Carnegie Mellon University
Research Showcase @ CMU

Department of Engineering and Public Policy | Carnegie Institute of Technology

6-2007

Fundamental Reform in Public Safety Communications Policy

Jon M. Peha
Carnegie Mellon University, peha@andrew.cmu.edu

Follow this and additional works at: http://repository.cmu.edu/epp

Part of the Engineering Commons

Published In
Federal Communications Law Journal, 59, 2.

This Article is brought to you for free and open access by the Carnegie Institute of Technology at Research Showcase @ CMU. It has been accepted for inclusion in Department of Engineering and Public Policy by an authorized administrator of Research Showcase @ CMU. For more information, please contact research-showcase@andrew.cmu.edu.

Fundamental Reform in Public Safety Communications Policy*

Jon M. Peha**

I. INTRODUCTION 518
II. QUESTIONING TODAY'S ORTHODOXY FOR PUBLIC SAFETY COMMUNICATIONS 519
A. *Today's Basic Assumptions* 519
B. *A Time for Change* 520
C. *Properties of a Good System* 521
D. *Let Each Local Agency Decide: Flexibility Above All* 523
E. *Commercial Service Providers Need Not Apply* 525
F. *Public Safety Does Not Share* 527
G. *Emphasis on Voice Communications* 528
III. ALTERNATIVE VISIONS 529
A. *Primary Systems Run by Government Agencies* 529
B. *Primary Systems Run by Commercial Wireless Carriers* 531
C. *Secondary Systems* 534
IV. ENSURING THAT LOCAL AGENCIES ARE WELL SERVED 537
V. NEXT STEPS TOWARD A MORE EFFECTIVE POLICY 540
VI. SUMMARY 544

---

* Some of this Article appeared in Jon M. Peha's working paper, *From TV to Public Safety: The Need for Fundamental Reform in Public Safety Spectrum and Communications Policy*, (New America Foundation, Working Paper No. 15, 2006).

** Jon M. Peha, Associate Director of the Center for Wireless and Broadband Networking, and Professor of Electrical Engineering and Public Policy, Carnegie Mellon University, peha@cmu.edu, http://www.ece.cmu.edu/~peha.

I. INTRODUCTION

All across the country, there have been failures in the communications systems used by first responders, such as firefighters, police, paramedics, and the National Guard. These failures can cost lives in emergencies both large and small. This problem has gained particular attention in the tragic aftermaths of the 9/11 attacks[1] and Hurricane Katrina,[2] when inadequacies in the current system were particularly obvious, but attention has not yet translated to significant progress. As observed by the House Select Bipartisan Committee to Investigate Hurricane Katrina, "[w]ithout functioning communications systems, first responders and government officials cannot establish meaningful command and control, nor can they develop the situational awareness necessary to know how and where to direct their response and recovery efforts."[3]

Policymakers have considered a variety of remedies to these problems. Most have been small incremental adjustments to long-standing policy. Incremental change is sometimes useful, but when problems are pervasive, the impact of incremental reform will be limited. This Article argues that the problems with public safety communications are rooted in policies that have been in place for many decades and have long outlived their usefulness. Fundamental reform is needed. In the long run, fundamental reform will yield superior systems and will save resources. In the initial transitional period, the federal government should provide resources in the form of spectrum and funding. These resources are indeed coming. With them comes a great opportunity to improve public safety communications. Unfortunately, these resources are likely to be used in ways determined well before 9/11, under the auspices of these same policies that led to today's problems. If so, the resources will be wasted, and the opportunity lost.

Thanks to the transition to digital television, 84 MHz of spectrum will become available in 2009, 24 MHz of which have tentatively been

---

1. *See generally* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf.

2. *See generally* INDEP. PANEL REVIEWING THE IMPACT OF HURRICANE KATRINA ON COMMC'N. NETWORKS, REPORT AND RECOMMENDATIONS TO THE FCC (2006), *available at* http://www.fcc.gov/eb/hkip/karrp.pdf.

3. SELECT BIPARTISAN COMM. TO INVESTIGATE THE PREPARATION FOR AND RESPONSE TO HURRICANE KATRINA, 109TH CONG., A FAILURE OF INITIATIVE: THE FINAL REPORT OF THE SELECT BIPARTISAN COMMITTEE TO INVESTIGATE THE PREPARATION FOR AND RESPONSE TO HURRICANE KATRINA, 165 (2006), http://a257.g.akamaitech.net/7/257/2422/15feb20061230/www.gpoaccess.gov/katrinareport/communications.pdf. [hereinafter HURRICANE KATRINA FINAL REPORT].

allocated for public safety.[4] This roughly doubles the spectrum under 2 GHz that is allocated to public safety.[5] Moreover, this spectrum is around 700 MHz, which means it has physical properties that are particularly useful when designing a communications system that must cover a large geographic region. A nationwide block of this size, unencumbered with old equipment, is a great opportunity, at least if it is governed by effective policies.

In a strangely unrelated effort, the federal government also has plans to invest $3 to $30 billion and a significant amount of spectrum in the Integrated Wireless Network ("IWN") program,[6] which is intended to provide communications services for a small fraction of first responders, i.e., those that work for federal agencies. This Article will discuss how these resources could be used to address the larger problems faced by all first responders.

Part II describes the policies that have produced today's public safety communications systems, and why it is time for fundamental change to those policies. Part III presents alternative directions for the future. Part IV discusses how to ensure that local public safety agencies are well served and given incentive to endorse and participate in the reform process. Part V presents the next logical steps in the reform process. The Article is summarized in Part VI.

II. QUESTIONING TODAY'S ORTHODOXY FOR PUBLIC SAFETY COMMUNICATIONS

Part II.A presents basic assumptions that have long dominated how public safety communications are provided. Part II.B explains why it is time to question such assumptions. Criteria for judging a good system are presented in Part II.C, and Parts II.D through II.G describe how today's basic assumptions can be harmful based on these criteria.

A. Today's Basic Assumptions

Today's public safety communications infrastructure is built on a

4. *See* Deficit Reduction Act of 2005, S. 1932, 109th Cong. 20–24 (2005) (as passed by Senate, Dec. 21, 2005).

5. *See* FCC, REP. TO CONG.: ON THE STUDY TO ASSESS SHORT-TERM AND LONG-TERM NEEDS FOR ALLOCATIONS OF ADDITIONAL PORTIONS OF ELECTROMAGNETIC SPECTRUM FOR FED., STATE, AND LOCAL EMERGENCY RESPONSE PROVIDERS 4–5 (2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-262865A1.pdf. [hereinafter FCC REP. TO CONGRESS].

6. U.S. Dep't of Justice, Integrated Wireless Network: Home, http://www.usdoj.gov/jmd/iwn (last visited Apr. 2, 2007). *See also* Wilson P. Dizard III, *Lockheed Martin, General Dynamics Units Win IWN Contracts*, WASH. TECHNOLOGY, June 9, 2006, *available at* http://www.washingtontechnology.com/news/1_1/daily_news/28740-1.html.

number of traditional assumptions. It is assumed that primary responsibility for and authority over public safety communications lies with local governments. In most states, final decisions about infrastructure are made by individual municipal public safety agencies—such as fire departments or police departments—beyond the control of even the central units of local government, such as the Chief Technology Officer for a city or county. Federal agencies provide some assistance in the form of grants or technical advice, but the majority of the funding also comes from local governments.

It is assumed that public safety agencies must operate their own communications systems and cannot make significant use of commercial companies or municipal networks that provide wireless services (although commercial companies usually provide wireline services without controversy).

It is assumed that public safety communications must take place in spectrum that is dedicated entirely to public safety using equipment that is dedicated entirely to public safety. Thus, public safety cannot share spectrum allocations or network infrastructure with either commercial subscribers or other government users.

It is assumed that narrowband real-time voice communications is the principal application for public safety. Other forms of communications are secondary in importance, or they are not available at all. Moreover, in most cases, voice communications are provided separately from other services. Thus, in the spectrum to be reallocated from TV, proposals to provide voice communications as one of many services over a broadband network have received less serious attention.

B. A Time for Change

The above assumptions have prevailed in the U.S. for many decades, so why question them now? Because the world has changed.

First, 9/11 marks a fundamental change in requirements. It is now far more important that we be prepared to respond to large-scale disasters that require a cooperative response from many public safety agencies. A failure rate for interagency communications that was acceptable before 9/11 may not be acceptable today, even if that means giving up some local autonomy.

Second, the technology has changed dramatically. The results of this progress are obvious in commercial and military wireless systems but are not so apparent in public safety systems. In many cases, current policy and its emphasis on flexibility is an impediment to adopting new technology. For example, effective use of wireless technology can require coordinated planning over a wide frequency band, a large geographic region, or both. Moreover, useful maps or photos may be stored in a jurisdiction far from the emergency, and such information cannot be shared dynamically unless

public safety agencies in both jurisdictions have independently decided to invest in a shared infrastructure to connect them.

Third, costs have changed. In particular, the rapid growth of commercial wireless services has led to mass production and low costs. Thus, equipment used by public safety could be much cheaper than was once possible, if it is similar enough to equipment used in commercial markets. On the other hand, demand for spectrum has increased, making it more valuable. Thus, the many public safety systems designed to reduce equipment costs by consuming more spectrum are far less appropriate today, particularly considering the opportunity costs of spectrum inefficiency to the larger economy.

Finally, some people have expressed frustration over the progress achieved, despite all of the money allocated to incremental improvements. As stated by the House Select Bipartisan Committee to Investigate Hurricane Katrina, "*[d]espite hundreds of millions in federal funding* for technology and communications, the absence of true communication interoperability within and between affected jurisdictions severely hindered rescue and response efforts at all levels of government" after Hurricane Katrina.[7] After all, Secretary of Homeland Security Michael Chertoff said in May 2006 that his Department alone had "allocated over $2.1 billion to states for interoperable communications" since 2003.[8] *Perhaps the problem is not a lack of resources for incremental change, but a lack of vision to promote more effective change.*

Not only is this a time to question old assumptions; it is a time to recognize an extraordinary opportunity coming to adopt a new approach in the band reallocated from TV spectrum, which has few legacy communications systems that must be altered or replaced and few entrenched bureaucratic procedures.

C. Properties of a Good System

By considering a new approach to public safety communications, we could try to make progress in the following critical areas.

Interoperability: Interoperability is the ability of individuals from different organizations to communicate and share information. It has often been cited as a major problem for public safety in the U.S. For example, when first responders from multiple public safety agencies arrived at Columbine High School after the shooting in 1999, interoperability problems were so great that they had to rely on runners to carry written

7. HURRICANE KATRINA FINAL REPORT, *supra* note 3, at 173 (emphasis added).

8. Michael Chertoff, Remarks by Homeland Security Secretary Michael Chertoff at the Tactical Interoperable Communications Conference (May 8, 2006), *available at* http://www.dhs.gov/xnews/speeches/speech_0281.shtm.

messages from one agency's command center to another.[9]

Spectral Efficiency: It is technically possible to support today's first responders using far less spectrum.[10] When spectrum is used inefficiently, there is a greater risk that public safety will experience a shortage. With a shortage, systems would become highly congested during large emergencies, forcing first responders to either wait for long periods before communicating or to interrupt each other. Many public safety agencies have expressed concern that a shortage of public safety spectrum is coming,[11] even assuming they do get 24 MHz of television spectrum. If we respond to the shortage by simply allocating even more spectrum to public safety and using that spectrum inefficiently, then less spectrum is available for other purposes.

Dependability and Fault Tolerance: Critical pieces of the system should rarely fail. Of course, some failures are inevitable when a hurricane the size of Katrina hits, but this need not bring an entire system down. In a fault-tolerant design, other parts of the system will continue to operate and compensate for failures to the extent possible.

Advanced Capabilities: Today, public safety systems primarily provide voice services. There are many other services that could be useful, including broadband data transfers, real-time video, and geolocation, which would allow dispatchers to track the precise location of first responders during an emergency.

Security: Systems should be designed so hostile parties cannot easily attack the communications system or eavesdrop on first responders—even for interagency communications. Protecting interagency communications from eavesdroppers is a greater problem, because protection must run end to end, and the two agencies at each end of the conversation often have dissimilar technologies today.

Cost: Obviously the cost to build and operate public safety communications systems should be as low as possible.

Recent incremental efforts at reform have tended to address one problem at a time. For example, spectrum has been reallocated to address the problem of spectrum scarcity, with limited attention to interoperability. There are grant programs specifically intended to improve interoperability without consideration for spectrum efficiency, dependability, or the

9. NATIONAL TASK FORCE ON INTEROPERABILITY, WHY CAN'T WE TALK? 4 (2003), *available at* http://www.safecomprogram.gov/NR/rdonlyres/322B4367-265C-45FB-8EEA-BD0FEBDA95A8/0/Why_cant_we_talk_NTFI_Guide.pdf.

10. *See generally* Jon M. Peha, *How America's Fragmented Approach to Public Safety Wastes Money and Spectrum*, 33RD TELECOMM'S POL'Y RES. CONF. 2 (2005), http://web.si.umich.edu/tprc/papers/2005/438/Peha_Public_Safety_Communications_TPRC_2005.pdf.

11. *See* FCC REP. TO CONGRESS, *supra* note 5, at 16.

capabilities made possible by new technology. However, there are multiple problems that put lives at risk, and they are interrelated. Interoperability may be improved by deploying a piece of equipment for "translations" that will cause the entire system to fail if this one component fails, which makes the system less dependable. Interoperability can also be improved by boosting coverage areas and thereby consuming far more spectrum for the same communications.[12] Similarly, relieving scarcity by allocating more spectrum to public safety with little thought to standards could make interoperability failures even more common. Indeed, interoperability problems seem likely in the newly allocated spectrum if broadband applications are introduced without standardization, which is an open option under consideration.[13] The best way to improve systems is to address all objectives together rather than piecemeal.[14]

In the coming sections, we will review the four basic assumptions described in Part II.A and the impact of these assumptions on the criteria listed above.

D. Let Each Local Agency Decide: Flexibility Above All

As discussed in Part II.A, U.S. policy places responsibility for first responder communications systems primarily with local governments. From the perspective of the federal government, this is a policy of *flexibility*. The Federal Communications Commission ("FCC") gives public safety agencies the flexibility to decide how they will use their spectrum, while the Department of Homeland Security ("DHS") and the Department of Justice offer grants that give local agencies flexibility on how to spend the money. The advantages of local control are that local decisionmakers are able to match local resources (e.g., tax dollars) to the most pressing local needs. This is an important advantage in many contexts, but in this case, it comes at a high cost.

There is an inherent tradeoff between flexibility and interoperability. For example, a long-distance phone call typically passes through multiple

---

12. *See* Peha, *supra* note 10, at 7.

13. The Dev. of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Commc'n's Requirements Through the Year 2010, *Eighth Notice of Proposed Rulemaking,* 21 F.C.C.R. 3668, para. 30 (2006) [hereinafter Dev. of Operational Requirements].

14. Congress would be better able to consider the full range of issues for public safety communications rather than address these issues piecemeal if Congress had the capability to do detailed technology assessment studies, as discussed in Congressional testimony. *See Scientific and Technical Assessment and Advice for the U.S. Congress Before the House Science Committee*, 109th Cong. (2006) (testimony of Jon M. Peha, Professor of Engineering and Public Policy, Carnegie Mellon University), *available at* http://science.house.gov/commdocs/hearings/full06/July%2025/Peha.pdf.

telephone networks. There are no interoperability problems between Verizon customers and Qwest customers, even though multiple distinct systems are involved, because these companies have largely abandoned flexibility in favor of standardization and a consistent national (and global) architecture. On the other hand, U.S. policy gives each public safety agency the flexibility to choose technology quite unlike that of its neighbors. Thus, interoperability failures do not occur because public safety agencies have somehow failed to follow the American vision. These failures occur specifically because agencies are following that vision.

Flexibility also greatly reduces spectral efficiency. When engineers design a wireless communication system to cover a large area, they can maximize capacity and minimize spectrum use by carefully determining where each transmitter is located, which technology it uses, what area it covers, and which block of spectrum it uses. These techniques can conceivably increase spectral efficiency for public safety by orders of magnitude.[15] However, it is not possible to adopt this approach if each municipality makes decisions independently. Decisions to minimize spectrum use and to ensure seamless coverage must be made across large regions with many municipalities.

For example, according to a report published in 1996, public safety needs 95.3 MHz of additional spectrum by 2010.[16] Although it is a decade old, this is still the most widely cited estimate of spectrum needs for public safety. However, the authority issuing the report based its analysis on many assumptions, including a continuation of policies that promote the independence of each local agency. Had it instead assumed the kind of frequency reuse that can easily be achieved with modern technology when a single system is designed to cover a large region and kept all other assumptions the same, it would have estimated that public safety already had more than enough spectrum in 1995 to meet its needs in 2010.[17] This does not imply that public safety needs no new spectrum, but it does imply that the shortage may have more to do with ineffective public policy than with technical necessity.

Flexibility has the same impact on infrastructure cost. By designing fixed infrastructure across a large area, one can greatly reduce the amount of equipment needed, which is why regions with greater political fragmentation—i.e., more government units per square mile—end up deploying far more equipment. Indeed, the number of communications towers constructed today in a county depends more on the number of

15. *See* Peha, *supra* note 10, at 9.

16. PUB. SAFETY WIRELESS ADVISORY COMM., FINAL REP. TO THE FCC AND NTIA 53 (Sept. 11, 1996), http://ntiacsd.ntia.doc.gov/pubsafe/publications/PSWAC_AL.PDF.

17. Peha, *supra* note 10, at 10.

municipal governments in that county than on the county's population, size, or terrain.[18] Flexibility can also increase expenses for mobile handsets. For example, in many cities, fire trucks must carry many kinds of radios in the hope that at least one will work at every fire.

A regional or national plan would also make it much easier to design a system that is fault-tolerant, i.e., that can continue to operate even after a significant percentage of its transmitters fail. This is possible through planned redundancy and by designing the system to reconfigure after a failure to make optimal use of whatever devices are still operational. This kind of coordinated redundancy is unlikely to emerge when each local agency is responsible only for itself, but it could occur when systems are designed over large areas.

Finally, if all public safety agencies adopt the same technology, then when first responders from different agencies communicate, they would all still have access to the same security features such as encryption and authentication. Thus, these security features would work as well for interagency communications as they do for intra-agency communications.

E. Commercial Service Providers Need Not Apply

For the most part, first responders are served by public safety agencies and not commercial wireless service providers. This policy is generally justified by the fact that the requirements of first responders are more demanding than those of the general public, so commercial wireless service providers are unable to provide adequate services. More specifically, public safety needs coverage anywhere an emergency might occur and not just those regions with a high density of paying customers. Public safety needs systems that are highly dependable, which means it needs more backup transmitters, more backup power supplies, and more rugged handsets. Public safety also needs greater protection against criminals or terrorists who would deliberately take down the system. In many cases, commercial carriers do not provide these capabilities to the extent public safety might wish—at least not today.

Unfortunately, public safety systems do not always meet these same standards. Public safety systems also have holes in coverage. Components also fail in these systems where there are no backups. Consequently, commercial systems are sometimes used when public safety systems are inadequate. For example, after Hurricane Ivan hit Western Pennsylvania in 2004, flooding destroyed equipment at the Carnegie Fire Department, and the wireless system failed. First responders scrambled to fill the void so they could run search and rescue missions by signing up for service with

18. *Id*. at 6.

Nextel and Verizon, whose systems were fully operational around the city of Carnegie.[19] Unofficially, many police and firefighters routinely carry cellular phones as backup when the official system proves inadequate. They do this at their own expense. Thus, public safety does use commercial services from time to time but often without careful and systematic thought about how to do it well. It is clear that the chances of communicating during an emergency would be improved if first responders could use any system that is still operating after an emergency, regardless of whether this is a public safety system, a commercial system, a municipal Wi-Fi network, or anything else.

Note that while public safety has demanding needs for mission-critical real-time applications, much of public safety communication is not mission-critical, so failure is tolerable, or first responders can simply try again later. For example, police officers can benefit from filing reports from a laptop in their car,[20] but a temporary outage of this service is not life-threatening. Thus, commercial services or municipal Wi-Fi systems may be adequate as a secondary provider of communications services. Moreover, where public safety infrastructure offers only voice services, first responders can expand their capabilities through use of other systems. For example, this is why the Pittsburgh police use data services from a commercial cellular carrier to supplement their own voice-only communications system.

In addition to adding capabilities and improving dependability, use of other systems can sometimes reduce costs. The fact that public safety has its own systems and its own technologies ensures that public safety systems will be expensive, and innovation will be slow. The commercial market is much larger, which brings mass production and rigorous competition. This drives prices down and gives all parties incentive for continuous improvement.

But can a commercial wireless system be the primary provider of public safety communication systems? Today, probably not.[21] We should not be surprised if a commercial wireless carrier does not offer a service that meets the high standards for mission-critical communications. Smart shopkeepers do not stock products intended to appeal to people who have vowed never to enter their store. The real question is whether commercial carriers could serve public safety if policies changed. It is technically

19. Interview with C.K. Ruch, Chairman, Allegheny Mountain Rescue Group (Aug. 22, 2006) (on file with author).

20. Based on our analysis of use of wireless technology by the Pittsburgh Police Department, this application alone allows police officers to spend an additional two hours per week on patrol, which more than pays for the technology and its operation.

21. *See* FCC REP. TO CONGRESS, *supra* note 5, at para. 45.

possible to prioritize public safety traffic to guarantee that public safety will have capacity in an emergency. It is also technically possible to improve backup power supplies, coverage areas, and other attributes to meet the needs of public safety. Whether or not profit-seeking commercial carriers can do this for public safety without increasing the cost to serve commercial users is unclear, but policymakers should at least give commercial carriers the opportunity to try.

F. Public Safety Does Not Share

First responders generally communicate over infrastructure that is dedicated to public safety and over spectrum dedicated to public safety. This ensures that other kinds of traffic will not interfere. It is also probably necessary today, because when each public safety agency makes its own decisions, there is no single voice with sufficient authority to represent public safety agencies throughout a region when discussing the possibility of sharing either infrastructure or spectrum with some other entity.

Communications systems for public safety must have sufficient capacity for those unusual periods when there are major emergencies involving many first responders. However, much of the time, public safety systems carry little traffic—and even less traffic that is mission-critical.[22] Thus, the capacity is unused much of the time. If there were sharing, someone could use these idle resources, thereby increasing spectral efficiency and possibly decreasing costs.

There are two ways to share. One is to share infrastructure, i.e., with infrastructure that serves public safety and other users. As discussed in Part II.E, public safety must have priority, but much of the time, public safety's demands will be low.

It is also possible to share spectrum without sharing infrastructure.[23] Consider the case where there is one system for public safety and another for commercial cellular. Each system has its own spectrum, but there is a band in which either of them is capable of operating. Most of the time, the band is dedicated exclusively to the commercial carrier, but whenever there is a major emergency, the band is dedicated exclusively to public safety on a priority-in-use basis. For both systems, this is almost as good as having dedicated spectrum all the time. The principal disadvantage of this sharing arrangement is that during major emergencies, the commercial cellular

---

22. FCC SPECTRUM POL'Y TASK FORCE, REP. OF THE SPECTRUM EFFICIENCY WORKING GROUP 22 (Nov. 15, 2002), *available at* http://www.fcc.gov/sptf/files/SEWGFinalReport_1.pdf.

23. *See* Jon M. Peha, *Protecting Public Safety With Better Communications Systems*, IEEE COMMUNICATIONS MAGAZINE, Mar. 2005, *available at* http://www.comsoc.org/cil/Public/2005/Mar/cireg.html [hereinafter *Better Systems*].

system must rely on spectrum bands to which it has exclusive access, which will decrease cellular call completion rates during these emergencies.

More complex and dynamic forms of spectrum sharing are also possible.[24] For example, cognitive radio devices might sense whether public safety spectrum is in use, and the devices can then dynamically determine whether transmission is possible based on current usage. Alternatively, these secondary devices might explicitly coordinate with public safety devices. Such schemes require additional care to ensure that appropriate safety standards can be met, but they can also yield greater spectral efficiency.

G. Emphasis on Voice Communications

Military wireless systems and commercial cellular systems have added many new capabilities which have been slow to arrive in public safety systems. These capabilities include the ability to transfer images, video, and data files as well as location technology that allows devices to be tracked. The Safecom Program in the DHS has identified many applications of these capabilities that might prove useful to first responders.[25] Some of these applications are not mission-critical and can therefore be done over multipurpose public networks operating in unlicensed bands or through commercial services using privately licensed spectrum, but some are mission-critical at data rates that require broadband allocation of spectrum. For example, real-time high-quality video could allow doctors in a hospital to observe patients at a remote disaster and provide immediate advice to paramedics at the scene.

A spring 2006 FCC proceeding[26] focused on the possibility of using some of public safety's new 24 MHz allocation for broadband communications. Before these proceedings, the spectrum could be used only for narrowband voice communications and wideband[27] data

---

24. *See, e.g.*, Jon M. Peha, *Approaches to Spectrum Sharing*, IEEE COMMUNICATIONS MAGAZINE, Feb. 2005, *available at* http://www.comsoc.org/ci1/Public/2005/Feb/cireg.html; Jon M. Peha, *Competing Models for Spectrum Sharing*, NATIONAL ACADEMY OF SCIENCES, Feb. 28, 2006, http://www7.nationalacademies.org/cstb/ntia_peha.pdf; Joshua Marsh, *Secondary Markets in Non-Federal Public Safety Spectrum* (Sept. 2004), http://web.si.umich.edu/tprc/papers/2004/384/tprc.pdf; Jon M. Peha & Sooksan Panichpapiboon, *Real-Time Secondary Markets for Spectrum*, 28 TELECOMM'S POL'Y 603 (2004).

25. *See* SAFECOM PROGRAM, U.S. DEP'T OF HOMELAND SEC., STATEMENT OF REQUIREMENTS FOR PUB. SAFETY WIRELESS COMMC'N'S & INTEROPERABILITY, VERSION 1.1 (2006), *available at* http://www.npstc.org/documents/SRSoR_V11_030606.pdf [hereinafter SAFECOM COMMC'N'S & INTEROPERABILITY].

26. *See* Dev. of Operational Requirements, *supra* note 13.

27. Wideband is 150 kHz or less, as might be appropriate for data applications operating at much lower speeds than broadband.

communications. Broadband is needed to achieve high data rates, as might be needed for TV-quality video or the rapid exchange of mug shots. There has been little opposition to the idea of allowing broadband—at least in roughly half of the new public safety band—and this will probably allow the FCC to take a positive step away from the traditional emphasis on narrowband voice.

For some applications, the availability of interoperable broadband wireless is not sufficient. For example, if the doctors described above are in the Center for Disease Control ("CDC") a thousand miles from the disaster, then public safety agencies on both sides of the conversation must also be connected to a backbone network, probably wireline, that can provide adequate capacity and quality of service. Today, this is not always possible.

III. ALTERNATIVE VISIONS

The weaknesses discussed in Part II can only be addressed with a broadband network that was designed as national infrastructure and not as a loose concatenation of thousands of local systems. There are a number of ways to achieve this. In this Part, this Article discusses some alternative visions of what public safety infrastructure and policy might look like and some advantages and challenges associated with each vision. As discussed in Part II.E, it is possible that public safety might make use of multiple wireless communications systems. Thus, this Article begins with various options for a *primary* system, which would at minimum support mission-critical voice communications and possibly more. This Article then presents some alternatives for *secondary* systems, should any be used.

In all of these models, note that there need not be any connection between how the communications infrastructure is designed and run and how that infrastructure is used. Local public safety agencies are free to design their organizations, their emergency response procedures, and their cooperative relationships with other agencies in whatever manner maximizes effectiveness. (Such issues are beyond the scope of this Article.) A police chief can develop a strategy to fight crime in his jurisdiction without caring who keeps the police radios working, just as he does not care who supplies the department with electricity.

A. Primary Systems Run by Government Agencies

Today, primary public safety communications systems are designed and run by government agencies. As described in Part II.D, they are run by many thousands of independent local agencies; this leads to interoperability failures, inefficient use of spectrum, lower dependability, and higher costs. One obvious response is to continue to rely on government agencies but to move away from flexibility and toward standardization and a consistent

nationwide architecture defined by one or more federal agencies.

Even with a national architecture defined at the federal level, the federal government may or may not actually operate the infrastructure.[28] Certainly, one option is for a federal agency such as DHS to deploy and operate a nationwide system. The federal government would pay directly for the infrastructure—although not necessarily the mobile devices used by first responders that connect to this infrastructure. Another option is for local or regional entities to continue operating the systems, but systems must be designed to be a piece of the national system and consistent with the national architecture, as opposed to an autonomous system clumsily glued to its neighbors. This arrangement is not new. For example, the Internet consists of many thousands of independent networks under separate administrative control, all of which operate and cooperate using protocols and architectures approved by the Internet Engineering Task Force.[29] Similarly, there are many telephone companies around the world using consistent standardized technology.

There is already one government program to develop a nationwide wireless network explicitly for law enforcement and homeland security. This network will be developed by federal contractors under the direction of the Departments of Homeland Security, Justice, and Treasury.[30] This Integrated Wireless Network ("IWN") will support 80,000 federal agents and officers. Ironically, the IWN program was intended as a "cost avoidance measure" because its creators understood that a single network shared by these departments would be much cheaper than separate networks for each agency and would be consistent with the National Telecommunications and Information Administration's drive toward spectral efficiency.[31] However, the IWN program did not take the obvious next step toward cost-savings and spectral efficiency by supporting state and local first responders. Thus, tens of thousands of public safety agencies would continue to run their own networks. Even though the IWN will be available to only a few percent of first responders, i.e., those from federal agencies, the network must still cover the entire country. The program is expected to cost between $3 and $30 billion.[32]

---

28. *See Better Systems*, *supra* note 23.

29. *See* Internet Engineering Task Force, http://www.ietf.org (last visited Apr. 4, 2007).

30. *See* U.S. DEPARTMENT OF JUSTICE, Integrated Wireless Network, http://www.usdoj.gov/jmd/iwn (last visited Apr. 4, 2007).

31. *Public Safety Communications From 9/11 to Katrina: Critical Public Policy Lessons: Hearing Before the H. Comm. on Energy & Commerce*, 109th Cong. 71–73 (2005) (statement of Vance E. Hitch, Chief Information Officer, U.S. Department of Justice), *available at* http://www.access.gpo.gov/congress/house/pdf/109hrg/24252.pdf.

32. *See* Dizard, *supra* note 6.

One challenge with developing a nationwide system for all first responders is migrating from current systems without a disruption. This challenge becomes vastly simpler with the spectrum made available by the digital TV transition. We now have the opportunity to construct a nationwide system using some or all of that new spectrum and allow local agencies to gradually migrate from the current systems to the new one over a period of years.[33] As they abandon their outdated technology and old spectrum allocations, some of these bands could become available for other uses. There is also a bureaucratic challenge as federal and local agencies adjust their roles and their budgets.

B. Primary Systems Run By Commercial Wireless Carriers

An obvious way to serve first responders using commercial carriers is simply to seek service from today's cellular companies. This has advantages. Multiple networks are already operating in much (but not all) of the country, and competition between these carriers drives costs down and quality up. However, as discussed in Part II.E, today's systems would rarely meet public safety standards as the primary provider of mission-critical communications. Perhaps this would change if carriers were encouraged to bid for public safety business, but this remains to be seen.

An alternative is to seek bids for a new nationwide system that would be specifically designed to serve public safety and would be run by a commercial provider. Many European nations have adopted this approach, using the Terrestrial Trunked Radio ("TETRA") standard[34] defined by the European Telecommunications Standardization Institute ("ETSI") in 1995. For example, the British government has signed a contract with British Telecom, which will build a TETRA-based wireless system and operate that system for 19 years in return for £2.5 billion.[35] The system is intended for public safety even though it covers not just first responders but also other public service agencies and even community health centers. Thus, the U.K. gains the efficiency and dependability of a national system with no possibility of interoperability problems, all provided through the existing expertise of British Telecom.

---

33. *See* Jon. M. Peha, *The Digital TV Transition: A Chance to Enhance Public Safety and Improve Spectrum Auctions*, IEEE COMMUNICATIONS MAGAZINE, June 2006, *available at* http://www.ece.cmu.edu/~peha/DTV.pdf [hereinafter *The Digital TV Transition*].

34. TETRA, Terrestrial Trunked Radio, http://www.tetramou.com (last visited Apr. 4, 2007).

35. *See BT Wins its Biggest Ever Government Contract To Set Up Police Digital Radio Service,* PR NEWSWIRE, Mar. 8, 2000, http://www.prnewswire.co.uk/cgi/news/release?id=18823 [hereinafter *BT Wins Contract*].

Although details are still forthcoming, it appears that Verizon is making a similar proposal,[36] wherein Verizon would operate in 12 MHz of spectrum in the 700 MHz band that is currently intended for public safety after the digital television transition. Based on press reports to date, it appears that Verizon would serve public safety users only in return for a fee. No spectrum or infrastructure would be shared with users who are outside of public safety.

As discussed in Part II.F, public safety systems must be designed for peak demand, but public safety demand is usually far below peak. Thus, further efficiencies could be gained if a network serves both first responders and commercial users where the former have priority. Cyren Call,[37] a start-up run by Nextel founder Morgan O'Brien, has requested a no-bid grant of 30 MHz in the 700 MHz band to establish just such a network in the U.S. These 30 MHz would come from spectrum that Congress currently expects to be auctioned, probably for around $5 to $10 billion.[38] In a sense, this reallocation of spectrum represents an upfront investment by the federal government. (In the Cyren Call proposal, public safety would still get its 24 MHz of additional spectrum in the 700 MHz band.) The network itself would be built and operated by a number of commercial carriers operating in different regions while Cyren Call plays the role of network manager by setting service requirements, negotiating deals with equipment and service providers, overseeing compliance with requirements, and managing the flow of payments.

Public safety agencies would pay for services on this network much as consumers pay for cellular services today. As discussed in Part II.E, dual-use infrastructure can work well if meeting public safety's stricter requirements for coverage, dependability, and security does not make the system too costly for commercial users. For example, a system serving only public safety would naturally be designed to maximize coverage, but a company deriving much of its revenues from commercial users would focus on population centers. Cyren Call proposes to bring terrestrial wireless coverage to 99.3% of the U.S. population but only 63.5% of the nation's area (75% of the area within the contiguous U.S.). This may have value for urban areas, but clearly other solutions must be found for rural areas. (Cyren Call proposes satellite communications for these areas.)

---

36. *See* Jeffrey Silva & Heather Forsgren Weaver, *Industry Pitches Public-Safety Alternative,* RCR WIRELESS NEWS, Sept. 11, 2006.

37. *See* Reallocation of 30MHz of 700 MHz Spectrum (747-762/777-792 MHz) From Commercial Use, *Petition for Rulemaking*, at v (Apr. 27, 2006), *available at* http://www.cyrencall.com/downloads/CyrenCall_PetitionRulemaking.pdf [hereinafter *Cyren Petition*].

38. *See* Drew Clark, *Estimates Vary on Value of Spectrum*, NAT. J., Aug. 1, 2005, http://www.njtelecomupdate.com/lenya/telco/live/tb-UDUP1122927526162.html.

The biggest challenge when many public safety agencies are served by a single commercial company is ensuring that this company has incentive in perpetuity for providing outstanding services at reasonable prices. If the only choices for public safety are to pay whatever this company asks or to discontinue wireless communications for first responders, then public safety is in trouble. A traditional solution is to impose cost and quality regulation, as is done with utilities. It is not clear whether such regulation would deter commercial companies like Cyren Call and Verizon from entering this market. There are also other ways to mitigate this risk, such as the following:

Individual public safety agencies have little power to negotiate with a nationwide company. Thus, this task can be given to a single national entity such as a federal agency or national consortium that represents all public safety agencies in negotiations.

Contracts must clearly define performance standards across many criteria, including but not limited to dependability, security, coverage, and quality of service, so companies will not be rewarded for cutting corners.

Contracts could run for long periods so renewals can be negotiated well in advance. The 19-year contract in the U.K. is an example.[39] If a contract is not renewed, this leaves more time to create an alternative.

Public safety might not be required to pay for its last few years of service. If the contract is renewed, then payments continue without interruption. If not, the company must provide several years of services without payment, which increases the company's incentive to renew, and public safety can use the money it would have paid to prepare for whatever is next.

Still, the commercial company is in a stronger bargaining position than public safety entities, which is dangerous. This is especially true when the company serves both commercial and public safety users, as in the Cyren Call proposal, so the latter users can be lost with limited reduction in revenues. More extreme measures would make the company as dependent on public safety as public safety is dependent on the company. For example, it might be established when spectrum is assigned that if the company fails to negotiate a deal acceptable to public safety, then the spectrum license will be immediately revoked, even if 99% of the network's users are not associated with public safety. License renewal could also depend on input from DHS and other responsible public safety agencies. To go even further, the contract with public safety might require the company to surrender its infrastructure to the next contract winner if the negotiation fails. Similar measures have been proposed in the past for a

39. *See BT Wins Contract*, *supra* note 35.

highly subsidized telecommunications provider "of last resort" in rural areas. Under this arrangement, there is no risk that vital public safety infrastructure will become unavailable, because it can always be reassigned. The challenge here is giving the company adequate incentive to invest in infrastructure that it could lose someday. Again, this requires long-term contracts and early negotiations. For more information on how this can be done, see my comments in the recent FCC Proceedings.[40]

In return for provisions such as the above that protect public safety from monopoly service providers, government might offer provisions that protect commercial carriers from other risks. For example, the government might guarantee that payments from public safety will not fall below a given level, even during the transition period when many public safety agencies are not yet making use of the new network.

Commercial companies may also go bankrupt—especially new companies with innovative business plans. Contracts must also address this possibility so critical infrastructure will not be lost to public safety, and there will be no disruptions in service. This problem is not new. Companies that operate other forms of critical infrastructure do go bankrupt from time to time, so there are models to follow.

C. Secondary Systems

A variety of options are possible as secondary systems, assuming that the mission-critical voice communications are provided through a primary system. These possibilities are not mutually exclusive, so several could be adopted.

Cellular carriers: As discussed in Parts II.E and III.B, cellular carriers can compete to offer services to public safety, and if this is viewed as a secondary system, the diversity of networks available to public safety can greatly increase dependability and coverage, even if individual commercial networks do not always meet public safety's requirements. It can also bring new services, such as 3G data communications, where these are not offered by the primary system.

A nationwide commercial carrier: As with the Cyren Call and Verizon proposals, a commercial company could provide services to public safety across the nation, but on a secondary basis, focusing on services such as broadband that are not widely available today to public safety. One

40. *See* Jon M. Peha, *A New Proposal for a Commercially-Run Nationwide Broadband System Serving Public Safety*, Comments in the Matter of Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, Federal Communications Commission PS Docket No. 06-229 and WT Docket No. 96-86, Feb. 7, 2007, *available at* http://www.ece.cmu.edu/~peha/safety.html.

such proposal comes from M2Z Networks,[41] which has offered to provide free services to first responders in return for just 20 MHz of spectrum near 2.1 GHz, which is less valuable than spectrum in the 700 MHz band. (M2Z Networks also pledges to provide broadband services to most of the U.S. population and to pay 5% of their revenues to the U.S. Treasury.) Their network would cover 95% of the U.S. population, so presumably the percentage of area covered would be considerably less than the 63.5% proposed by Cyren Call.[42] Since the services are free, there is obviously no danger of M2Z Networks overcharging. However, it is still necessary to worry about whether public safety's service requirements will be met adequately and in perpetuity, as discussed in Part III.B.

Alternatively, there could be many regional commercial networks offering broadband services to public safety as a secondary provider. One recent proposal[43] would change the way spectrum is managed at 700 MHz to advance this approach. In this proposed bandplan, two 5.5 MHz blocks of spectrum would be adjacent, one for commercial license holders and one for public safety agencies. If the same broadband technology were deployed nationwide in both bands, then mobile devices that could operate in both bands would be cheaper. This could allow first responders to make use of commercial spectrum in addition to public safety spectrum during major emergencies. Of course, this level of harmonization would be very hard to achieve with tens of thousands of public safety agencies making their own decisions independently, and it would be even harder with multiple commercial license holders operating in this band in different parts of the country. This proposal also argues that a bidder for these commercial licenses should be given some form of preference if the bidder agrees to carry public safety traffic. The preference would be even greater if the bidder agrees to build out its network beyond the areas of greatest commercial profit and/or to enhance the network to meet public safety's stricter requirements.

Municipal infrastructure operating in unlicensed spectrum: More and more cities are creating or facilitating the creation of municipal multipurpose broadband wireless networks using Wi-Fi technology. Municipal systems that blanket a city with wireless broadband coverage, or just serve strategically placed hotspots, could play a useful role for public

41. *See* M2Z Networks, Inc., *Application for License and Authority to Provide National Broadband Radio Service in the 2155-2175 MHz Band*, at 1 (Sept. 1, 2006), http://www.m2znetworks.com/xres/uploads/documents/mz2-application.html (click "About the Application" and then click on "FCC Filings.").

42. *See Cyren Petition*, *supra* note 37, at 13.

43. Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, 71 Fed. Reg. 48,506–07 (Aug. 21, 2006).

safety. In some regions, this is already occurring.[44] These Wi-Fi-based municipal systems are relatively low-cost, provide high data rates, and can serve many needs including but not limited to public safety. While this technology's ability to completely cover a large region is currently not adequate for some mission-critical applications, it is fine for fixed applications like transferring data from a fixed surveillance camera to a remote command center, or for applications where lives do not depend on ubiquitous and instantaneous access, like transferring arrest reports from a police car back to the station. Many (but not all) of the broadband applications identified to date for public safety[45] could be accommodated in this way using currently available technology.

Ad hoc networks: Ad hoc networks are ideally suited for applications where all devices are mobile or are transported to an emergency as needed. These systems have little or no fixed infrastructure and must automatically self-configure to form a functional network. For example, such networks might be set up quickly among portable devices placed in a burning building or between police cars that are traveling at 90 miles per hour.[46] This is also an effective solution where much of the communication is local, e.g., to allow public safety devices operating within an urban subway system to communicate with each other at high data rates. These networks could operate effectively in unlicensed bands or in the 4940-4990 MHz band allocated to public safety. The former would be far less expensive because it would be possible to use off-the-shelf mass-produced components. Consequently, this is probably the appropriate choice with the many applications for which current commercial technology is adequate. The latter has the advantage of being largely free from congestion because it is available only to public safety. Thus, there may be cases where this is preferable.

Satellite networks: Satellite systems are outstanding resources because they cover vast regions, and they are immune from earthquakes, hurricanes, and most terrorist attacks. Thus, they may play an important role in sparsely populated areas where terrestrial coverage can be expensive or in areas where terrestrial systems have been destroyed by a recent disaster.[47] However, they are generally not the first choice where good

---

44. *See* Naveen Lakshmipathy, *Wireless Public Safety Data Networks Operating on Unlicensed Airwaves: Overview and Profiles,* NEW AMERICA FOUND., Feb. 21, 2006, http://www.newamerica.net/files/archive/Doc_File_2633_1.pdf.

45. SAFECOM COMMC'N'S & INTEROPERABILITY, *supra* note 25.

46. Carnegie Mellon University has already constructed ad hoc wireless systems with each of these two environments in mind: in cars and at the site of an emergency.

47. *See, e.g.*, Dale Hatfield & Phil Weiser, *Toward a Next Generation Strategy: Learning From Katrina and Taking Advantage of New Technologies*, MOBILE SATELLITE VENTURES, 2005, *available at* https:// www.msvlp.com/news_docs/papers/NextGenOct21R

terrestrial options are available. The time it takes a signal to travel to a satellite and back is inherently problematic for some applications, including basic voice communications. Today's mobile satellite devices tend to be more expensive, larger, heavier, and more power-hungry than their terrestrial counterparts, which makes the satellite devices less attractive for many first responders. (These are important issues for those proposed multipurpose networks that would use satellites in rural areas where commercial services would not be profitable, as in the Cyren Call approach.)

IV. ENSURING THAT LOCAL AGENCIES ARE WELL SERVED

Although improving public safety communications requires shifting technical design decisions from local agencies to a regional or national entity, we must remember that the objective is to serve local public safety agencies. These agencies must play an important role in defining requirements for the communications systems of the future and in ensuring a safe transition. This Part discusses why public safety agencies might have reason to oppose the reforms proposed in this Article and how to address these agencies' legitimate concerns.

Today, local agencies often embrace some or all of the traditional assumptions discussed in Part II.A. These agencies do so for very good reasons. Current U.S. policy would punish decisionmakers for moving in the right direction. Consider the challenges facing the person handling communications decisions for a municipal police department. His job is to provide the best communications services he can for local police officers, while spending as little of the department's limited budget as possible. Should he invest in infrastructure that will allow his department to aid a neighboring town if they experience an outage? Should he make criminal records available to neighboring police departments over a costly broadband network at his department's expense? Such actions may benefit other municipalities in the region, but any benefits to his agency are not sufficient to justify the costs. Spending money to serve the region rather than his own agency could even constitute a serious dereliction of duty.

He also has reason to avoid excessive reliance on commercial services. As discussed in Part III.B, commercial carriers today may not design services to meet public safety needs, but even when they do, a lone public safety agency has no control over how those services will change over time. For example, some police departments used commercial CDPD[48] services for low-speed data transmission. When the carriers

2.pdf.

48. CDPD is cellular digital packet data, the first generation of data services offered by many cellular companies.

switched from CDPD to a higher speed CDMA service-based[49] system, some of these departments were unprepared to upgrade their equipment. A carrier might have been willing to help a large customer make this transition, at least by giving advanced warning if not by providing support for legacy equipment, but the carriers have little incentive to do this for a single public safety agency.

This police department has even less reason to share spectrum, no matter how much this would increase spectral efficiency, if the department can get an exclusive allocation of spectrum. After all, spectrum is free to a police department. It always makes sense for this department to hoard as much as it can. If it doesn't need the spectrum this year, perhaps it will someday. This may reduce the amount of spectrum available to others, but that is someone else's concern.

Finally, many public safety agencies have good reason to rely on whatever technology their favorite vendor provides without demanding more. Most public safety agencies are small: 75% support 50 users or fewer.[50] Their small staffs need to focus on their core missions, like fighting crime or fires. This leaves little time to develop experts in communications technology, so these agencies naturally rely heavily on vendor representatives.

Unless they have adequate support, we should expect some public safety agencies to oppose fundamental reform. For better or worse, they have a system in place. They will be concerned that reform could bring significant costs, which city governments are unlikely to underwrite at budget time. They will be concerned that reform could come with risks of communications failure that are beyond their control, possibly interfering with their ability to respond to an emergency. The technical experts supplied by the vendors of current systems will favor the status quo. Experience has also taught state and local public safety agencies to be cautious about relying on federal assistance, which has tended to wax and wane over time.

These above concerns can and must be addressed. Assurances begin with a clear division between federal and local functions that aligns responsibility with authority and prevents the finger pointing among federal, state, and local agencies that we saw after Hurricane Katrina. In particular, a federal entity would be responsible for providing communications services to first responders and for the consequences when

49. CDMA is code division multiple access, a technique used to multiplex data streams.

50. Booz, Allen & Hamilton, *Cost Study Data Characterization Report*, PUB. SAFETY WIRELESS NETWORK, III-2, Feb. 8 1999, *available at* http://www.safecomprogram.gov/NR/rdonlyres/5EBE930C-47D9-49E1-A16E-27B1183798B2/0/Cost_Study_Data_Characterization_Report.pdf.

these systems fail, but this federal entity would not be responsible for how those services are used. Local agencies would maintain authority to protect the public using these services and responsibility for successes and failures. This may alleviate a fire chief's fears that he will lose control over his department by relying on communications infrastructure not operated by his own staff.

As discussed in Part III, this federal entity could be a federal agency that provides service directly, or it might simply be the agent that negotiates on behalf of public safety with commercial service providers. Since it represents many public safety agencies, it would be a large customer that no commercial company could ignore. It could provide coherent centralized management of spectrum and a technical support staff that serves local agencies better than the commercial vendors do today.

Clear responsibility and authority are important, but it is funding that will determine success or failure. City budgets are limited. Local agencies will participate when they are convinced that they can then reallocate funds and staff time for other purposes. The effectiveness of this approach has been demonstrated in moves toward regional consolidation of some 911 call centers; local public safety agencies typically participate if and only if it is clear that participation will yield significant cost savings.[51] When the transition is complete, local agencies should still be responsible for purchasing the devices that first responders carry to emergencies, but they would no longer have to pay all the costs of building and operating transmission towers for wireless communications or the broadband wired backbone that ties these wireless systems together. In the balkanized system of today, these costs are considerable, but they would be much smaller in the future. Moreover, these costs to the federal entity could be offset by freeing up spectrum through tremendous gains in spectral efficiency.

During the transition period, the federal government probably has to play an even larger role. It should underwrite some of the costs of the transition, including subsidizing the purchase of mobile handsets for the new system so older devices can be retired early. This will relieve state and local agencies of these costs, which may deter participation. At the same time, the federal government would stop providing the grants and spectrum that merely enable local agencies to prop up the old infrastructure. Local agencies that choose autonomy over the many benefits of regional planning and standardization will have to do so entirely on their city budgets.

---

51. The call center in Allegheny County, Pennsylvania is a good example. *See* Timothy McNulty, *City Urged: OK 911 Merger-Recovery Team Touts Advantages*, PITTSBURGH POST-GAZETTE, Mar. 3, 2004, at A9.

Another legitimate concern of public safety is that a federal entity will impose a solution without listening to those they will serve. Local public safety agencies must have a voice to state their own needs and preferences. Moreover, there is much to learn from those agencies that have been developing innovative approaches. For example, the greater Washington, D.C. area, which includes public safety agencies in the District of Columbia, Virginia, and Maryland, has made significant progress on a sophisticated regional system.[52] Experienced staff from local public safety agencies must participate in the process of defining a new system. Some should simply be hired by the federal entity. Others should act as representatives of all local public safety agencies, although generally not as an advocate for one particular agency, as this reinforces today's balkanized approach. National organizations representing public safety can play an important role here.

V. NEXT STEPS TOWARD A MORE EFFECTIVE POLICY

In a December 2005 report to Congress,[53] the FCC correctly concluded that first responders would benefit from a nationwide broadband network. The digital TV transition affords us an historic opportunity to establish this network. However, without a policy change, this opportunity will be lost. In this Part, we discuss how to move forward.

The initial focus should be on establishing a nationwide broadband network for data services that are not widely available to public safety today. Each agency can later migrate voice communications over to the new system when the agency is ready, yielding a gradual transition that never leaves first responders without service. After the migration is complete, outdated equipment operating in other bands can be discarded, and existing spectrum allocations can be released for other uses. Thus, providing public safety with spectrum and the ability to use it more efficiently today can free other spectrum in the future to be auctioned for licensed use or made available for unlicensed use. This might also make it possible to release public safety allocations in TV channels 14 to 20.

If this nationwide broadband system is to be run by a commercial company, a number of complex issues must be worked out with players like Cyren Call, Verizon, M2Z Networks, and others who may come forward. If the system is to be run by government entities, policymakers could begin the process today. This latter process is essentially the same

52. *See* Robert LeGrande II, Deputy Chief Tech. Officer, Gov't of D.C., Presentation at the New America Foundation (Oct. 26, 2006), *available at* http://www.newamerica.net/files/Robert%20LeGrande%20Presentation%20Slides.pdf (slides), http://www.newamerica.net/events/2006/from_tv_to_public_safety (video).

53. FCC REP. TO CONGRESS, *supra* note 5, at para 2.

regardless of whether the network will ultimately be run by one federal entity or a collection of local or regional entities. I recommend that policymakers pursue both paths in parallel.

The first step is to establish the technology and architecture for a nationwide broadband network that will meet the long-term needs of public safety. Both the FCC and DHS would presumably have roles to play in this process, with plenty of input from public safety organizations, equipment manufacturers, wireless service providers, and other stakeholders, as well as more objective researchers. The process itself should resemble the development of an open technical standard more than it resembles either the typical rulemaking of a regulatory body or the opaque pronouncements that are possible for an executive branch agency. The typical standards process allows technical input from all participants and healthy debate where technical differences exist. Ultimately, architecture should be adopted based on open standards for which no entity (other than the federal government) owns intellectual property. It would include a broadband backbone, which is likely to be based on the versatile Internet Protocol ("IP") and standards for wireless communications. It would incorporate gateways to legacy public safety systems, as well as potential secondary systems such as commercial cellular carriers, municipal Wi-Fi systems, ad hoc networks, and satellite systems. Use of these secondary systems may allow the primary system to operate with less spectrum in the 700 MHz band.

Given the stakes of such a fundamental shift in public safety infrastructure, the process should allow time to consider a variety of current and emerging technical options and to seriously investigate the long-term implications of each. Thus, funds should be provided to agencies like the Homeland Security Advanced Research Projects Agency ("HSARPA"), the National Science Foundation, and perhaps the Defense Advanced Research Projects Agency ("DARPA") specifically to engage forward-looking researchers outside of government in this process, much as DARPA has been used to consider major shifts in technology for military use.

It is also time to reevaluate the IWN program. There is no reason to invest billions of taxpayer dollars in a network that serves only federal first responders when the vast majority of first responders work for state and local agencies. One possibility is to greatly expand this program such that the IWN supports all first responders, presumably in federal spectrum instead of the 700 MHz band. If this vast change in scope is not practical, then the IWN should be shelved, so that the funding intended for IWN can be spent on a more complete solution to the problems of communications for public safety and homeland security.

Assuming that new infrastructure is needed, and it will be government-run, the next step is to design and build a nationwide network in the 700 MHz band based on the above architecture. The FCC must allocate spectrum from the 700 MHz band to public safety for this purpose. This need not increase the total amount of spectrum going to public safety, but it does mean that the FCC must abandon the policy of granting local public safety agencies maximal flexibility regarding use of spectrum at 700 MHz. This implies that none of the current bandplan proposals before the FCC can be adopted.

Federal funding will also be needed for construction of this nationwide public safety infrastructure, although much or all of the funding for the mobile devices held by first responders might eventually come from local agencies. In the long run, the taxpayer dollars saved by an efficient system should be far greater than those spent, but not during the initial transition period. One possible source of funds is auction revenues from the TV spectrum that will be allocated for commercial use. Some have estimated the value of 60 MHz of this spectrum at between $20 and $28 billion, but the Congressional Budget Office scores it at $10 billion.[54] As I have previously proposed,[55] simply by ensuring that any auction revenues beyond the $10 billion projection ("score") by the Congressional Budget Office be earmarked for a nationwide public safety system operating in the 700 MHz band, it might be possible to raise well over $10 billion without affecting current budget projections. However, this is just one of many options. Despite some of the rhetoric on this topic, there is no legitimate reason that Congress can only pay for critical public safety infrastructure from spectrum auction revenues. This is simply a useful accounting trick to make it appear that the infrastructure costs nothing. Surely in the age of terrorist threats on American soil, policymakers need no such excuses to spend money that will advance homeland security and public safety, especially when the short-term expenditures will lead to long-term savings.

In parallel with the path toward a government-run nationwide infrastructure, we must seriously consider the proposals of Cyren Call, M2Z Networks, Verizon, and perhaps others to come. A commercial public safety network may have the potential for greater benefits than a government-run system. This is especially true if the network also serves users outside public safety, so the system can be put to good use between emergencies, leading to much greater efficiencies in the use of expensive infrastructure and the use of scarce spectrum. However, a commercial system also carries greater challenges and risks. In particular, we can only

54. Clark, *supra* note 38.
55. *The Digital TV Transition*, *supra* note 33.

rely on commercial companies if we can ensure that public safety's requirements will be met, including requirements for coverage, dependability, and security, and that requirements and fees can safely evolve over time as technology and needs change. Commercial companies will have strong incentives to cut costs and raise prices where they can, and public safety may be in a poor position to negotiate. Moreover, commercial companies who hope to derive their profits from paid subscribers will naturally try to avoid serving sparsely populated areas. This is why the current Cyren Call proposal would provide terrestrial service to only 63.5% of the U.S.,[56] and rival proposals may serve even less. As discussed in Part III.B, the provisions that offer the greatest protection to public safety may also deter commercial companies from participating. It is not clear yet whether these issues can be resolved to the satisfaction of all. None of the proposals to date are sufficiently specific to address these issues. Since the risks and rewards of this approach are both great, more detailed consideration of these proposals is warranted. For more detailed discussion on how to bring companies to the table to discuss this approach without putting vital spectrum resources at risk, see my recent comments to the FCC.[57]

Regardless of whether public safety's new nationwide network is operated by the government or a commercial company, if it serves only public safety, then the spectrum allocated to this network will sit idle much of the time. In this case, the spectrum should be shared with another user who would have secondary access. Given that public safety would not need the spectrum often, secondary rights might be auctioned for almost as much as dedicated spectrum. Thus, for example, if public safety had exclusive access to 12 MHz and primary access to 24 MHz that is shared with commercial systems, then this might be far better for both public safety and commercial users than giving public safety exclusive access to just 24 MHz. This could also generate greater auction revenues. Alternatively, the underutilized spectrum could be opened for limited sharing with unlicensed cognitive radios with coexistence rules carefully defined to protect public safety from harmful interference.

Since commercial carriers could play a more important role for public safety, either as primary or secondary service providers, we should adopt policies that would increase their dependability. As I proposed in an earlier article,[58] policymakers should first provide market incentives for carriers to be more dependable. Carriers are rewarded for investing in better service

56. *See Cyren Petition*, *supra* note 37, at 13.

57. Peha, *supra* note 40.

58. Jon M. Peha, *Communication Challenges After the Hurricane*, WASH. POST, Sept. 15, 2005, at A32.

only if customers are willing to pay more as a result. Today, customers cannot know which carrier provides the most dependable service, with or without a major disaster, so no one will pay more for a dependable service. If the FCC released annual report cards on each commercial carrier's dependability and security, then the carriers might have incentive to compete with their rivals to be more dependable and secure. If we later come to view these carriers as critical infrastructure, policymakers should take the additional step of increasing their priority with respect to power restoration after a disaster.

VI. SUMMARY

American policies on communications systems for public safety have evolved over many decades, and those policies have outlived their usefulness. In particular, the U.S. system is based on assumptions that local agencies should have maximum flexibility at the expense of standardization and regional planning, that commercial carriers have little role to play, that public safety should not share spectrum or infrastructure, and that narrowband voice applications should dominate. These policies have led to a system that fails too often, costs too much, consumes too much spectrum, and provides too few capabilities. Moreover, public safety requirements have changed since 9/11, and the technology has changed as well, so there are many reasons to consider a fundamental change in policy.

Some will argue that we cannot afford the cost of a change in policy. In fact, the current policies are so wasteful that a policy change could easily reduce the cost of public safety communications infrastructure in the long term, in addition to saving lives and saving spectrum.

The digital television transition will provide a new block of prime spectrum, where new forward-looking policies and more effective technologies can prevail. Some or all of this spectrum could be the home of a new nationwide system built on open standards and a consistent architecture. This system could be run by the federal government, a coordinated confederation of state and local government agencies, or by a commercial carrier. All of these options have significant advantages over the current approach. Assigning this responsibility to a commercial carrier offers the potential for greater efficiencies, but only if we find long-term solutions to some important challenges. A nationwide public safety system run by and for government has the advantage of being lower risk.

There are steps we can and should be taking today to move toward this nationwide system. This includes either expanding IWN to meet the needs of state and local first responders or shifting IWN funding and spectrum elsewhere—funding efforts inside and outside of government to develop an appropriate architecture for a nationwide public safety network

based on open standards, raising funds to pay for the transition to a new nationwide system that is based on this architecture, and publicly evaluating proposals from commercial service providers to determine whether they can operate a network that would meet the long-term needs of public safety.

We must also change the way TV spectrum will be used for public safety. More specifically, for the 700 MHz band, we must abandon policies that allow each public safety agency to make technical choices that are incompatible with its neighbors. Thus, flexibility should be replaced by standardization and regional or national planning. Some of the newly allocated spectrum could also be shared between public safety and other users. This can be done in a manner that gives public safety ample capacity when emergencies hit but makes valuable spectrum useful for other purposes the rest of the time. This approach may even raise additional funds through auctions that could be used to build a new national public safety communications infrastructure.

Even as the role of federal government expands, we must ensure that state and local public safety agencies have a voice. Most importantly, the federal government must pay the cost of the transition rather than forcing local governments to do so, thereby giving local public safety agencies strong incentive to participate. Moreover, the role of federal government must be limited and clearly defined, so that local agencies can welcome support on communications infrastructure without fearing a complete loss of autonomy.

This is also an appropriate time to consider how commercial carriers, broadband networks operating in unlicensed spectrum, and satellites can be used as secondary providers to public safety. A growing number of municipalities and counties already operate multi-use networks that include pervasive mobile data connectivity to police, fire, emergency response, utility, and other public safety-related services. While none of these secondary systems will operate in the 700 MHz band, their inclusion may affect the architecture of the public safety's nationwide broadband network. Moreover, it might be possible to reduce the amount of dedicated spectrum allocated to public safety and also improve dependability, reduce equipment costs, and introduce valuable new capabilities by making effective use of secondary systems.

Some will complain that the steps discussed in this Article will take too long. It would certainly be better if there were a quick fix, but we have been spending time and money on quick fixes for years with little effect. More than five years have passed since 9/11, and there are still failed, ineffective policies. It is time to start the process of meaningful reform to meet truly long-term needs for public safety and homeland security.