Hearing on
The 700 MHz Auction: Public Safety and Competition

Statement of
Philip J. Weiser
Professor of Law and Telecommunications
Executive Director of the Silicon Flatirons Program
University of Colorado

Before the
U.S. Senate Committee on Commerce, Science and Transportation
US Congress

June 14, 2007

EXECUTIVE SUMMARY

The upcoming 700 MHz auction promises to provide public safety agencies with access to new wireless networks that will both facilitate greater levels of interoperability and next generation network functionalities. With respect to this opportunity, I emphasize three points: (1) the emerging new policy strategy to facilitate the development of next generation networks for public safety is far superior to the traditional model; (2) the linchpin of a new model—the concept of a public safety spectrum licensee—must be implemented with a number of safeguards to be effective; and (3) there will be a difficult transition period necessary to migrate from the old model of public safety communications to the new one.

In short, the old policy model for public safety communications leads public safety agencies to use antiquated equipment, makes it more difficult to facilitate interoperability, and is at odds with spurring the development and deployment of a next generation network. For public safety agencies to enjoy the type of less expensive and more powerful equipment routinely used by most American companies and the military, they need to adapt commercially developed equipment to meet their own requirements. Similarly, rather than seek to use only spectrum dedicated to public safety, public safety agencies should embrace the opportunity to share spectrum with a commercial (or more than one commercial) partner, thereby enabling greater spectrum efficiencies and subsidizing a next generation network buildout.

To spur the development of a next generation network model, the FCC has wisely introduced the concept of a public safety spectrum licensee that would control a nationwide 12 MHz license to be used to develop and deploy a next generation network based on broadband technology. This policy innovation promises considerable benefits to public safety, provided that the licensee is able to negotiate an effective framework with a commercial partner. To ensure that such a partnership is an effective one, can adapt to changing circumstances, and deliver its promised benefits, the licensee will need to rely on highly qualified advisors and a legal framework that protects its prerogatives as well as enables it to ensure that its partner follow through on its promises.

Finally, I want to close by emphasizing that, even with the right supportive policies in place, the transition to a new technological architecture for public safety communications will be quite challenging. As a starting point of bringing them on board, local agencies absolutely must have a voice in how the next generation network will operate and they should be empowered to operate virtual private networks along the lines of those used in corporate America. In any event, the development and deployment of a next generation network must take place at higher levels—i.e., it cannot and should not be operated locally. This paradigm shift will require a culture change from the mindset of where local agencies actually owned and controlled communications networks to one where they become smart users of them. I recognize that this shift will not happen overnight and it will take considerable political leadership at all levels of government to ensure that it happens at all.

In conclusion, my bottom line is that the old culture of public safety communications is ill-suited to supporting the development of modern networks and thus the only question for policymakers is whether this paradigm shift will occur sooner or later. For the sake of all of those involved in emergency response and all of us who depend on first responders, I hope this transformation happens sooner.

I. Introduction

Thank you Mr. Chairman, Senator Stevens, and members of this Committee for the opportunity to testify on the important public policy challenge of ensuring that the upcoming 700 MHz auction and related policy initiatives facilitate the development and deployment of advanced communications technologies for use by public safety agencies. I approach this issue from the standpoint of my position as a professor of law and telecommunications at the University of Colorado, where I also serve as the Executive Director of the Silicon Flatirons Program. More particularly, my testimony reflects my intense research focus on this issue over the past year, during which I authored a report for the Aspen Institute, wrote an article recently published in the Federal Communications Law Journal, and co-authored a report informed by a roundtable recently sponsored by CTIA-The Wireless Association.[1] My testimony today, however, reflects solely my own views and any recommendations I offer should not be ascribed to any of the entities I have worked with on this issue.

In my remarks today, I will focus on four themes that merit particular attention as this Committee and the Federal Communications Commission wrap up their important work related to public safety communications and the upcoming 700 MHz auction. *First,* I will discuss the need for a national public safety entity to manage a block of spectrum (i.e., "a public safety spectrum licensee") to promote the rollout of a wireless broadband network to support the use of advanced information and communications technologies by public safety. *Second,* I will address the concept of a shared public safety/commercial wireless network, explaining the powerful logic behind this proposal both with regard to enabling public safety agencies to use advanced technologies and in promoting spectral efficiency. *Third,* I will discuss the issues of governance and enforcement that must be addressed in order to make a public safety spectrum licensee model a success. *Fourth,* I will emphasize the importance of moving forward quickly with the auction, managing expectations, supporting ongoing innovation in this area, and not letting the

perfect be the enemy of the good. In short, promoting the development and widespread deployment of an advanced communications infrastructure for use by public safety is critically important, difficult, and likely to take some time. Before I develop these themes, however, I will begin by detailing some important background information.

II. Background

For many years, the development of communications infrastructure for public safety agencies remained largely an afterthought in telecommunications policy. This reflected the conventional wisdom that local public safety agencies should be assigned specific blocks of spectrum and use that spectrum to operate their own wireless telecommunications networks. This policy was arguably a sensible one when public safety agencies were among the relatively few established entities that operated wireless networks. Over the last several years, however, two distinct concerns have arisen as to the state of public safety communications: (1) different agencies cannot communicate with one another using their legacy equipment; and (2) advanced communications technologies increasingly being offered by commercial wireless providers are not available to public safety agencies. I will address each point in turn.

A. The Traditional Interoperability Concern

The concerns related to the inability of public safety agencies to communicate with one another reflects the continuing lack of interoperability between many legacy public safety radio systems. In general, legacy radio systems are engineered to meet specific requirements articulated by public safety agencies—such as a very quick call setup time to enable communication during "shoot-don't shoot" situations, effective talk group functionality, and "talk-around" capability. Radio systems manufactured to meet these specifications, however, are produced solely for public safety agencies, often rely on proprietary technology, and are generally quite expensive. Consequently, if one public safety agency adopts a particular system and another public safety agency adopts a different system, there often is no easy way for the two systems to communicate with one another. As you all appreciate, this lack of interoperability can be at best challenging (by making communication between different first responders difficult or impossible) or at worst tragic (as in the case of 9/11 when lives were lost because messages were not relayed between different agencies).

The often touted solution for addressing the lack of interoperability between public safety radio systems is that all public safety agencies should purchase new equipment that can enable them to talk to one another. Under this strategy, local agencies would all purchase new equipment and operate that equipment using the same spectrum bands. Indeed, the Project 25 initiative rests on this vision, as it aimed to develop an open standard for digital trunked radio systems that would enable agencies to cooperate with one another, share spectrum between them, and, ideally, enjoy interoperable communications across jurisdictions. As a recent GAO report detailed, however, the Project 25 initiative has failed to deliver on its promise, largely because the relevant standards never facilitated a more competitive market in equipment.[2] Stated simply, "the Project 25 [initiative] made the mistake of treating public safety communications as a distinct island, giving rise to proprietary technologies that are not compatible with commercially developed (and far cheaper) alternatives."[3] Finally, Project 25 radios are

designed to support narrowband voice communications, but not broadband communications that can enable public safety agencies to gain access to useful information and communicate more effectively.

A second interoperability solution is the use of gateways that use Internet Protocol technology to connect otherwise incompatible systems. Such gateway solutions are considerably cheaper than purchasing new Project 25 radios for a particular area, but they do not necessarily enable as effective or efficient communications as direct radio connections. Nonetheless, as a cost effective method of enabling different agencies to communicate at all (which is often what is needed), such solutions are quite promising and continue to improve in terms of their level of functionality.

A third interoperability solution is for agencies to adopt new wireless broadband systems that enable them to use Internet-based communications (such as voice over Internet Protocol) that can communicate directly to other agencies equipped with broadband systems or indirectly through gateways solutions (such as those described above). Unlike the Project 25 model, the purchase of wireless broadband systems is relatively inexpensive (as they rely on commercially marketed products) and can support an array of applications other than voice communications. Like the gateway solution, however, the use of interoperability at the Internet layer—i.e., voice over IP connections—does not provide the same level of operability (at least using today's technology) as traditional dispatch systems. But again, in many situations, such as the often cited failings at the Columbine tragedy, 9/11, and the aftermath of Hurricane Katrina, the critical problem was an inability to communicate at all, not an inability to communicate at the required call setup times that public safety agencies sometimes need.

The case for promoting wireless broadband and advanced information and communications technologies is not merely that it constitutes a potential interoperability solution. Rather, such technologies can enable public safety agencies to operate more efficiently and effectively. Indeed, such technologies are increasingly a source of important efficiencies in the hands of corporate America and the military—think of how FedEx tracks packages or how Walmart tracks its inventory—and there is every reason to believe that advanced information and communications technologies can empower public safety agencies in numerous ways. The challenge, however, is to develop a policy strategy to promote the development of a next generation network for public safety agencies.

Before I discuss the opportunities created by and the strategy necessary to develop next generation networks for public safety, let me emphasize two sobering points about the above discussion. First, it is important to appreciate that the need for short term interoperability solutions—such as the gateway model—will not disappear once we embark on the road toward a next generation network. Second, the next generation network will not, at least in the reasonably near term, function as a replacement for the traditional public safety dispatch systems. Rather, over at least the next decade (while a next generation network is developed, deployed, and proven out as sufficient to meet the requirements of public safety), it is likely that public safety agencies will need to support *both* their traditional dispatch systems and a next generation system. Among other things, this means that the funding needs of public safety agencies with respect to information and communications technologies are likely to increase in the near term.

B. A Next Generation Network Architecture

During my initial exposure to the issue of how to develop a next generation network for public safety, the conventional wisdom was that public safety agencies would never face up to a challenging cultural shift as to how public safety communications should operate. In particular, the prevailing wisdom was that public safety agencies would always insist on operating their own networks and would never accept an architecture that would call for the sharing of spectrum between public safety and commercial services. In my experience, however, a number of public safety officials have led the way in embracing the logic behind the move to a new technological architecture and a new policy strategy to deliver next generation network services to public safety agencies. For that progressive vision, I applaud their leadership and willingness to break from the old model.

The increasing interest in a policy strategy to promote next generation networks for public safety reflects the realization that broadband networks are critical to the future of public safety communications and the services now available to corporate America should be adapted to meet their needs. As one public safety official put it, "[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."[4] The public policy challenge is how to facilitate the emergence of this future.

To spur the development of broadband networks, it is reasonably clear that the old model of networks operated and used solely by public safety agencies themselves is inefficient and unsustainable. That model, which was borne of necessity in an era where there were no suitable commercial wireless services, ignores a powerful case for using spectrum more efficiently. After all, public safety agencies use spectrum intensely at particular moments, but often use their spectrum on a limited basis. Consequently, the ability to share spectrum between a public safety entity and other customers can ensure that the network and spectrum is used more efficiently.

On a practical level, it makes sense to develop and operate broadband infrastructure for public safety in concert with other providers. After all, we do not expect public safety agencies to manufacture their own uniforms or cars. As with uniforms and cars, it is not difficult to develop next generation technologies that can be adapted to the needs of public safety. The advantage of relying on commercial technologies is that public safety agencies will be able to benefit from commercial economies of scale and purchase equipment far more economically than they have been able to with respect to their traditional dispatch networks. Consider, for example, that "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."[5]

The bottom line in terms of the policy strategy for next generation networks for public safety is that the traditional approach for supporting public safety communications will not work effectively. Consequently, policymakers need to appreciate that our nation's effort to develop next generation networks for public safety agencies will turn on our ability to spur a new model of governance, new cultural mindsets amongst the relevant stakeholders, and new funding models to support a new technological architecture. As I will emphasize in closing, these are

difficult transitions and policymakers should both be vigilant in prodding them forward as well as understanding that they will not take place overnight.

III. The Importance of A National Public Safety Spectrum Licensee

The Federal Communications Commission initially assumed that the traditional policy model would govern the use of the 700 MHz spectrum dedicated to public safety. In particular, the vision animating early discussions of how the spectrum would be used assumed that agencies would purchase new systems, such as Project 25 radios, and operate them at the same frequencies. Over the last several years, however, it has become clear that this solution is neither cost effective nor would it enable public safety agencies to use advanced broadband technologies. Indeed, this model is often associated with the "narrowbanding" concept that is antithetical to the development of broadband networks.

Over the last year, the Federal Communications Commission has moved in a new direction. This new direction has made the Commission's work on the relevant rules for the soon-to-be assigned spectrum far more challenging, but I applaud Chairman Martin and his fellow Commissioners for their leadership on this issue. If, for example, the Commission carved up the entire 24 MHz of spectrum devoted to public safety into narrowband channels and distributed them to local agencies, it would have undermined the ability to use this spectrum for broadband. Instead of following the old model, however, the Commission created a new one. In particular, it proposed the creation of a public safety spectrum licensee that would receive a nationwide 12 MHz license and use it to spearhead the development and deployment of a broadband network (or network of networks) to be used by public safety.

The model of a national public safety spectrum licensee is one that poses a number of risks, but I believe that these risks can be managed. Moreover, I believe that the principle that networks should be operated at higher levels than local agencies—i.e., regional or state—is essential to enabling next generation networks to be deployed. In other words, the development of regional and national cellular networks is not an accident; there are real economies of scale in deploying such networks at higher levels. For both cost purposes and expertise purposes, the development of next generation networks by a public safety spectrum licensee is a considerably better bet than expecting localities to do so themselves.

The national public safety spectrum licensee would enjoy several important advantages not available to local agencies who have traditionally managed public safety's communications systems. In particular, this licensee would be uniquely positioned both to develop a more attractive bargain for public safety (by purchasing in bulk and using its assembled expertise) and could ensure a level of consistency as to the technology adopted by public safety. Today, for example, early next generation public safety systems being developed in New York and Washington use different technologies and different bands of spectrum, meaning that a radio devised for the New York City system will not operate in Washington. By contrast, a public safety spectrum licensee would be in a position—presumably in concert with a commercial operator—to develop a standardized air interface (or a relatively economical commitment to a multi-mode device) that would afford public safety agencies a similar mobility with their devices to that enjoyed by customers of commercial wireless firms.

One of the principal risks of a national public safety spectrum licensee is that this entity will be insufficiently attentive to the needs of local public safety agencies and will attempt to craft a "one size fits all" solution. To guard against this risk, localities should be afforded an effective voice as to what kind of offering should be available to them. (An alternative safeguard is that local public safety agencies would be able to receive federal grant money and not use the offering sponsored by the national public safety spectrum licensee provided that they demonstrated that they were adopting another effective interoperability solution.) Finally, state, regional, or local planning efforts will be critical to developing the appropriate rules for how different agencies receive priority to the network in different scenarios.

Fortunately, the nature of Internet Protocol-supported applications are that they can easily be adapted to deliver different functionalities and to empower local agencies to operate their own virtual private networks—even if local agencies do not control the physical infrastructure. In fact, that is exactly the model used by almost every major American enterprise company. Ideally, leadership at the state level will emerge (and be encouraged to emerge by federal policy[6]) to spearhead the development of these networks, public safety-centric applications, and wired Internet Protocol backbones that can interface with other critical systems (such as E-911 services, electric utility information, and public health information). To date, however, such state leadership is the exception, not the rule.[7]

IV. The Shared Public Safety/Commercial Wireless Network Concept

The creation of a national public safety spectrum licensee is the essential starting point for the development of an effective next generation network. The FCC's proposal to create such a licensee is thus an important start for ensuring the development and deployment of a next generation network. The next question is whether that is the only necessary step. As I will explain, I believe that the federal government will either need to provide significant funding to subsidize the development of this network directly or, as a second best option, enable spectrum to be monetized as an asset to support the network development and deployment. Let me be clear at the outset—I would prefer to see government fund the development of such networks directly, but in the absence of this development, the other model may well be a second best strategy. Indeed, in the ideal world, such funding might come through a reform of the federal government's own wireless network project (the IWN initiative), which is estimated to run between $5 billion to $10 billion and to only serve a limited number of federal agencies.[8]

In its proposal for a public safety spectrum licensee, the FCC states that the 12 MHz to be licensed to the public safety spectrum licensee can be leased to commercial users when not being used by public safety (on a preemptible basis). This policy innovation—and it is a progressive step away from the silo-mentality that often has characterized spectrum policy—offers the licensee a revenue source to support the development of a next generation network. Moreover, Frontline has suggested that this policy be supplemented with a further encumbered 10 MHz band of spectrum that would be auctioned to an entity willing to develop a next generation network that would be used by public safety (as well as others). In principle, the encumbering of spectrum with a requirement to serve public safety would depress the price of the relevant spectrum and thereby constitute an indirect subsidy to public safety.

In developing its proposal, Frontline has suggested that an open access requirement should be coupled with a commitment to serve public safety. The theory behind this proposal appears to be that the current wireless operators are insufficiently motivated to support a variety of applications and equipment developers, thereby stifling innovation.[9] If this suggestion is indeed valid, policymakers should be concerned about a lack of competition in the wireless industry. After all, competition is the most powerful and effective facilitator of innovation; that is, even in the best of worlds, regulatory responses are only a second best strategy. To that end, I am very sympathetic to the goal of attracting new entrants (particularly wireless broadband providers) via this auction and believe the rules for the auction should be hospitable to them. But the proposal to attach an open access mandate to spectrum encumbered with a requirement to serve public safety seems to me like a misfit as it would limit the number of eligible bidders, potentially compromising on the goal of finding the best possible partner for public safety.

As I emphasized above, the relevant question is how much money public safety will be given directly to support the development of next generation networks. With enough money, public safety agencies can lease spectrum in the marketplace and build a next generation network—as is currently happening in New York City. Without a commitment of serious resources, however, the encumbered spectrum model becomes a possible second best strategy. I am not opposed to this strategy and appreciate that in the current environment, it might be the best opportunity available and a risk worth taking. But if the FCC decides to take this risk, I believe it needs to implement a series of measures to enhance its chances of success.

V. The Public Safety Spectrum Licensee and The Importance of Effective Governance

The public safety spectrum licensee concept, whether or not coupled with encumbered spectrum such as that proposed by Frontline, must be implemented with a number of safeguards to ensure that it will be able to deliver on its promise. The first, and in some ways the most critical, challenge is to ensure that the public safety spectrum licensee is assisted by able and independent advisors so that it can negotiate effectively as to how the 12 MHz of spectrum will be used and how a next generation network system will be developed and deployed. There are a number of important details that will need to be hammered out and, just like corporate America relies on specialized consultants to craft contracts related to their information and communications technology needs, public safety will similarly need the aid of highly qualified advisors. Thus, I would emphasize the importance of hiring of qualified consultants to aid the public safety spectrum licensee in its series of important decisions.

The second principal strategy related to the public safety spectrum licensee concept is that this entity must be held accountable for its decisions and the FCC will need to exercise its oversight of the relevant licensee to ensure that it is operating responsibly. Notably, the FCC's oversight should not entail second guessing of that licensee's decisions or invite appellate review of them. It should, however, stand ready to investigate any concerns that the licensee is abusing its authority.

The final two strategies related to ensuring an effective public safety spectrum licensee function address directly the challenges that emerge from the proposal to encumber 10 MHz of

spectrum with a requirement to serve public safety. Again, whether or not the Frontline proposal is adopted, it is both likely and desirable that public safety cooperate with commercial firms to develop a joint public safety-commercial network. In principle, this network would both meet the requirements of public safety (to the extent reasonably practicable) and enjoy the economies of scale that emerge from a shared network that relies on commercially produced equipment (as opposed to equipment specially produced for public safety). In short, the Frontline proposal raises two wrinkles that require special attention: (1) public safety agencies must be afforded with the right to walk away from the proposed partnership; and (2) the FCC must ensure that some level of enforcement be self-executing (say, binding arbitration) in the event that the winner of an auction for encumbered spectrum failed to follow through on its commitments.

As I noted above, a proposal like the Frontline model reflects a second best strategy in the absence of an available revenue source to support the development and deployment of a next generation network for public safety. Significantly, the Frontline proposal is not premised on any need by public safety agencies to gain access to more spectrum to deploy such a network. Indeed, without any additional spectrum assignment at all, the City of New York is contracting for the development and deployment of a next generation network. But the City of New York is able to contract for that network because it possesses the necessary financial resources to do so. Thus, unless there is a more robust funding commitment from the federal government, the option of using encumbered spectrum becomes a plausible second best strategy.

The advantage of simply endowing the public safety spectrum licensee with a funding commitment is that this model makes clear that they are in the driver's seat when it comes to negotiating the relevant contractual terms. In the case of an encumbered spectrum solution, the nature of the negotiation becomes more complex and, in the worst possible case, it might represent a "forced marriage" whereby the public safety spectrum licensee is, in effect, coerced to deal (and share its spectrum) with an entity that it views as either unqualified or untrustworthy to deliver on its promises. To avoid this scenario, the public safety spectrum licensee must be in a position to walk away from any possible deal with the winner of an auction for encumbered spectrum. Moreover, if the public safety spectrum licensee did walk away from such a partnership for "reasonable grounds," the winner of the encumbered spectrum would necessarily be judged unable to deliver on its commitment to facilitate the development of a next generation network for public safety.[10] Going forward, it will be important that the public safety spectrum licensee and its commercial partner develop strategies for instituting new requirements to meet the needs of public safety and ensure that the commercial partner is not able to take advantage of public safety—i.e., in effect becoming an unregulated monopoly.[11]

The second important safeguard that should accompany the award of a spectrum license with a commitment to provide a next generation network to public safety is that there must be real and self-executing enforcement mechanisms. The history of spectrum policy is littered with the commitments of spectrum licensees who made, and have failed to keep, any number of assorted commitments. As noted above (and as I have argued elsewhere[12]), the use of a spectrum license to generate public interest benefits is suboptimal to using direct fiscal support to achieve those benefits. But the fact that this approach has failed elsewhere does not mean it is destined to failure here—only that regulators should approach any regulatory bargain with their eyes open and a well devised strategy to hold a licensee to its commitments.

In terms of the relevant commitments that a licensee should be forced to make, I am aware that overly onerous commitments could backfire insofar as they might undermine the ability of the licensee to attract sufficient funding via the capital markets. This concern, however, only means that the relevant performance bond, lien on the spectrum, or lien on the infrastructure should be triggered with sufficient sensitivity so that public safety does not possess an ability to pull out the rug from the licensee unfairly. Again, the historical concern tends to argue that the more realistic scenario would be an overly forgiving posture towards a failure to perform rather than an overly harsh judgment as to whether a licensee had actually performed. In short, an appropriately balanced enforcement mechanism should be clear, provide fair warning, be self-executing (i.e., not require a lengthy proceeding), and provide significant consequences so as to ensure effective performance.

VI. The Importance of Ongoing Innovation and Responsible Leadership

Before I conclude, I must emphasize that the current focus on the upcoming auction and the proposals now taking center stage should be kept in appropriate perspective. In particular, the current 700 MHz auction is not the last opportunity to facilitate improvements in public safety communications. Rather, it is merely one important chapter in an ongoing effort to improve the use of information and communications technology by public safety.

As I have discussed above, a next generation network offers enormous opportunities for public safety agencies to operate more efficiently. Indeed, if the public safety spectrum licensee can help facilitate the development of a hybrid traditional land mobile radio and broadband device, that development will provide public safety agencies with access to capabilities that will enable them to perform far more effectively, more efficiently, and facilitate improved interoperability using Internet Protocol connections. The development of such a device, however, should only be the beginning of an ongoing technological development cycle that will enable public safety agencies to operate more effectively. Indeed, one important architectural feature of a next generation network is that it can allow ongoing modular development and the use of secondary systems (e.g., commercial cellular systems, municipal wifi systems, and satellite technology) to supplement the principal communications systems.

The traditional model of buying expensive and specialized equipment dedicated to public safety has disserved public safety agencies by ensuring that they operate networks using equipment that is quickly antiquated and expensive to replace. A new model whereby public safety agencies purchase equipment premised on commercially developed standards would break from this tradition by enabling public safety agencies to benefit from technological advancements on an ongoing basis. Consider, for example, that cognitive radio technology continues to improve and should be able to ultimately facilitate the use of radios that can operate both at different frequencies and using different modes, thereby providing a promising interoperability solution.[13] Similarly, the ongoing development of satellite technology that can operate in conjunction with terrestrial wireless networks (the so called “ancillary terrestrial component” systems) could also have a significant impact on public agencies by enabling them to have a redundant communications connection as well as a way to reach all outdoor coverage areas. [14]

The new policy model necessary to promote a next generation network will take time for the relevant stakeholders to adjust to a new opportunity. For this model to be successful, it is critical that, in addition to spectrum policy decisions by the FCC, other governmental actors (such as the Department of Homeland Security, the National Telecommunications and Information Administration, and state and local governments) all embrace and support this new policy strategy. Even with the effective focus of all involved, this process will take years to succeed and, even when complete, it will, by necessity, be imperfect in terms of its overall coverage and capacity. This model, however, provides a far more effective solution to the ongoing failings of public safety communications than any other strategy I can fathom.

Conclusion

In short, I commend the Federal Communications Commission for recognizing that public safety must take advantage of new information and communications technology opportunities—i.e., the promise of a next generation network built around broadband technology—by acting as an enterprise that seeks to leverage the advances of a converged ecosystem. That ecosystem features ongoing development of new technologies for commercial users and, with a commitment by public safety to adapt such technologies for its own needs, it can avoid the mistake of the Project 25 initiative. In that case, public safety operated in an environment where it was confined to its own silo and could only use equipment produced uniquely for it. By embracing a strategy whereby it shares spectrum with one or more commercial partners, public safety will facilitate a win-win arrangement where unused public safety spectrum can be put to good use, money from that leasing arrangement can be dedicated to supporting public safety's advanced communications needs, and public safety can have access to more spectrum (than it would itself control) when it needs it.

The opportunity to develop a next generation network to afford public safety access to cutting edge technologies will require a major reorientation on the part of all stakeholders as to how public safety agencies use communications technology. This reorientation will require leadership on the federal, state, and local levels as well as a compelling explanation as to how the public safety spectrum licensee concept can facilitate opportunities that will otherwise not become available or will be prohibitively expensive for most agencies. I recognize that the public safety spectrum licensee concept comes with some risks, but provided that this licensee is supported by able advisors and with a sensitivity toward the needs of individual localities, I believe this policy strategy is a sound linchpin of the effort to spur the development of a next generation network. It can only succeed, however, if other stakeholders rally around this strategy and embrace the importance of a next generation network and work hard to make it a success.

---

[1] The Aspen Institute report, *Clearing the Air: Convergence and the Safety Enterprise*, can be found at http://www.aspeninstitute.org/atf/cf/%7bDEB6F227-659B-4EC8-8F84-8DF23CA704F5%7d/C&S%20FINALAIRSREP06.PDF. The article, *Communicating During Emergencies: Toward Interoperability and Effective Information Management*, 59 Fed. Comm. L.J. 547 (2007), can be found at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=980285. The CTIA-sponsored roundtable report, *Toward A Next Generation Network for Public Safety*

Communications, can be found at http://www.silicon-flatirons.org/conferences/Hatfield_Weiser_PublicSafetyCommunications.pdf (hereinafter, "*Next Generation Network Report*"). I have also co-authored a paper discussing the role of satellites in a next generation architecture. *See* Phil Weiser et al, *Toward A Next Generation Architecture For Public Safety Communications*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=903151. That earlier work emerged from a project undertaken on behalf of MSV. *See* Dale Hatfield & Phil Weiser, *Toward A Next Generation Strategy*, available at http://www.msvlp.com/news_docs/papers/NextGenOct21R2.pdf.

[2] United States Government Accountability Office, First Responders: Much Work Remains to Improve Communications Interoperability 3 (Apr. 2007), *available at* http://www.gao.gov/new.items/d07301.pdf [hereinafter GAO Report].

[3] *Next Generation Network Report*, *supra* note 1, at 36.

[4] Testimony of Stephen T. Devine, Missouri State Highway Patrol, House Comm. on Energy and Commerce Subcomm. on Telecommunications and the Internet (Mar. 22, 2007).

[5] Robert Rouleau, *Connecting Data Networks*, Public Safety Rep., Aug. 2006, at 98, 102.

[6] To date, federal policy has not always effectively encouraged strategic leadership at the state level. *See* United States Government Accountability Office, First Responders: Much Work Remains to Improve Communications Interoperability 20-21(Apr. 2007), *available at* http://www.gao.gov/new.items/d07301.pdf 21 ("[A]lthough 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").

[7] The Aspen Institute report, see note 1, *supra*, discusses the importance of such leadership. And, in a promising development, the Southern Governors Association is investigating a strategy for providing such leadership on a regional basis. *See* http://www.southerngovernors.org/resolutions/Interoperability.html.

[8] *See Next Generation Network Report*, *supra* note 1, at 35.

[9] To put the issue in terms of economic analysis, it boils down to whether the incumbent platform providers view applications developers hospitably (i.e., because they make their platform more valuable) or as a threat (for any number of possible reasons). For a comprehensive discussion on how information platform providers view applications developers, see Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration and Open Access Policies: Towards A Convergence of Antitrust and Regulation in The Internet Age*, 17 Harv. J. L. Tech. (2003).

[10] It is critical that any consequences to the winner of an auction for encumbered spectrum be confined to a "reasonable grounds" scenario. Otherwise, the public safety spectrum licensee would have an incentive to use its hold-out leverage to extract unfair and inappropriate concessions from the encumbered spectrum licensee.

[11] The public safety spectrum licensee and its commercial partner will, in all likelihood, enter into what economists call a "bilateral monopoly relationship." Such partnerships are generally characterized by mechanisms to guard against undue opportunistic behavior by one side, including a stylized "hostage exchange" scenario, where each side gives something of value to the other and can threaten to keep it in the event the other side acts unreasonably. *See* Oliver Williamson, The Mechanisms of Governance (1996).

[12] *See* Phil Weiser, Promoting Informed Deliberation and A First Amendment Doctrine For A Digital Age: Towards A New Regulatory Regime for Broadcast Regulation," *Deliberation, Democracy, and the Media* (Costain and Chambers, eds., 2000). As Richard Posner explained in

his classic article, the use of a spectrum license—or any regulatory program—to achieve such benefits indirectly can be termed "taxation by regulation." Richard Posner, *Taxation by Regulation*, 3 Bell J. Econ. 22 (1971). As Posner explained, such an approach has certain merits, but also comes with notable risks. *Id.*

[13] SDR Forum, Software Defined Radio Technology for Public Safety 26 (Apr. 14, 2006), http://www.sdrforum.org/uploads/pub_36302706_a_0001_v_0_00_public_safety_04_14_06.pdf ("the 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."); Testimony of Stephen Devine, *supra* note 4 (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").

[14] This point is more fully elaborated upon in Phil Weiser, Dale Hatfield and Brad Bernthal, *Toward A Next Generation Architecture For Public Safety Communications*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=903151.