *See* Ninth NPRM *supra* note 4, ¶ 38 (allowing public safety personnel to communicate on twelve megahertz in the 700 MHz band).

[44] The limited requirements were imposed by the frequency coordinators and Regional Planning Committees. The Roundtable participants suggested that, while some such entities were effective in spurring cooperation (including on interoperability issues), the great majority of them have a mixed record of promoting cooperation and interoperability as opposed to simply managing concerns related to spectrum interference (which is their core mandate).

cilitated or frustrated interoperability or the ability to migrate to advanced networks. This strategy, while borne of decisions made over decades and the technological realities of an early era, still hampers the ability of public safety agencies to develop an NGN architecture and leads to networks that are inherently inefficient (as Carnegie Mellon Professor Jon Peha has emphasized).[45]

The nature of public safety's spectrum assignments makes the transition to an NGN quite challenging. First of all, some of the assignments (particularly those from the extreme bands) have propagation characteristics that limit their utility. Second, the spectrum dedicated to public safety agencies is not contiguous,[46] making it more difficult to support broadband communications. In particular, it is not merely the lack of contiguity that is incompatible with wide-area, broadband networks, but also the fact that channel assignments are "channelized"[47] into narrow blocks. Finally, the traditional model's require-

---

[45] In particular, Professor Peha identifies key ways in which fragmented spectrum assignments result in the inefficient use of spectrum and funding. First, municipalities license spectrum beyond their coverage areas, foreclosing the use of that spectrum by other public safety agencies. As a consequence, some portion of this reserved spectrum then sits idle. Second, infrastructure must be in place to serve an entire area, regardless of the number of first responders. Thus, deploying a few large systems is more efficient than deploying many small systems. Third, spectrum assignment is limited to distinct channels. As a result, spectrum sits idle when agencies with limited needs are assigned a full channel. Fourth, when agencies do not share spectrum, they must be assigned a sufficient number of channels to ensure that they have enough spectrum even during busy times. Spectrum sharing, on the other hand, means that if one agency is particularly busy, users can switch to another channel. Finally, patching is an inefficient use of spectrum in that it consumes twice the bandwidth to create one communications channel. Peha, *supra* note 35. Similarly, as George Rittenhouse, a vice president at Alcatel-Lucent, explained in his testimony to the House of Representatives:

> Most notably, fragmented use of public safety spectrum and a patchwork of incompatible systems has restrained the development of interoperable communications across geographic regions and among various agencies. Further, it has resulted in inefficient use of spectrum. Accordingly, a shift to public safety networks shared across jurisdictions is necessary to promote interoperability.

Hearing on Oversight of the Nat'l Telecomm. Info. Admin. and Innovations in Interoperability Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce, 110th Cong. (2007) (testimony of George Rittenhouse, Vice President of Tech, Integration for Bell Labs at Alcatel-Lucent), *available at* http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.032207.Rittenhouse-testimony.pdf.

[46] Testimony of Harlin R. McEwen, *supra* note 30, at 5 ("Historically, the FCC has allocated individual channels, not contiguous channel blocks, for public safety use. These channels are immediately adjacent to channels allocated for taxicab companies, truck operators, and other businesses. The channels typically are no larger than 25 kHz bandwidth and more frequently 12.5 kHz . . . .").

[47] The term "channelized" refers to the fact that the FCC has adopted rules requiring the use of specific channels based on particular technologies as opposed to allowing the spectrum licensee to determine how to use the spectrum.

ment of narrowbanding is increasingly problematic in an era in which all communications services are moving to broadband networks.

From today's vantage point, it is clear that the legacy policy towards public safety communications will not facilitate the development of an NGN and thus a new policy strategy is appropriate. To its credit, the FCC has investigated and begun to act on options for using the digital television transition to spur broader cooperation between public safety agencies.[48] Additionally, federal grants, such as those provided by the NTIA and the Department of Homeland Security ("DHS"), are now conditioned upon the development of a statewide interoperability plan and the establishment of a statewide executive interoperability council.[49]

To date, neither FCC decisions nor the DHS grants have galvanized strategic planning at the regional or state levels to the degree necessary to transform the culture of public safety communications.[50] Moreover, a substantial risk remains that the next round of grants will similarly fail to spur essential strategic cooperation unless there is some requirement built into the system for the evaluation and dispersal of funds to ensure how they are going to be used.[51] Indeed, as the Government Accountability Office ("GAO") concluded, "although DHS has required states to implement statewide plans by the end of 2007, no process has been established for ensuring that states' grant requests are consistent with their statewide plans."[52]

---

[48] Ninth NPRM, *supra* note 4, ¶ 2.

[49] U.S. GOV'T ACCOUNTABILITY OFFICE, FIRST RESPONDERS: MUCH WORK REMAINS TO IMPROVE COMMUNICATIONS INTEROPERABILITY 2–3 (2007) [hereinafter GAO INTEROPERABILITY REPORT], *available at* http://www.gao.gov/new.items/d07301.pdf.

[50] Addressing this very issue, the United States Government Accountability Office concluded that, despite the award of over $2 billion in grants from 2003 to 2005, "strategic planning has generally not been used to guide investments and provide assistance to improve communications interoperability on a broader level." *Id.* at 3. As to its finding with regard to specific states, it is clear the funds dispersed to date have not galvanized states to play an oversight role. Consider, for example, Kentucky where the "[g]rant reviewers at the state level who are in charge of disbursing DHS grant money to localities have had limited means for determining whether funding requests for equipment and training were compatible with statewide interoperability goals." *Id.* at 21.

[51] *Hearing on Oversight of the Nat'l Telecomm. Info. Admin. and Innovations in Interoperability Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong. (2007) (prepared statement of Stephen T. Devine, Chief, Mo. State Highway Patrol) [hereinafter Statement of Stephen T. Devine], *available at* http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.032207.Devine-testimony.pdf.

[52] GAO INTEROPERABILITY REPORT, *supra* note 49, at 16.

B. Toward a New Policy Paradigm

The Roundtable participants largely agreed that the traditional policy paradigm is ill-equipped to advance the laudatory goal of facilitating the transition to an NGN architecture. After all, it generally makes sense to operate networks at regional or state levels and to empower local agencies with the ability to use information and communications technology as needed without bearing the responsibility for running advanced networks. Thus, while it is clear that "[n]ew public safety applications and capabilities involving broadband communications, IP technologies and flexible radios and spectrum sharing opportunities with commercial providers where appropriate are all in public safety's future,"[53] policymakers have yet to spur the transition to an NGN-based strategy. Fortunately, the spectrum to be made available in the wake of the digital television transition provides a unique policy opportunity, which must not be wasted.

1. The Next Generation Network in Practice

During the Roundtable, the participants emphasized that the NGNs are not simply theoretical possibilities. Rather, they are already being implemented in New York City and Washington, D.C.

a. New York City

In September 2006, New York City awarded Northrop Grumman a $500 million, five-year contract to build and operate a broadband wireless network that could be used by all public safety agencies as well as other governmental entities.[54] Using 10 MHz of leased spectrum (reportedly in the 2.5 GHz BRS spectrum range), this network will rely on commercially developed technology supported by the internationally-recognized, third-generation wireless standard UMTS TD-CDMA to facilitate peak data rates of over 2 MB/s to individual users.[55]

---

[53] Statement of Stephen T. Devine, *supra* note 51.

[54] Press Release, Northrop Grumman, Northrop Grumman Wins $500 Million New York City Broadband Mobile Wireless Contract (Sept. 12, 2006), *available at* http://www.it.northropgrumman.com/pressroom/press/2006/pr31.html.

[55] Dave Plank, *Why Not WiMAX?,* PUB. SAFETY COMM., Apr. 2007, at 33, 35.

b. Washington, D.C.

The National Capital Region Interoperability Program ("NCR") has developed a plan for constructing an NGN to serve Washington, D.C. and eighteen other jurisdictions within Virginia and Maryland.[56] This network, which will use spectrum allotted to public safety agencies after the digital television transition (in the 700 MHz band), will be built to meet public safety requirements. It promises to deliver users up to 3.1 Megabits per second and average receiver rates of 1.1 Megabits per second. To facilitate the development of this NGN, the FCC granted the NCR a waiver that allowed it to use spectrum not yet officially assigned to it, emphasizing the importance of broadband communications to public safety agencies.[57] To build this network, the NCR contracted with Alcatel-Lucent to "provide a seamless interoperable, redundant wireless broadband network of networks with the capacity to transmit video, data and voice communications."[58]

2. Strategies for a Next Generation Architecture

To spur the development of an NGN for public safety, this article develops two strategies—"government as contractor" and "public safety spectrum licensee." To be sure, these models are not entirely distinct approaches, but instead, blur in their application. The essential difference is that the latter uses the license itself—which can be used for both commercial and public safety uses—as an incentive for a commercial firm to develop an NGN for public safety. In either case, however, it is critical that the expectations and requirements for a public safety NGN be set forth clearly at the outset and enforced upon implementation.

a. Government as Contractor

In general, the government as contractor model can be quite effective. In the United Kingdom, for example, the government outlined the relevant requirements and held a competitive reverse auction that allowed private firms to bid

---

[56] *National Capital Region First to Deploy 700 MHZ Wireless Network for Public Safety Communication*, GOV'T TECH., Mar. 2, 2007, http://www.govtech.com/gt/104189 [hereinafter *National Capital Region First to Deploy*].

[57] *In re* Request by National Capital Region for Waiver of the Commission's Rules to Allow Establishment of a 700 MHz Interoperable Broadband Data Network, *Order*, 22 F.C.C.R. 1846, ¶¶ 9–10 (Jan. 31, 2007).

[58] *National Capital Region First to Deploy*, *supra* note 56.

for the right to build the relevant network and serve public safety agencies for a defined term.[59]

The principal virtue of a government as contractor model is that the initial competition can provide valuable efficiencies—at least if the government defines and enforces the terms effectively. Consider, for example, that a commitment to a period of years can enable the government to avoid paying all of the capital costs up front. Of course, even if the government need not pay all of the costs up front, this model still requires a significant government investment. As Vice Chair of the National Public Safety Communications Council Harlin McEwen noted at the Roundtable, the New York City and Washington, D.C. projects are being built due to the availability of considerable federal funding. Unfortunately, such funding is unlikely to be available for most of the nation's public safety agencies.

The government as contractor model remains imperfect and requires thoughtful planning, sufficient funds, and careful oversight to work effectively. When planning, governmental entities must not only develop their necessary requirements initially, but also must be mindful of the possibility of vendor lock-in[60] on the applications and equipment side. Furthermore, discounts offered early on will not last forever. Rather, the use of proprietary equipment may require expensive upgrades. Finally, firms might be willing to make commitments that they cannot ultimately keep, requiring an effective oversight process to address any failures to deliver the promised levels of performance.

b. Public Safety Spectrum Licensee

Recently, the concept of using a license for wireless spectrum to spur the development of a public safety NGN has attracted considerable support. This concept can be implemented through a variety of forms, including an approach that assigns a portion of the public safety spectrum to a nonprofit organization (as the FCC has adopted);[61] an approach that makes spectrum available to a commercial carrier as long as the carrier can meet public safety's requirements

---

[59] Jerry Brito, *Sending Out an S.O.S.: Public Safety Communications Interoperability as a Collective Action Problem*, 59 FED. COMM. L.J. 457, 483–84 (2007) (discussing the United Kingdom Airwave network).

[60] Vendor lock-in refers to the situation in which a company adopts a technology for which a single vendor can charge supra-competitive prices because that company cannot easily switch to a competitive alternative. *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES 103–225 (1999).

[61] Spectrum Auction Rules Order, *supra* note 4, ¶¶ 371–73 (eligibility criteria for Public Safety Broadband Licensee).

(as Jon Peha proposed);[62] or an approach that encumbers some additional band of spectrum with a requirement to serve public safety entities (as the FCC has adopted).[63] Ultimately, all of these approaches illustrate the logic of a mixed-use network. In particular, while public safety requires certain specifications for its information and communications technology needs, its uses are generally episodic, leaving considerable capacity underused at most points in time.

The emergence of the public safety spectrum licensee model owes a debt to Morgan O'Brien, whose Cyren Call proposal was built around this concept.[64] Building on this proposal, Frontline Wireless set forth a model with similar characteristics based on an auctioned-off block of spectrum.[65] After considering whether a duty to serve public safety via a block of auctioned spectrum was a sound policy strategy, the FCC adopted a variant of this proposal and instituted a new policy framework to govern public safety communications.[66]

At the core of the FCC's new policy framework is the concept that a national nonprofit entity, a "Public Safety Broadband Licensee," would be given a license for 12 MHz of spectrum to encourage the development of a nationwide, interoperable broadband network.[67] Moreover, to provide a partner for

---

[62] *In re* Implementing a Nationwide Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket No. 06-229; Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, WT Docket No. 96-86, *Comments of Jon M. Peha*, at 4–5 (Feb. 6, 2007) (accessible via FCC Electronic Comment Filing System). Under Peha's proposal, the FCC would reassign the license if the carrier did not meet public safety requirements. *Id.*

[63] Spectrum Auction Rules Order, *supra* note 4, ¶¶ 386–513 (nature of 700 MHz Public/Private Partnership).

[64] *See In re* Reallocation of 30 MHz of 700 MHz Spectrum (747-762/777-792 MHz) From Commercial Use; Assignment of 30 MHz of 700 MHz Spectrum (747-762/777-792 MHz) to the Public Safety Broadband Trust for Deployment of a Shared Public Safety/Commercial Next Generation Wireless Network, *Petition for Rule Making*, RM-11348 (Apr. 27, 2006) (accessible via FCC Electronic Comment Filing System).

[65] *See In re* Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, WT Docket No. 06-150; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, CC Docket No. 94-102; Section 68.4(a) of the Commission's Rules Governing Hearing Aid-Compatible Telephones, WT Docket No. 01-309; Biennial Regulatory Review—Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services, WT Docket No. 03-264; Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission's Rules, WT Docket No. 06-169; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket No. 06-229; Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, WT Docket No. 96-86, *Initial Comments of Frontline Wireless, LLC* (May 23, 2007) (accessible via FCC Electronic Comment Filing System).

[66] *See* Spectrum Auction Rules Order, *supra* note 4, ¶ 325.

[67] *See id.* ¶ 373; *see also* Public Safety and Homeland Security Bureau Solicit Applica-

this licensee, the FCC decided to make available an additional 10 MHz of spectrum that would be auctioned off to any interested bidder willing to cooperate with the public safety spectrum licensee and to operate a public safety-centric network.[68] In theory, the winner of this auction, in conjunction with the 12 MHz dedicated to public safety, would be capable of operating a broadband network designed for public safety, but available for other commercial users.[69]

A critical question related to this new policy model is how the relevant governance structure will work in practice. Under the FCC's rules, the agency selects an applicant for the public safety broadband license and, in so doing, approves its governance structure and legitimacy.[70] In adopting the relevant rules, the FCC did not offer many details, but it did suggest that such an entity must be a nonprofit body able to represent public safety.[71] Moreover, the FCC set forth a framework for a Network Sharing Agreement ("NSA") between the public safety broadband licensee and the winner of the encumbered spectrum available via the auction, emphasizing the need for flexibility in this arrangement.[72] In so doing, the FCC positioned itself as the arbiter over the development of the NSA as well as over any disputes as to whether the commercial partner complied with its terms.[73]

The allure of the public safety spectrum licensee model is that it uses spectrum, in combination with the mixed-use concept and public safety as an anchor tenant, as the asset with which to attract capital investment.[74] Given its untested nature, the public safety spectrum licensee model raises a number of questions, such as: (1) whether the model will be economically viable in practice; (2) whether a network can be built to meet public safety's requirements, including offering prioritization for public safety uses; and (3) whether this network will attract private users. In evaluating these questions and concerns, policymakers must juxtapose them against the question of whether it is reasonably likely that the government will finance an NGN in the future.

---

tions for The 700 MHz Public Safety Broadband Licensee, *Public Notice*, DA 07-3885 (Sept. 10, 2007), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3885A1.pdf.

[68] *See* Spectrum Auction Rules Order, *supra* note 4, ¶ 386.

[69] *See id.* ¶ 412 (noting the right of public safety licensee to provide spectrum access to commercial users on interruptible basis).

[70] *See id.* ¶¶ 371–77 (detailing licensee eligibility requirements).

[71] *Id.* ¶ 371.

[72] *Id.* ¶ 383.

[73] *Id.* ¶ 497 (providing for binding arbitration if negotiation over NSA cannot resolve outstanding issues); *id.* ¶ 508 (authorizing Chiefs of the Wireless Bureau and the Homeland Security Bureau to adjudicate disputes).

[74] *See id.* ¶ 396. An anchor tenant is an entity whose tenancy provides sufficient rent to serve as an anchor for a larger development.

In discussing the optimal strategy, many Roundtable participants indicated that the most efficient approach to facilitating the development of an NGN would involve the direct appropriation of funds (from auction revenues or otherwise) to subsidize it. To date, however, Congress has declined to fund such a program, raising the question of what second-best option is available. Thus, it is quite plausible that, even with its uncertain success, the public safety spectrum licensee model is the best strategy for facilitating the development of an NGN architecture. Nonetheless, any such model must be implemented in a careful and effective manner, ensuring that commitments are kept and abuses prevented. Notably, the governance challenges to avoid such shortcomings are significant and must be considered seriously by policymakers.

In practice, the public safety licensee model can succeed alongside the government as contractor model to the extent that local or state efforts work to develop a next generation architecture that can be incorporated into the public safety licensee's overall strategy. It is thus theoretically possible that there will not be a single, nationally driven NGN, but rather an allied and compatible "network of networks."[75] Ideally, there will be a formal effort, led by the public safety licensee in conjunction with a commercial partner, to support this network of networks. But if the public safety licensee initiative fails, it is conceivable that different local, regional, and state-based next generation projects—like the ones in New York City and Washington, D.C.—will gravitate toward compatible standards and will be interoperable. Such an achievement will require, at a minimum, some national effort to ensure uniformity. Such a result is unlikely, however, as the history of locally developed systems, which have traditionally adopted incompatible equipment, is quite discouraging.

The Roundtable participants agreed that there were notable advantages to establishing a nonprofit board to oversee the development of a public safety NGN, but emphasized that it must be done carefully and that many important issues had yet to be addressed. As an initial matter, there was a clear consensus that one of the benefits of such a board is that it would be more focused on the needs of public safety than the FCC. The success of the board would depend upon the development of its charter and membership. Thus, ensuring that the board serves as an effective negotiator and overseer of any commercial con-

---

[75] *See* NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL VII, COMMUNICATION ISSUES FOR EMERGENCY COMMUNICATIONS BEYOND E911, at 31 (2005), http://www.nric.org/meetings/docs/meeting_20051216/FG1D_Dec%2005_Final%20Report.pdf. The FCC has contemplated this possibility and, as a result, a local entity can construct a network if the public safety spectrum licensee gives its approval. *See* Spectrum Auction Rules Order, *supra* note 4, ¶ 484.

tracts to develop an NGN for public safety organizations is of vital importance.[76]

To ensure success, the board must uphold several duties. First, the board must be concerned about, and representative of, the public interest in general and public safety interests in particular. Second, the board, either as a result of its members or hired consultants, must be technically savvy. Third, the board must be empowered to act on its own. It is critical that it not routinely need to seek permission of the FCC or be subject to its review through an appeals process. Finally, it is important that the board have a broad perspective and diversity of membership. This can be accomplished by including state and local officials mindful of public safety funding and management issues.

The success of a public safety licensee model will correlate with selecting a public safety spectrum licensee who could lease capacity to, and cooperate with, a commercial provider to oversee the development of the NGN. It is critical that the licensee be well positioned to ensure that the cooperating firm meets its commitments. An effective enforcement mechanism is particularly important to the extent that the commercial firm bid on spectrum licenses that are required to serve public safety. The Roundtable did not expressly identify a single enforcement strategy, but participants suggested a number of options, including a performance bond, a lien that would apply to the license purchased at auction, or alternatively, a lien that would apply to the infrastructure associated with the spectrum intended to serve public safety. The FCC addressed the enforcement issue by calling for the public safety spectrum licensee and the relevant commercial partner to enter into a network sharing agreement ("NSA"), subject to FCC approval.[77]

One important caution the Roundtable participants emphasized was that private-public partnerships and public authorities have a mixed track record due to ineffectiveness of their boards. Unfortunately, the boards sometimes consist of unqualified individuals, such as those appointed for purely political reasons, that do not make effective business decisions. Moreover, in some cases, such bodies are not politically accountable or subject to any oversight, thereby invit-

---

[76] *See Hearing on Oversight of the Nat'l Telecomm. Info. Admin. and Innovations in Interoperability Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong. (2007) (statement of Jon M. Peha, Professor of Electrical Engineering and Public Policy, and Associate Director of the Center for Wireless & Broadband Networking, Carnegie Mellon University), *available at* http://www.ece.cmu.edu/~peha/Peha_testimony_public_safety_comm_March2007.pdf ("Every move [the nonprofit board] makes will be scrutinized by equipment vendors and potential service providers. Its leadership must be strongly motivated to serve the public interest, while countless Fortune 500 companies try to influence its decisions.").

[77] *See* Spectrum Auction Rules Order, *supra* note 4, ¶ 386.

ing ineffective management, corruption, or other abuses. In creating the board, it is therefore critical to build in checks against abuses. Additionally, the FCC, in its role as licensor, must be mindful of the board's composition and actions without immersing itself in the decision making process. In particular, the FCC must insist upon a reporting structure that ensures appropriate levels of transparency. There must also be assurances that the spectrum dedicated to public safety is actually used to facilitate the development of an NGN, which can include leases to commercial providers that will help subsidize the development and deployment of this network. In theory, the NSA and the possible consequences for non-compliance (i.e., a forfeiture of the license[78]) should accomplish these goals; however, the failure of past commitments by spectrum licensees creates a reasonable cause for concern.

Underscoring the critical nature of an effective enforcement regime are the significant cost implications of providing broad-ranging coverage. As discussed above, providing robust indoor coverage can significantly increase network costs and, more generally, covering all geographic areas effectively will substantially increase costs. Consequently, if the commercial providers that gain access to spectrum with a requirement to serve public safety are able to disregard costly requirements without consequence, they will have considerable incentives to do so.

3. The Importance of Flexibility, Adaptability, and Local Tailoring

In facilitating the development of an NGN for public safety, it is critical that the network be designed so as to allow for local tailoring. In particular, such a network should empower public safety officials to use information and communications technologies to meet their needs. In effect, each organization using the NGN would own a separate Intranet-like, virtual private network tailored to meet its specific needs. Thus, decisions regarding network-enabled applications, types of security provided, and management of when, how, and by whom the network is accessed, will be made by the relevant local official. Finally, if a locality desired additional coverage beyond the level contracted-for or required of the licensed network provider, it would be in a position to pay for it. In practice, however, it is more likely that such a local entity would want to enforce the required level of service rather than pay for additional service.

---

[78] *Id.* ¶ 523 (noting the Commission's authority to oversee compliance with NSA, to create rules on licensing, and to cancel the license).

4. Challenges for a New Policy Strategy

The development of a new policy strategy must take seriously the need to change the legacy mindset of those operating networks on behalf of public safety agencies. There are, in fact, three distinct cultural legacies that a next generation network must overcome. First, agencies must learn to work cooperatively and rely on communications technology that they do not control directly. Second, different agencies must agree to shared-governance rules that will specify how the NGN will operate. Finally, public safety agencies must adopt a broader view of communications technology and embrace the idea of a "converged ecosystem," while forgoing the notion of a specialized network built solely for, and operated solely by, public safety agencies.

The challenges related to cooperation between different agencies cannot be underestimated. Notably:

> [T]he history of fiefdoms within the respective agencies obscures "gains from cooperation." In many cases, managers of legacy radio systems tell chiefs that "you need to stick with the traditional land mobile radio system" or the system won't remain secure. To be sure, education and demonstration projects are part of the answer because there is a basic lack of understanding about how modern networks are designed and managed - for example, security typically stems from effective encryption, not physically separate networks. Yet education alone will not do the trick. As Chief Werner recounted from his experience, getting beyond the silo-based approach is starting to happen where incentives for cooperation - in the form of federal grants - create opportunities to bring together groups of distinct agencies and individuals through consensus-building leadership.[79]

These observations are demonstrated through the experience of the integrated wireless network ("IWN"), which is being developed for the Department of Justice ("DOJ"), the DHS, and the Treasury Department.[80] From an NGN perspective, the IWN project is of questionable wisdom insofar as it envisions a nationwide wireless network built for voice communications and limited in terms of access—i.e., it does not support nor necessarily interoperate with state or local first responders. Given its $5-$10 billion price tag over the

---

[79] *See* PHILIP J. WEISER, ASPEN INST., CLEARING THE AIR: CONVERGENCE AND THE SAFETY ENTERPRISE 24–25 (2006), *available at* http://www.aspeninstitute.org (search "Clearing the Air;" then follow hyperlink to article) (quoting Charlottesville Fire Chief Charles Werner). Many others have emphasized the centrality of this issue. *See, e.g.*, SPACE & ADVANCED COMMC'NS RESEARCH INST., GEORGE WASH. UNIV., WHITE PAPER ON EMERGENCY COMMUNICATIONS 1 (2006), *available at* http://satjournal.tcom.ohiou.edu/issue10/PDF/Final_Version_White_Paper.pdf (quoting Garry Briese's Dec. 13, 2005 keynote address at the NCEC: "The hardest part of improving emergency warning and recovery efforts is changing human behavior.").

[80] *See* U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN. AUDIT DIV., PROGRESS REPORT ON DEVELOPMENT OF THE INTEGRATED WIRELESS NETWORK IN THE DEPARTMENT OF JUSTICE (2007), *available at* http://www.usdoj.gov/oig/reports/OBD/a0725/final.pdf.

next fifteen years, there is a powerful case for scrapping the IWN initiative altogether and folding it into the plans for an NGN for public safety agencies. Significantly, however, it is not the IWN's limited ambition that has drawn criticism of late, but the inability of the key partners in the project—the DOJ, DHS, and Department of Treasury—to work together. As the DOJ Inspector General recently explained, the IWN program was unlikely to be successful both on account of funding failures as well as an inability to develop an effective governance strategy between the relevant agencies.[81] Indeed, on the governance front, the project envisions decisions between the three agencies to be made by consensus, but provides no alternative when deadlock occurs on some key issues.[82]

The Roundtable participants generally viewed the IWN project as an example of the traditional silo-based culture and recommended a more enlightened strategy that includes all emergency responders as part of an enterprise. Stated differently, the IWN model not only fails to develop a next generation architecture, but it also makes the mistake of building separate networks for individual agencies (i.e., it does not provide access to an array of federal, state, and local agencies), thereby making interoperability more difficult and network development costs greater.

Once organizations are willing to work together, there remain challenging governance questions that must be resolved. Notably, the organizations must cooperate based upon a shared understanding of how the network will be used, who will have access to it, and how prioritization issues will be managed. In particular, an NGN will need to develop policies, based on discrete scenarios, which will govern priority access to the network and set forth legitimate usage policies.[83] To some extent, a requirement to pay for services—such as video streaming—will counter any incentives to be a bandwidth hog, but during times of crisis, it may well be the case that all users of the network would insist that they need priority access, or at least some assured access, to the network.

While the aforementioned challenges are formidable, they are not novel and they can be overcome. In particular, some states have already developed governance structures that enable different agencies to work together effectively. In Virginia, for example, the commonwealth developed a well-functioning

---

[81] *Id.* at xi.

[82] *Id.* at 27.

[83] Several of the participants, including Charles Werner, Chief of the Charlottesville, Va. Fire Dep't, stressed the importance of dealing with governance issues early. In addition, Peter Erickson, CoCo Communications' Vice President of Business Development, provided the example of Texas's three security levels for disaster situations. Each includes full auditing and recording of who was and who was not on the network during any relevant time period.

governance structure to facilitate cooperation regarding issues ranging from the use of communications technologies to the use of a common language (moving from so-called "ten-code" abbreviations such as "10-4" to plain English).[84]

Finally, for an NGN to operate effectively, users must be trained and willing to take advantage of new functionalities and applications. To encourage such willingness, leaders must advocate on behalf of the advantages of a new network and encourage public safety agencies to change their usage habits. To do so, it is likely that officials will need to create "living laboratories" that demonstrate how new IP-based technologies can enable public safety agencies to operate more effectively. Officials will also need to provide incentives and accountability mechanisms to change the traditional silo-based orientation.[85]

IV. TRANSITIONAL CHALLENGES

A. Working Within the Current Technological Framework

It is critical that policymakers begin planning for a next generation architecture. Such plans, however, cannot ignore the reality that current networks often fail to provide interoperability on a broad basis. Efforts to facilitate interoperability using the traditional architecture included encouraging the sharing of digital trunked systems and specialized radio systems. This effort succeeded only on a relatively limited basis, however, as the price of such radios has remained high and many emergency response organizations have not adopted them. Just recently, the GAO summarized the pitfalls of the P25 initiative and criticized the DHS for emphasizing this effort in its grant guidance.[86] In retro-

---

[84] *See* Chris Essid, *Virginia Puts Interoperability Together*, MISSION CRITICAL COMM., May 2005, at 70, 70, 74; Chris Essid, *A Model for Interoperability*, MISSION CRITICAL COMM., Feb. 2007, at 68, 68, 72–73.

[85] *See generally* Philip J. Weiser, *Communicating During Emergencies: Toward Interoperability and Effective Information Management*, 59 FED. COMM. L.J. 547 (providing an in-depth discussion of the intergovernmental relations strategy necessary to facilitate adoption of a next generation network for public safety). In adopting a new regulatory strategy, the FCC is very mindful of the need to move behind the traditional silo-based perspective. *See* Spectrum Auction Rules Order, *supra* note 4, ¶ 370.

[86] Even at present, as the GAO explained in a recent report:

> [A]mbiguities in the published standards [for the Project 25 initiative] have led to incompatibilities among products made by different vendors, and no compliance testing has been conducted to ensure that vendors' products are interoperable. Nevertheless, DHS has strongly encouraged state and local agencies to use grant funding to purchase Project 25 radios, which are substantially more expensive than non-Project 25 radios. As a result, state and local agencies have purchased fewer, more expensive radios, which still may not be interoperable and thus may provide them with minimal additional benefits. Until DHS modifies its grant guidance to provide more flexibility in

spect, P25 erred by treating public safety communications as a distinct entity, giving rise to proprietary technologies that are not compatible with commercially developed and far cheaper alternatives.[87] Even putting aside any evaluation of P25's merits, it is incontestable that P25 focuses on narrowband voice communications and that this technology falls short in an era in which IP-based, broadband networks are becoming the preferred mode of communications.

As noted previously, the Roundtable participants agreed that the development of a next generation architecture is going to take time and will succeed in replacing existing systems only once it is proven to be fully effective.[88] Thus, the foreseeable future will be a transitional state in which NGNs are developed and used alongside their traditional counterparts. By adopting a modular architecture, which might include multi-mode radios, multiple devices, or both, localities can select the best available technologies to meet their needs. Moreover, they should investigate opportunities to provide interoperability on a cost-effective basis, realizing that, in the long term, the most effective form of interoperability will be the prevalent use of IP-based, broadband networks.

Even for public safety agencies using traditional land mobile radio systems, a number of firms, including Cisco, Twisted Pair, and CoCo Communications, have developed solutions using Internet Protocol-based technologies to enable interoperability without replacing existing radio systems with expensive Project 25 radios.[89] These solutions have already demonstrated, in deployments such as one in Dallas's Love Field, that they can enable interoperability in a relatively inexpensive fashion.[90] Moreover, with emerging technologies like mesh networking systems, radios connected through such solutions can even communicate directly with one another and without the aid of a central gate-

---

purchasing communications equipment, states and localities are likely to continue to purchase expensive equipment that provides them with minimal additional benefits. GAO INTEROPERABILITY REPORT, *supra* note 49, at 4.

87 *See* Rouleau, *supra* note 31, at 98, 103.

88 Mark Adams, Chief Architect, Networks & Communications of Northrop Grumman IT, suggested that there will likely be a ten to fifteen year transition period. On this point, Joe Hanna, former President of APCO, emphasized the importance of not "chopping off" old technologies before new ones were established as reliable and sufficient to meet the needs of public safety. However, Jon Peha, Professor of Electrical and Computer Engineering at Carnegie Mellon University, stressed that even though it will be a long transition period, requirements should be imposed on new technologies to ensure that they eventually replace the legacy systems.

89 *See, e.g.*, CISCO SYSTEMS, BEYOND RADIO: REDEFINING INTEROPERABILITY TO ENHANCE PUBLIC SAFETY (2007), *available at* http://www.cisco.com/application/pdf/en/us/guest/products/ps6718/c1244/cdccont_0900aecd80535985.pdf.

90 McKay, *supra* note 37.

way.[91] Finally, such solutions can also, through the use of encryption technology, address security concerns and even provide users of the system with "Type 1 encryption" used by the United States military.[92] Certainly, such solutions are imperfect, but they do offer cost-effective alternatives to purchasing new radio systems that are very expensive and technologically inferior to NGN systems.

Increasingly, states are spearheading cost-effective solutions to promote interoperability using traditional LMRs. In Washington, for example, the State Executive Interoperability Committee is promoting the use of a voice over Internet Protocol ("VoIP") backbone network to enable state and local agencies using a variety of different radio frequencies to interoperate with one another.[93] To that same end, the Olympic Public Safety Communications Alliance Network ("OPSCAN"), which is using Twisted Pair's WAVE technology, operates a network that provides for interoperability among forty-two agencies and organizations in five counties.[94] Notably, this interoperability occurs among agencies with disparate environments, including VHF, UHF, 700 MHz, and 800 MHz frequencies. Significantly, the IWN network is using a similar technology to address interoperability issues.[95]

In short, during the transition period from today's traditional systems to a next generation system, local agencies should not only adopt interoperability

---

[91] *See, e.g.*, Donny Jackson, *Vendor Says New Release Will Deliver Nationwide Interoperable Communications*, MOBILE RADIO TECH., Apr. 11, 2007, http://mrtmag.com/infrastructure/news/nationwide-interoperable-communications-041107 (according to CoCo Communications' Director of Technology, Riley Eller, "CoCo has enabled interoperable communications between disparate systems through a mesh-networking protocol that could scale to thousands of digital gateways . . . . With the 4.0 release, CoCo has improved the scalability of its meshing protocol and designed a system that only resorts to ad-hoc mesh networking when an agency's IP network fails . . . .").

[92] *See* Donny Jackson, *Big D's Magic Bullet*, MOBILE RADIO TECH., Mar. 1, 2007, http://mrtmag.com/mobile_voice/mag/radio_big_ds_magic/. Type 1 encryption refers to a level of protection, as defined by the National Security Agency, that suffices for such products to be used by the United States government.

[93] Spencer Bahner & Dave Zehrung, *Interop on the Border*, MISSION CRITICAL COMM., Nov.-Dec. 2006, at 57, 64.

[94] Press Release, Twisted Pair Solutions, Twisted Pair Solutions Teams with Customer, Partner to Reach Finals for TWO WSA Industry Achievement Awards (Jan. 19, 2007), *available at* http://www.twistpair.com/index/news-app?section=Press%20Releases&offset=10 (follow hyperlink to press release).

[95] Wilson P. Dizard III, *General Dynamics to Build Integrated Radio System*, WASH. POST, Apr. 30, 2007, at D4 (quoting Jeff Osman, General Dynamics' executive program manager for IWN, saying that it will use "various types of gateway systems to mix and match the modern digital radio systems with the old-style analog systems that are still used by many police departments nationwide." Osman added that the "federal government study contractor [for the IWN program] recommended an Internet protocol-based solution . . . . It opens up the ability to tie together multiple types of radio systems.").

solutions, but should also use available technologies to supplement their traditional networks. Although sometimes overlooked, the reality today is that many public safety agencies use commercial services and products for a number of purposes.[96] Such services are not only affordable and user-friendly, but they are increasingly provided according to service level agreements that were developed to meet the needs of public safety and specify a required level of performance.[97] Moreover, a number of public safety agencies are already using broadband connections provided by wireless broadband technologies such as Wi-Fi, EVDO, and mesh networking.[98] Such systems enable public safety agencies to access a range of applications, including photo databases, video camera feeds, and driver's license information.[99]

B. Building A Sustainable Funding Base For Public Safety Communications

Public safety has yet to follow the lead of leading commercial firms such as Wal-Mart in realizing that an investment in information and communications technology can pay great dividends in terms of the ability to operate effectively and efficiently.[100] Until, however, policymakers appreciate this insight and view public safety as an integrated enterprise, public safety agencies will continue to lack access to the cutting edge information and communications technologies necessary to best protect the public. As Harlin McEwen explained,

---

[96] The DHS National Interoperability Baseline Survey, for example, found that sixty-eight percent of public agencies use commercial wireless phones on a daily basis, seventy-nine percent use a personal digital assistant, and twenty-seven percent use laptop computers and commercial broadband wireless networks. SAFECOM, 2006 NATIONAL INTEROPERABILITY BASELINE SURVEY 45 (2006), *available at* http://64.210.244.119/NR/rdonlyres/40E2381C-5D30-4C9C-AB81-9CBC2A478028/0/2006NationalInteroperabilityBaselineSurvey.pdf.

[97] Justin Schmid, *Upward Mobility*, MISSION CRITICAL COMM., July 2006, at 44, 51 (noting that over eighty percent of Verizon Wireless transmission sites in Florida were built with their own backup power generators to enable them to function in case of a power outage during an emergency).

[98] Russell H. Fox & Jennifer A. Lewis, *Whither WiMax?*, MISSION CRITICAL COMM., Mar. 2006, at 48, 51; Mannie Garza, *EnMESHed*, PUB. SAFETY COMM., Dec. 2006, at 46, 47 (discussing Motorola Mesh Enabled Architecture purchased by the City of Providence); *id.* at 48 (discussing Tropos mesh network adopted by the City of Tucson); *id.* at 51 (discussing PacketHop system); TROPOS NETWORKS, METRO-SCALE WI-FI FOR PUBLIC SAFETY: SAN MATEO POLICE DEPARTMENT (2004), *available at* http://www.tropos.com/pdf/SMPD_Casestudy.pdf.

[99] Fox & Lewis, *supra* note 98, at 51–52.

[100] Marc L. Songini, *Wal-Mart Details its RFID Journey*, INFO WORLD, Mar. 2, 2006, http://www.infoworld.com/article/06/03/02/76038_HNwalmartrfid_1.html (discussing some of the benefits of Wal-Mart's RFID system, including tripling the rate of replenishing out-of-stock items).

"[o]ur public safety users who should have the best, most advanced, and most robust capabilities too often must rely on systems that are inadequate for their needs today, much less the expanded responsibilities with which they will continue to be charged in the future."[101]

In many respects, the near-term presents the most challenging funding demands of all—policymakers must make do with legacy systems as well as facilitate the development of a next generation system. Ultimately, once a next generation system is well-proven and adopted by public safety agencies, there may be an opportunity for those agencies to abandon their legacy equipment and their traditional spectrum allocations. But such a day is both far off and uncertain. Until then, policymakers face the dual challenges of facilitating the development of the best possible technologies to work in conjunction with existing systems as well as laying the groundwork for a next generation architecture.

The funding challenges related to public safety communications are often discussed in policy circles as one-time issues related to solving the interoperability problem. Again, the ultimate solution is the effective development and widespread adoption of NGNs. Like the issues related to the upgrade of the E911 system, however, policymakers often fail to develop dedicated revenue streams to support public safety's technology needs. Indeed, even where they have done so, they have sometimes failed to use those funds for their intended purposes.[102]

Finally, when discussing proposals such as the public safety spectrum licensee proposal, some emphasize that the spectrum could be monetized to support the development of public safety technologies and mistakenly suggest that as a substitute for public support. This approach, however, does not relieve public safety agencies of the need to pay for the adoption of new technologies. After all, such proposals envision that public safety agencies would, at least for the foreseeable future, maintain their traditional LMRs while paying additional funds for access to an NGN. Consequently, even under the public safety licen-

---

[101] Testimony of Harlin R. McEwen, *supra* note 30.

[102] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, STATES' COLLECTION AND USE OF FUNDS FOR WIRELESS ENHANCED 911 SERVICES 17–20 (2006), *available at* http://www.gao.gov/new.items/d06338.pdf; *see also* Letter from William P. Challice, Audit Dir., State of N.Y. Office of the State Comptroller, to Wayne E. Bennett, Superintendent, Div. of State Police, Randy Daniels, Sec'y of State, Dep't of State, and Andrew Eristoff, Acting Comm'r, Dep't of Taxation & Fin. (Feb. 18, 2004), *available at* http://osc.state.ny.us/audits/allaudits/093004/03f9.pdf (finding that between August 2002 and June 2003, more than forty percent of funds earmarked for expanding 911 capabilities were diverted for general budget relief in New York State).

see model—as well as the government as contractor model—there is an essential need for an investment in public safety's use of cutting-edge technologies.

C. Developing Clear Requirements, Specifications, and Standards That Will Meet Public Safety Needs

The Roundtable briefly discussed methods of developing the technologies that will comprise an NGN. By all accounts, any national body interested in promoting an NGN will face the question of how to promote and ensure the adoption of some standardized architecture. At one level, the commitment to use IP-compatible technologies provides an important assurance that all systems will be reasonably compatible (able to exchange IP packets across a wired backbone). However, that commitment does not imply that all mobile devices will be able to communicate with the nearest base station tower or that all applications will work properly across administrative boundaries. Thus, it is important to appreciate that an effective public safety communications ecosystem will benefit from a defined set of standards that supports critical applications and encourages a variety of vendors to compete to meet public safety's needs.

In terms of standardization efforts, there was widespread agreement that Internet Protocol-based technologies would form the basis of a next generation network. Nonetheless, many participants emphasized that there still exists a critical need for the public safety community to define the requirements of important applications and for technologies to be adapted to meet those specific needs. Although rights management technologies are already widely deployed to enable large enterprise businesses like Wal-Mart to operate a virtual private network with access to a variety of information regulated by rights management,[103] such technologies must be adapted to the public safety context.

The federal government has already started to support the development of next generation standards for public safety, but considerable work remains.

---

[103] Such technologies would, for example, enable numerous individuals and firms to have access to the company's network, but would restrict access to employee records, supply chain information, and accounting records. Similarly, a system of rights management in the public safety context would allow all agencies to share an Intranet-like service, but would, for instance, restrict access to criminal histories to police and medical information to emergency medical personnel. *See generally* Barry Bozeman & Stuart Bretschneider, *Public Management Information Systems: Theory and Prescription*, 46 PUB. ADMIN. REV. 475 (1986) (discussing the differences between rights management systems developed in the private context and those needed in the public setting).

Both SAFECOM[104] and the National Institute of Standards and Technology,[105] for example, are involved in an initiative to determine how VoIP can be used to support public safety, but it is still at a very preliminary stage.[106] Nonetheless, efforts to develop standards need not, and should not, seek to replicate or substitute for commercial development. Rather, as Doug Smith, Ericsson Executive Vice President and General Manager of Government Solutions, emphasized, they should follow commercial standards activity and highlight the requirements that must be included within the commercially developed standards. Indeed, Smith noted that Ericsson was mindful that public safety agencies could benefit from next generation technology and Ericsson was already focused on the need for the commercial standards development process to develop the architecture for NGN standards.

The most controversial question related to the development of standards is how public safety entities should embrace a single air interface.[107] Smith stressed the importance of choosing a single air interface, noting that a multi-mode radio that could provide both broadband and P25 access would be most economical. Smith said that without a single air interface, a true multi-mode radio based on multiple standards would not be economical. However, any effort to choose an air interface would risk slowing the development of next generation products for public safety and possibly repeat the P25 failure to deliver competitively provided and affordable equipment. Consequently, some champion the alternative approach of defining performance requirements and leaving it to the market to determine whether that would be provided via a single air interface. The risk of this approach is that it would require users to purchase multi-mode radios to be assured of ubiquitous coverage.

The attractiveness of a multi-mode access device would increase substantially if the costs of the relevant chipset decline. Nevertheless, the cost of additional modes of operation will never fall to zero. Without pre-defined stan-

---

[104] SAFECOM is an entity within the DHS's Office for Interoperability and Compatibility. It is charged with developing standards to promote interoperability between first responders. *See* About SAFECOM, http://www.safecomprogram.gov/SAFECOM/about/default.htm (last visited Nov. 12, 2007).

[105] The National Institute of Standards and Technology is the agency within the U.S. Commerce Department's Technology Administration whose mission is promoting the federal government's standards development efforts. *See* Nat'l Inst. of Standards & Tech., Mission, Vision, and Core Competencies, http://www.nist.gov/public_affairs/nist_mission.htm (last visited Nov. 16, 2007).

[106] *See* SAFECOM, ROUNDTABLE ON PUBLIC SAFETY INTEROPERABILITY AND VOICE OVER INTERNET PROTOCOL (VOIP) 3 (2006), *available at* http://www.safecomprogram.gov/SAFECOM/library/technology/1293_roundtableon.htm (follow hyperlink to report).

[107] An air interface is the technology that defines the communications link between a mobile device and its active base station.

dards, however, it is unclear how many modes each handset must support in order to work effectively in most scenarios. Alternatively, by endorsing a variety of interfaces, public safety entities could leave some discretion to equipment developers and network operators in a manner that strikes a sound balance between standardization and market experimentation. Finally, this debate might well become moot to the extent that commercial licensees operating in nearby bands all adopt a particular technology and thereby create huge economies of scale, and a powerful incentive, for public safety entities to embrace that technology.[108]

D. Research and Development Efforts That Can Lead to Transformative Technologies

The ongoing development of software defined/cognitive radio[109] presents dramatic opportunities for a more efficient and more effective use of spectrum dedicated to public safety agencies. Notably, policies that embrace cognitive and software defined capabilities represent a logical evolution of spectrum policy trends over the past twenty-five years.[110] Moreover, in principle, "[t]he flexibility inherent in [software defined radio] technology facilitates multi-protocol, multi-band, and multi-service devices that can operate across multiple systems, thereby supporting the 'system of systems' concept for public safety communications."[111] In practice, however, there are still a number of important areas for research and development to resolve, including technical matters, development of necessary standards, and economic issues.[112] To address such issues, policymakers must continue to support research and devel-

---

[108] The FCC appears to take this very perspective in concluding that the public safety licensee and its broadband partner would agree on a broadband standard as part of the NSA. *See* Spectrum Auction Rules Order, *supra* note 4, ¶ 364. By contrast, with respect to whether a specific technology would be required to access satellite communications, the FCC declined to call for the selection of any specific technology. *See id.* ¶ 468.

[109] Cognitive radio technology enables spectrum to be used on a more dynamic basis by enabling radio devices to become aware of their surroundings and adjust their behavior accordingly. *See In re* Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum use Employing Cognitive Radio Technologies, *Report and Order*, 20 F.C.C.R. 5486 (Mar. 10, 2005).

[110] Bernthal et al., *supra* note 39, at 2.

[111] SDR FORUM, SOFTWARE DEFINED RADIO TECHNOLOGY FOR PUBLIC SAFETY 26 (2006), *available at* http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-06-P-0006-V0_00_DP_T.pdf; *see also* Statement of Stephen T. Devine, *supra* note 51 (suggesting that "new frequency agile software based radios, capable of operating on multiple public safety frequency bands, can soon be used as a tool to bridge existing gaps between frequency bands").

[112] SDR FORUM, *supra* note 111, at 25.

opment of this promising technology, and they should ensure that spectrum policy decisions, such as ones related to a new test-bed for experimental uses, enable the testing of public safety applications of software-defined radio technology.[113]

In many cases, policymakers invest in a single approach, ignoring the possibility that technological change will create new opportunities. For public safety communications, it is quite likely that even the best version of a next generation architecture strategy will leave open opportunities for different approaches to be tried, such as one based on cognitive radio. As industry professionals Nancy Jesuale and Bernard C. Eydt suggest, cognitive radio technology, along with a rights management system operated through a trusted provider, promises an effective interoperability solution that can also facilitate broadband access.[114] Moreover, other technologies, such as multiple antenna wireless links or multiple-input, multiple-output ("MIMO") communications, deserve serious consideration. MIMO systems provide a number of advantages, including increased coverage, higher throughputs, and improved network reliability.[115] In short, policymakers should both develop today's cutting-edge technologies and invest in the development of tomorrow's technologies that may yield considerable benefits in the ongoing construction of an NGN for public safety.

V. CONCLUSION

Over the last twenty-five years, a number of distinct wireless networks have developed—commercial, state and local public safety, and the federal government. In each sphere, the networks have largely existed without cooperating with one another. This fact is underscored and reinforced by a lack of shared infrastructure, a reluctance to use technologies developed for the other, and distinct funding models. IP-based technologies, however, promise to change that.

For public safety agencies, IP-based technologies can facilitate the development of products and services that can be tailored to meet public safety requirements, offer them broadband capability and local adaptability, and enable

---

[113] *In re* Federal Communications Commission Seeks Public Comment on Creation of a Spectrum Sharing Innovation Test-Bed, ET Docket No. 06-89, *Comments of the Software Defined Radio Forum*, at 3–4 (July 10, 2006) (accessible via FCC Electronic Comment Filing System) (noting that a test-bed could provide the basis to evaluate sharing opportunities between adjacent spectrum using shared technologies).

[114] JESUALE & EYDT, *supra* note 24, at 8.

[115] *See* ArrayComm, An Overview of MAS Principles, http://www.arraycomm.com/serve.php?page=principles (last visited Nov. 12, 2007).

them to leverage ongoing commercial development. Such technologies, moreover, can meet the requirements of public safety agencies without requiring individual public safety agencies to build and operate their own separate networks. They do so by allowing shared infrastructure and capacity among a large number of users, thereby enabling them to leverage commercially-driven economies of scale and open standards.

Remarkably, Roundtable participants reached a consensus on a number of key points related to the development of an NGN for public safety. Ultimately, there was a broad consensus regarding the importance of investing in and equipping public safety agencies with the cutting edge information and communications technologies necessary to perform at a highly effective level. Similarly, there was a broad consensus that a new policy model would be necessary to facilitate the development of an NGN and that local agencies operating their own networks would be highly unlikely to facilitate this development. Thus, the most difficult question going forward concerns the optimal strategies for using different policy tools. In particular, it remains to be determined what the ideal balance is between relying on government contracting for NGN development and a public safety licensee model.

The opportunities presented by a next generation architecture promise to enable public safety agencies to communicate effectively with one another and use cutting-edge applications that will enable them to do their jobs more effectively. But the transition to this network will take time and will require an ongoing investment of resources. In particular, such a network will not develop rapidly and public safety agencies must continue to operate their traditional networks, and make them interoperable, until an NGN is proven to be an effective substitute for traditional LMRs.

In short, for public safety agencies, the decision to invest in state-of-the art information and communications technology is long overdue. To rectify this failing, policymakers must realize that this investment is as critical to the success of these agencies as providing them with effective equipment to protect our citizenry and respond to emergency situations across a range of life-and-death situations. Over time, the case for such an investment will only become more compelling and the costs of not making such an investment will increase. Thus, the time to start the transition to an NGN for public safety is now.