2007

Communicating During Emergencies: Toward Interoperability and Effective Information Management

Philip J. Weiser
University of Colorado Law School

Communicating During Emergencies:

Toward Interoperability and Effective Information Management

Philip J. Weiser*

I. INTRODUCTION

The crisis of communications on 9/11 and in the aftermath of Hurricane Katrina underscores that emergency responders are largely ill-equipped to communicate effectively in times of disaster as well as in day-

* Professor of Law and Telecommunications, University of Colorado. Thanks to Brad Bernthal, James Crowe, Dale Hatfield, Jennifer Manner, Tricia Paoletta, Jill Van Matre, and Charles Werner for helpful comments and encouragement.

to-day emergency situations that require the coordination of several different public safety agencies. The reason for this state of affairs is that public safety agencies traditionally have made individualized decisions about information and communications technology,[1] generally failing to purchase state-of-the-art technology that operates effectively and interoperates with others involved in emergency response. Thus, even in today's Internet-connected world, public safety agencies continue to rely on single-purpose technologies that do not provide economies of scale, network flexibility, or the broader functionalities routinely used by the military and private sector enterprises.

Unfortunately, the failings among public safety communications systems on 9/11 and in the wake of Hurricane Katrina were entirely predictable and avoidable. After all, "[d]espite numerous after-action reports, public safety services have yet to make significant progress in comprehensively addressing interoperability."[2] Part of this failing can be explained by the traditional reluctance of public safety communications managers to invest in new technologies; in many cases, such managers claim that only traditional land mobile radio ("LMR") services designed specifically for their use can meet their needs.[3] Thus, until public safety agencies are willing to embrace technologies other than their traditional LMRs, they will continue to possess limited communications capabilities and perpetuate the failings of our current system.

To change the culture and realities of public safety communications, policymakers must develop a new architecture for the use of information and communications technologies (i.e., one that leverages the power of Internet technology) and provide a framework for leadership (subject to benchmarking) to transition to a next generation system for public safety communications. Such a culture change would include not only an embrace of new technologies, but a new framework for technology leadership—at

1. This Article uses the term "public safety" to capture a broad range of entities involved in emergency response. In particular, it emphasizes that opportunities to use information and communications technology effectively are not limited to traditional "first responders" (such as fire and police), but also extends to all of those likely to respond to emergency situations (ranging from agencies concerned with transportation infrastructure to public health providers to the 9-1-1 system to electric utilities). Moreover, this Article also takes a broad view of information and communications technology—including not simply wired and wireless local telecommunications networks, but also the information technology associated with accessing and sharing critical information. Nonetheless, it sometimes uses as shorthand the term "public safety communications."

2. *See* William L. Pessemier, *Top Priority: A Fire Service Guide to Interoperable Communications* 2, International Association of Fire Chiefs (2006), http://www.interoperability.publicsafety.virginia.gov/pdfs/FireService-InteropHandbook.pdf.

3. Larry Irving, *Land Mobile Spectrum Planning Options*, app. at 1, Oct. 19, 1995, http://www.ntia.doc.gov/osmhome/reports/slye_rpt/appendix.html.

the state or regional level—that spurs decision making in a coordinated fashion (and not through ad hoc decisions by over 50,000 different local agencies). In short, this Article explains which new technologies can transform public safety communications and which intergovernmental relations strategy will be necessary to facilitate the implementation of such technologies.

This Article proceeds in five parts. After this Introduction in Part I, Part II outlines the current state of public safety communications. Part III discusses five technological developments—multimode radio systems; Internet Protocol-based architectures; cognitive radio technology; broadband wireless systems; and distributed information management—that can, taken together, dramatically improve the state of public safety communications. Part IV discusses the optimal intergovernmental strategy for developing and implementing such new technologies. Part V offers a short conclusion.

II. BACKGROUND

The state of information and communications management among today's emergency responders reflects a technological architecture that, in most cases, was designed and implemented based on (at best) 1980s technology. Consequently, for most emergency responders (ranging from police departments to fire departments to public health officials), their limited use of advanced information and communications technology largely reflects the fact that each agency has traditionally purchased special-purpose equipment designed for their particular needs. These needs, as traditionally understood, constituted merely the ability to talk to one another, with limited interest in interoperability, broadband connectivity, or adaptability to new technology.[4]

The traditional public safety mindset about information and communications technology focuses on the value of a radio link that provides each agency with a single channel for analog voice communications with their staff in the field. Consequently, as late as 1995, "most public safety radio systems remain[ed] based on 50-year old spectrum technology—i.e., single-channel, 15 kHz bandwidth analog FM radio—which has been superseded in many services by more efficient technology."[5] Over the last ten years, and particularly over the last five years (i.e., since 9/11), there is an increased awareness about the limits of

4. *See* Jon M. Peha, *From TV to Public Safety: The Need for Fundamental Reform in Public Safety Spectrum and Communications Policy* 3 (New America Foundation Working Paper No. 15, 2006), *available at* http://www.newamerica.net/publications/policy/from_tv_to_public_safety (setting out basic assumptions of public safety agencies).

5. Irving, *supra* note 3, at app. 1.

such a system both in terms of its capabilities and its lack of interoperability with other systems. To address these limits, an oft-prescribed cure is to develop "centralized trunked radio systems" that pool spectrum licensed to particular agencies and authorize two-way radio communications on an "as needed" basis,[6] thereby providing greater spectrum efficiency and interoperability between the different participating agencies.[7] Notably, such systems are far more efficient than their traditional counterparts because "[f]ar fewer channels are needed to serve multiple agencies if those channels are shared by all agencies, or equivalently, the same number of channels can support far more mobile users when channels are shared among agencies."[8]

To date, a number of jurisdictions have improved spectrum efficiency and interoperability by instituting systems of shared "digital trunked systems." Notably, the Alaska Land Mobile Radio ("ALMR") system provides an impressive example of how such a system can greatly improve public safety communications; in particular, the ALMR enables federal, state, and local governments to share frequencies.[9] In this arrangement, which is the first statewide sharing agreement of its kind, federal and state agencies pool their spectrum with the high-band VHF channels used for communications from mobile units and the state spectrum used for fixed infrastructure transmissions.[10] By so doing, the ALMR system operates

---

6. Viktor Mayer-Schönberger, *The Politics of Public Safety Interoperability Regulation*, 29 TELECOMMS. POL'Y 831, 833 (2005) (suggesting a path to interoperability based on the "willingness of public safety agencies to replace their existing analog equipment with new digital-trunked infrastructure using a common standard and frequency.").

7. As Dale Hatfield has explained:

> Trunking systems are premised on the insight that pooling a group of channels together and giving the users access to all channels on an "as needed" basis provides better service by reducing the likelihood of a channel-busy condition. Trunking may be accomplished in a centralized or decentralized manner. In a *centralized* trunking system, information on the status of the pooled channels, e.g., in-use or idle, is stored in a computer like device or controller typically located at the base station transmitter or repeater site. A dedicated control channel is then used to exchange signaling information between the controller at the central site and the mobile units. In this architecture, the mobile units continuously monitor the control channel when they are in the idle state.

Dale N. Hatfield, Lessons From Trunked Radio Systems (2006) (working paper on file with the author).

8. *Id. See also* Jon M. Peha, *Protecting Public Safety With Better Communications Systems*, IEEE COMM. MAG., Mar. 2005, at 9, *available at* http://www.comsoc.org/ci1/Publi c/2005/Mar/cireg.html (citations omitted) (noting opportunities for greater spectral efficiency).

9. App'ns of State of Alaska Request for Waiver, *Memorandum Opinion and Order*, para. 1, DA 03-2612 (Aug. 7, 2003) [hereinafter Alaska Request].

10. Donny Jackson, *Trailblazers*, MRT MAGAZINE, Apr. 1, 2006, *available at* http://mrt mag.com/mag/radio_trailblazers/index.html.

more efficiently than conventional systems, allowing all of the relevant agencies "to use fewer channels to provide the same communications capability."[11] Moreover, the ALMR system has received "rave reviews" following a 2005 exercise where federal agencies (such as FEMA) worked in partnership with their local counterparts.[12]

To understand the traditional public safety mindset, one must appreciate that, in many cases, police officers value their radios more than their guns. Local LMR systems thus constitute a vital tool that police departments, for example, will often insist on controlling and operating themselves. Viewed from this perspective, it is understandable how even a single channel system dedicated to the police department may seem preferable to a multichannel, trunked system that is shared between different agencies and not controlled by the police department. In principle, trunked systems shared between different agencies should operate as or more effectively than traditional systems, but some departments have yet to adopt such systems, either based on a lack of funding, ineffective coordination, or a fear of the unknown. Whatever the reason for the challenges in promoting trunked radio systems that facilitate interoperability, it is important to appreciate—as Part III emphasizes—that such systems only solve interoperability issues to a limited degree (i.e., they generally leave some relevant agencies unconnected to the particular system[13]) and fail to address the larger and more systematic weaknesses of public safety communications systems.

As a result of the traditional resistance to new technologies, public safety agencies generally have used (even in the trunked system model) specialized blocks of spectrum that are paired with single-purpose radio infrastructure. In practice, this means that public safety agencies are limited to narrowband channels and do not benefit from the economies of scale garnered by commercial, off-the-shelf systems. To justify this practice, public safety agencies insist that only this model of communications can meet their needs. Relatedly, they often reject the suggestion that commercial providers could meet any of their communications needs, highlighting that their requirements are more demanding and could not be met by commercial providers.

---

11. Alaska Request, *supra* note 9, at para. 18 (citation omitted).

12. Jackson, *supra* note 10.

13. "The U.S. Conference of Mayors reports that 23 percent of the nation's 60,000 police and fire departments cannot communicate with each other over the radio, one-third cannot talk to county sheriffs, and most cannot talk to state or federal agencies." Spencer S. Hsu, *FEMA Overhaul Debate Stalls Funds For Interoperable Radios*, WASH. POST, Sept. 14, 2006, at A12.

Almost all observers agree that trunked radio systems improve upon the traditional model of public safety communications and that the relevant technology is well established (and has been for nearly twenty years).[14] Compared to the opportunities to improve public safety communications based on emerging technologies, the relative benefits of this upgrade are relatively minor. Consequently, unless the culture around public safety communications changes, the improvements related to the Internet Protocol revolution will not be adopted by public safety agencies, and they will continue to exist in their own state of technological isolation. Or, to use Thomas Hazlett's more colorful language, "[e]mergency radio services need to exit their government technology ghetto and get onboard advanced networks—as smart customers, not Soviet-style suppliers."[15]

As they currently exist, public safety communications systems are a case study of how *not* to develop an IT enterprise. First, the current model—centered on expensive single-purpose radio systems—ensures that most agencies adopt an architecture that does not allow for evolution and dynamism. Second, despite the aspirations of the Project 25 effort,[16] the model of "public safety exceptionalism" has left agencies isolated and with a limited number of vendors prepared to meet their needs by selling them expensive equipment. Finally, in a move that ignores the recent technological trends, public safety agencies generally depend on radios where the intelligence is hardwired in physical devices—as opposed to in a logical layer (e.g., consisting of Internet Protocol-related standards) that is easily configurable and extensible—that are only engineered for voice communications (and not data or video).

When policymakers talk about the public safety interoperability problem, they are generally reacting to the symptoms of a larger problem while failing to address the broader, systemic challenges. Going forward, policymakers should not continue to fund and encourage public safety agencies to adopt advanced shared systems built on a technologically

14. Indeed, this may well be what Secretary Chertoff had in mind when he stated that the shortcomings in the state of emergency responders' communications are "not a technological challenge," but rather a management one. Michael Chertoff, Remarks at the Tactical Interoperable Communications Conference (May 8, 2006), *available at* http://www.dhs.gov/xnews/speeches/speech_0281.shtm. I certainly concur with this judgment, although, as discussed below, I think the better technological course is to pave the way for tomorrow's technology (as opposed to investing in yesterday's technology).

15. Thomas W. Hazlett, *Katrina's Radio Silence*, FT.COM, Oct. 24, 2005, http://www.ft.com/cms/s/8defb2f6-4486-11da-a5f0-00000e2511c8.html.

16. The "Project 25" initiative, spearheaded by the Association of Public Safety Communications Officials ("APCO") and supported by the Telecommunications Industry Association ("TIA"), has sought to craft a set of open standards that would invite entry and facilitate interoperability into the world of public safety communications. *What Is Project 25?*, PTIG, http://www.project25.org/modules.php?name=Content&file=viewarticle&id=2.

antiquated model.[17] Rather, they should embrace a broader architecture that can include a role for traditional LMRs as well as embrace a role for commercially available off-the-shelf equipment and technologies that can be readily adapted to meet the requirements of public safety. In so doing, policymakers should end the tradition of allowing public safety agencies to remain on a technologically isolated platform in the midst of ever-more powerful and innovative networks and equipment. In some cases, this tradition will be hard to break given that a number of current projects revolve solely around a shared trunking system specialized for particular public safety agencies and, as is always the case, it is difficult to abandon projects that have been in the development process for quite some time.[18] To continue ahead with such projects, however, would only exacerbate the current failings and defer the move to a more flexible and technologically advanced platform.

III. TOWARD A NEW ARCHITECTURE FOR PUBLIC SAFETY AGENCIES

Building on Part II's critique of the state of public safety communications, this Part develops the broad architecture and explains the specific technologies that promise—if given an opportunity—to transform public safety communications. In short, this Part focuses on five related technologies that mutually reinforce one another: (1) a modular architecture; (2) a reliance on Internet Protocol technology; (3) the use of cognitive radio technology; (4) the development of broadband access technology; and (5) the use of rights management to shared information resources. Taken together, these technologies promise to enable public safety agencies to operate in a more technologically dynamic climate and to achieve far greater levels of operability and interoperability than possible with a strategy centered on centralized trunked systems.[19]

---

17. Some have suggested that the failure of the Project 25 endeavor to facilitate more competition reflects the influence of Motorola in pushing for incompatible standards. One commentator, for example, suggested that Motorola:

> [L]obbied the FCC to adapt the standard it had helped design. The standard provided backward compatibility with both old analog and non-trunked systems. This standard was also incompatible with a standard developed at about the same time by the Europeans . . . . This in effect limited access to the U.S. market. Not surprisingly by 2000, only one major equipment manufacturer—Motorola—offered infrastructure compatible with the standard Motorola had successfully lobbied for.

Mayer-Schönberger, *supra* note 6, at 835, n.15.

18. As Jon Peha explains, this description may well apply to the federal government's own Integrated Wireless Network Initiative. *See* Peha, *supra* note 4, at 8.

19. For an argument along these lines (and similar to the thrust of this Article), see Tamara Casey et al., *Architecting a Next Generation Network for Public Safety* (2006), http://www.cyrencall.com/downloads/CyrenCall_Technical_Exhibit.pdf.

A. *The Importance of a Modular Architecture*

The first principle of a next generation strategy is to embrace a modular, flexible, and extensible architecture that can incorporate new networks and equipment. Such an architecture is increasingly used in the commercial cellular environment where firms integrate traditional cellular networks alongside other networks (say, Wi-Fi) and enable switching between the two on either a selected or automatic basis. In many cases, this modularity is stitched together by multimode phones, but it can also simply be achieved by enabling both functions to operate at the same time. To appreciate how such an architecture would operate, consider Figure 1 below,[20] which depicts the use of a satellite overlay network and a related terrestrial cellular network ("ATC") as well as a legacy LMR network.

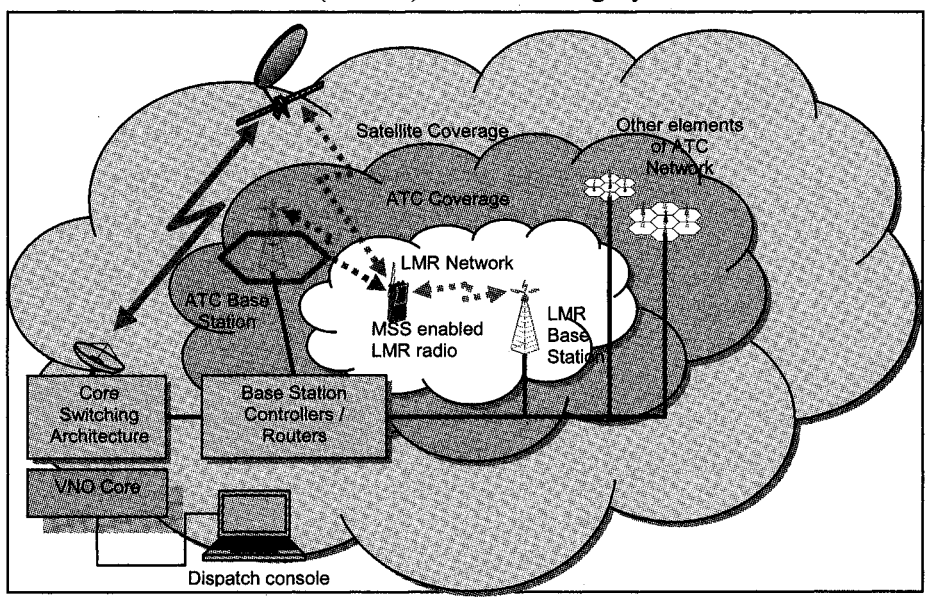

Figure 1
(note: diagram is conceptual in nature and not drawn to scale)

As suggested by Figure 1, the optimal technological architecture is one that recognizes a role for different devices and networks (including legacy LMRs and emerging wireless broadband systems), allowing them to be integrated by users in a sensible manner.[21] But even a suboptimal

20. Figure 1 and the explanation of how such an architecture would operate and fit the needs of public safety come from Philip J. Weiser et al., *Toward a Next Generation Architecture For Public Safety Communications* 10–11 (2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=903151#PaperDownload.

21. For most major enterprises, this type of tailoring is quite common and is often performed by firms referred to as "system integrators."

version of this architecture, where public safety personnel carry multiple devices in the field, improves upon the current state of public safety communications. In fact, as Jon Peha has recognized:

> 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.[22]

Fortunately, this recognition is attracting increasing support, with the FCC recently underscoring that "there may now be a place for commercial providers to assist public safety in securing and protecting the homeland."[23]

The modular architecture outlined above would greatly improve performance, operability, interoperability, and redundancy without compromising on the ability to use LMRs for mission-critical (i.e., shoot/don't shoot) situations. Again, as Jon Peha has observed, "while public safety has demanding needs for mission-critical real-time applications, much of public safety communications is not mission-critical, so failure is tolerable, or first responders can simply try again later."[24] For such situations, like many of the communications needs in the aftermath of Hurricane Katrina, a modular communications environment that included a satellite overlay (such as that facilitated by an ATC system) would be likely to operate effectively when other terrestrial-based options were inoperable. Recognizing this point, FCC Chairman Martin explained that "[i]f we learned anything from Hurricane Katrina, it is that we cannot rely solely on terrestrial communications."[25]

B. The Opportunities From an Integrated Communications Architecture Built Around Internet Protocol Technology

In all sectors other than public safety, the powerful trend in information technology as well as in communications policy has moved

---

22. Peha, *supra* note 4, at 6.

23. *Report to Congress On the Study to Assess Short-Term and Long-Term Needs for Allocations of Additional Portions of the Electromagnetic Spectrum*, 37 Comm. Reg. (P & F) 706, 707 (2005). *See also* Peha, *supra* note 8 (stating that "the United States should reevaluate the traditional separation between public safety systems and commercial systems.").

24. Peha, *supra* note 4, at 6.

25. *Hearing on Communications in a Disaster Before the S. Comm. on Commerce, Science and Transportation*, 109th Cong. 7 (2005) (statement of Kevin J. Martin, Chairman, FCC) [hereinafter Statement of Kevin J. Martin].

away from a silo-based mentality. Increasingly, information technology and communications equipment capitalizes on the rapid improvements in processing power, advances in storage technology, and the innovations unleashed by the wide adoption of Internet Protocol-based networking. This powerful trend is captured under many rubrics (such as the "digital broadband migration" or "next generation network" concepts), but it essentially envisions that data broadband networks will carry Internet Protocol-based packets that will liberate particular services from traditional networks. In such an environment, numerous different networks are accessible by a range of devices, and all can interact with shared services.

For public safety agencies, Internet technology is often viewed as irrelevant to their mission. After all, the argument goes, the Internet is a general purpose platform and could not begin to meet their needs. This argument, however, ignores two critical points. First, Internet technology (i.e., the use of the TCP/IP protocol suite) is not the same as the Internet itself. Second, with respect to both Internet technology and the Internet itself, many sectors of the economy (including the military) take advantage of "the near-ubiquity of the Internet and the wide availability of advanced wireless" services, suggesting that public safety agencies could use such technologies effectively as well.[26] To be sure, any such development will require an abandonment of the "public safety exceptionalism" mentality and the recognition that Internet technology (and not necessarily the Internet per se) can afford enormous flexibility and provide an effective platform for applications that can be tailored to meet the specific needs of public safety.

The commitment to a flexible, Internet-based architecture that includes commercial systems would enable public safety agencies to capitalize on innovations that are creating new opportunities for all users of information and communications technology ("ICT"). In an effort to advance this vision, the FCC's National Reliability and Interoperability Council's ("NRIC") Focus Group 1D called for an emergency communications system linked in an "inter-network" fashion. In particular, it recommended "a set of policies, tools, interfaces and standards that connect securely the multiplicity of local, regional and national wireline and wireless networks."[27]

A public safety ICT vision that incorporated Internet Protocol ("IP")-based networks offers the potential to transform public safety communications systems from islands of proprietary technology to a sea of

26. LINDA K. MOORE, CONG. RESEARCH SERV., PUBLIC SAFETY COMMUNICATIONS: POLICY, PROPOSALS, LEGISLATION AND PROGRESS 17 (2005).

27. FOCUS GROUP 1D, NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL VII, COMMUN. ISSUES FOR EMERGENCY COMMUN. BEYOND E911 3 (2005).

compatible and more efficient infrastructure. In particular, such a vision would move public safety agencies—say, on a state-wide basis—to an *enterprise architecture* that could be designed and implemented in a manner that enables all parts of the enterprise to communicate effectively with other parts and to share information as needed. Significantly, the notion of an enterprise system, which is facilitated by IP-based technology, reflects a more robust concept of interoperability than the effort to patch together legacy radios through a shared trunked system.

The importance of embracing an enterprise architecture built around IP technology is that it can incorporate and include different entities which operate networks that need to interact with public safety agencies to address a particular set of circumstances. To attempt to engineer specialized networks with the aim of connecting particular agencies—say, fire, police, and sheriffs—is doomed to leave out relevant agencies. Consider, for example, that public health agencies, electric companies, and forest services are also likely to be involved in mission-critical responses in particular emergency situations.

Stated simply, if the relevant ICT system is engineered as a closed universe, it will be difficult—if not impossible—to share important information with agencies not connected via the specialized network. By contrast, an IP-based network can easily authorize and include other agencies on a limited and as needed basis. Moreover, an IP network provides valuable flexibility that can easily allow for end-to-end encryption whereby users of the network would not be able to receive and process encrypted communications unless authorized to do so.

Given the possibilities of an enterprise architecture, it makes sense to embrace a broad version of interoperability that can link together all affected agencies and enable them to communicate not merely via voice communications, but to exchange data and video communications as well. A recent Senate bill (S. 2845) articulated just such a conception, calling for a definition of "interoperable communications" as:

> the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary . . . utilizing information technology systems and radio communications systems, and to exchange voice, data, or video with one another . . . in real time, as necessary.[28]

Significantly, this definition mirrors the NRIC model, which specifically calls for the use of IP technology to accomplish this objective.[29]

---

28. H.R. REP. NO. 108-796, at 213 (2004).

29. This solution mirrors the one called for by NRIC VII Focus Group 1D, which suggested that:

> [a] single, interconnected Internet Protocol system should be used for all emergency communications, connecting a wide variety of agency-run and public

Even without a clear federal commitment to a public safety architecture built around IP technology, commercial firms are developing solutions to interoperability based on IP. Notably, Cisco, Twisted Pair, and others have developed a proposal for connecting existing radio systems into an IP gateway. Cisco's system, for example, uses one channel to connect to the gateway, allowing for interoperability through a gateway that allowed other channels (presuming that there is more than one channel) to be used for ordinary radio communications.[30] In the case of Twisted Pair Solutions, it has pioneered what it calls a "WAVE management system," which uses a server to enable public safety communications to operate more effectively. Using the WAVE system, public safety agencies can—based on the open IP standard—utilize more advanced dispatch systems, host multiple different types of user groups (which can be configured on an as needed basis), and adopt new innovations that can ride on this platform.[31] To date, a number of public safety agencies (such as the Coast Guard) have implemented this approach, both improving the functionality of their systems and saving money by enabling their legacy systems (including personal computers) to broaden their ability to communicate.[32]

C. *Cognitive Radio Technology*

In many respects, cognitive radio (or "smart radio") technology builds perfectly upon—and enables the virtues of—IP networking and a modular architecture. Unlike traditional radio technology, cognitive radio

---

networks, both wireline and wireless. Focus Group 1D calls this an "Internetwork" to emphasize that this group does not believe a new physical network is needed. It is a system of systems approach.

FOCUS GROUP 1D, *supra* note 27, at 7.

30. *See* Cisco Systems, *Solutions for Communications Interoperability* 2–3 (2005), http://www.cisco.com/application/pdf/en/us/guest/products/ps6718/c1244/cdccont_0900aecd80350fee.pdf.

31. *See* TWISTED PAIR SOLUTIONS, HOW WAVE WORKS 3–4 (2006), http://www.twistpair.com/index/cms-filesystem-action?file=Product%20Overview/wave-howworks-po-8.5x11.pdf. As their marketing material explains:

> WAVE is a software application suite that manages secure, real-time group communications over the IP network, enabling interoperable communications between any connected devices. Importantly, WAVE is an interoperability solution that works with your current radio system, connects with any radio equipment from any manufacturer at any frequency, and always remains under your control.

TWISTED PAIR SOLUTIONS, WAVE FOR INTEROPERABILITY 1 (2007), http://www.twistpair.com/index/cms-filesystem-action?file=Solution%20Brief/wave-interop-sb-8.5x11.pdf.

32. *See* TWISTED PAIR SOLUTIONS, UNITED STATES COAST GUARD: THE USCG SAVES LIVES WITH INTEROPERABLE COMMUNICATIONS SOLUTIONS POWERED BY WAVE (2006), http://www.twistpair.com/index/cms-filesystem-action?file=Case%20Study/wave-coastguard-cs-a4.pdf.

technology relies on intelligence at the edges of the network,[33] whereby radios are "aware" of their environment and can adapt accordingly.[34] In many cases, the cognitive capabilities are driven by software—thus, the concept of a "software defined radio"[35] ("SDR")—meaning that the physical layer is programmable and reconfigurable. In an SDR (as opposed to a traditional radio's fixed hardware), capabilities traditionally controlled by hardware—including signal processing, modulation/demodulation, and power control—are accomplished by reconfigurable software. Ideally, this flexibility and dependability on software renders such radios "future proof" (i.e., immune to becoming technologically antiquated).

An important feature of cognitive radios is that they are able to change how and where they operate. By enabling the same radio to use different modulation schemes, waveforms, and frequencies, they are able to, as the FCC explained, "identify and use spectrum that otherwise would not be available for fear of causing interference."[36] For this reason, Chairman Martin has championed their use by public safety agencies, explaining that they would enable agencies to use "multiple frequencies in multiple formats" and benefit from a more "flexible infrastructure."[37] This flexible infrastructure would be less expensive insofar as base stations

33. The NTIA defined cognitive radio systems as "[a] radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, [and] access secondary markets." In the Matter of Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum, *Comments of Nat'l Telecomm. & Info. Admin.* 44, ET Docket No. 03-108 (Feb. 15, 2005).

34. For a survey of the developments in this area, see Ian F. Akyildiz et al., *NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey*, 50 COMPUTER NETWORKS 2127 (2006).

35. As defined in 47 C.F.R. § 2.1, a SDR is a:

> radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.

47 C.F.R. § 2.1 (2005). *See also* Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Techs., *Report and Order*, 20 F.C.C.R. 5486, para. 9 (2005) (citing 47 C.F.R. § 2.1) [hereinafter *CR Report and Order*].

36. *Id.* at para. 11.

37. Statement of Kevin J. Martin, *supra* note 25, at 7. Chairman Martin's observation echoed the findings of an earlier GAO Report. That report explained that "[s]oftware-defined radios will allow interoperability among agencies using different frequency bands, different operational modes (digital or analog), proprietary systems from different manufacturers, or different modulations (such as AM or FM)." U.S. GOV'T ACCOUNTABILITY OFFICE, TECHNOLOGY ASSESSMENT: PROTECTING STRUCTURES AND IMPROVING COMMUNICATIONS DURING WILDLAND FIRES 61–62 (2005). *See also* Jonathan Adelstein, Commissioner, FCC, Remarks at the Global Regulatory Summit on SDR and Cognitive Radio (June 20, 2005), *available at* http://www.npstc.org/documents/Adelstein%20Keynote.pdf (praising the benefits of SDR).

could support multiple technologies, and radios could be aware of their environment, locating unused spectrum and utilizing it on an as needed basis.

In a flexible environment, there would be an opportunity to automate spectrum coordination between adjacent public safety agencies, enabling the sharing of spectrum as well as the reconfiguration of radios over time. Significantly, "smart radio" technology promises to "enable operability among public safety agencies on multiple air interfaces, overlaying existing systems without disruption, upgrading legacy systems, including possible transition from one radio interface to another, and the easy selection of [radio frequency] band, air interface, and group affiliation by users of portable [smart radio] equipment."[38] This ability to adapt to different environments can be particularly significant in the public safety context where radios for certain agencies might need to operate on different frequencies in their home territory and in adjacent ones. Moreover, the sharing opportunities for public safety radio users are likely to be significant, as the legacy system of spectrum management for public safety (as discussed above) leaves different agencies with particular spectrum assignments that often lay fallow.

To appreciate how "smart radio" technology enables a more flexible and efficient use of spectrum assigned to public safety agencies, it is worth emphasizing how this technology resembles (and improves upon) the use of trunking technology. As discussed above, trunking arrangements can be an effective coordination tool, but smart radio technology takes this basic framework and implements it in a more effective manner. Notably, smart radio technology can be viewed as "trunking writ large," as it uses the same basic insight as trunking (i.e., the sharing of capacity on a dynamic basis) to achieve efficient use of the spectrum. Consequently, smart radio technology operates in the same manner as decentralized trunking,[39] albeit using a different technological architecture.

The ability of smart radio technology to improve public safety communications dramatically is one that the federal government should seek to promote aggressively. To date, there are some important research

---

38. *Id.*

39. Dale Hatfield explained the difference between centralized and decentralized trunking as:

> Decentralized trunking systems do not store information on the status of the pooled channels on a centralized basis and no dedicated control channel is involved. Instead, in a decentralized system the mobile and dispatcher radio units can be said to continuously scan or monitor all of the pooled channels in the system. When a dispatch call is initiated by a mobile unit or dispatcher, the unit immediately stops at the next idle channel in the pool.

Hatfield, *supra* note 7.

initiatives, such as the National Institute of Justice grant to build a "Prototype Public Safety Cognitive Radio for Universal Interoperability."[40] As noted above, such technology is able to find unused spectrum, configure itself to use it, and be able to operate based on simple commands. Moreover, this radio, as depicted in Figure 2 below, would provide an ability for public safety agencies to interoperate at the physical layer (as opposed to through IP-based communications). In a sense, this ability to provide interoperability would reinforce and provide additional assurance to the interoperability that could exist through IP-based communications.[41]

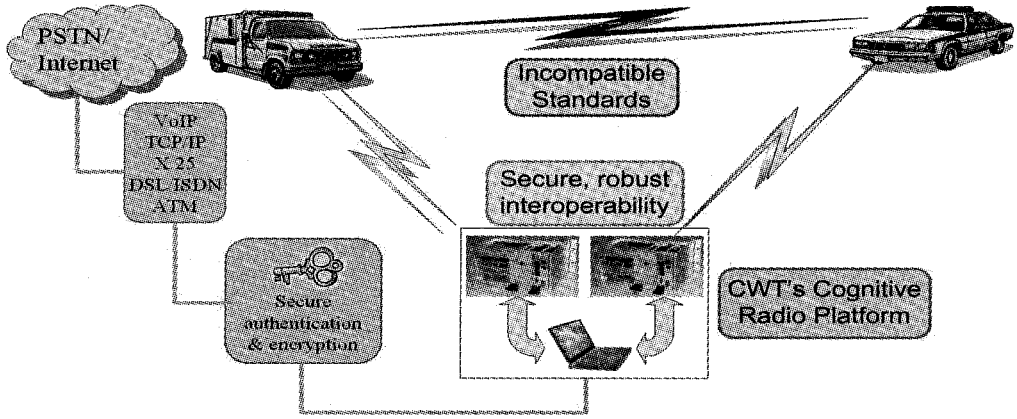

Figure 2 [42]

D. Broadband

Even among traditional public safety radio administrators, there is an increasing recognition that public safety agencies need to adopt broadband technology to enable a series of mission-critical applications (such as relaying pictures or video to and from the field). Indeed, a recent survey of U.S. and Canadian consumers concluded that broadband is "the

40. This research project is now being conducted at Virginia Tech. *See* http://www.irean.vt.edu/research_workshop_april2006/Rondeau_Thomas.pdf.

41. In fact, the architecture of a cognitive radio-based solution is quite similar to that of an IP-based solution in that a cognitive radio solution "can interconnect mutually incompatible networks [by] allowing full interoperability through a *system of systems* approach." Thomas W. Rondeau et al., *Cognitive Radios in Public Safety and Spectrum Management*, Telecomm. Pol'y Research Conf. (2005), at 13, http://web.si.umich.edu/tprc/papers/2005/430/Rondeau- Cognitive_Radios_in_Public_Safety_and_Spectrum_Management.pdf.

42. REED & BOSTIAN, UNDERSTANDING THE ISSUES IN SOFTWARE DEFINED COGNITIVE RADIO 10, http://www.mprg.org/publications/presentations/CognitiveRadioIssues.pdf.

communication service they can least live without."[43] Nonetheless, which broadband technology should be adopted and which model of financing should be selected to facilitate the buildout of a broadband system remain pressing and unanswered questions. While I do not have a particular proposal in mind, I do believe that it is critical that policymakers embrace the overall goal and develop an effective strategy for reaching it.

There are a number of strategies now being debated for spurring the buildout of broadband technology to serve public safety agencies. Notably, both Cyren Call and Frontline Wireless have offered to build broadband networks for use by public safety agencies—in return for free spectrum or specific restrictions on spectrum set to be auctioned.[44] Similarly, there are efforts underway to reallocate how the spectrum in the 700 MHz band—which is slotted for public safety—is going to be organized so as to facilitate the development of broadband access networks.[45] Finally, there are a number of proposals that would enable public safety agencies to share spectrum with commercial providers so that both public safety agencies and commercial providers could have access to more spectrum on an as needed basis.[46]

Broadband access solutions can also be—and are being—developed via dedicated high-speed wide area broadband technologies (e.g., EV-DO) as well as using a Wi-Fi or WiMAX-based solution. For state and local governments, the FCC has sought to encourage such efforts by making available spectrum at 4.9 GHz so that localities can use Wi-Fi and WiMAX technology for their public safety needs.[47] Today, for example, Tropos is using Wi-Fi equipment, and Alvarion has developed WiMAX equipment that can provide speeds sufficient to deliver pictures and video to police officers in the field.[48] Significantly, an Internet-based architecture is

43. North American Homes Rate Broadband as Key Wireless Service, IQ ONLINE, Oct. 27, 2006, http://www.arm.com/iqonline/news/marketnews/15168.html.

44. Marguerite Reardon, *Public Safety Bids Spur Spectrum Spat*, CNET NEWS.COM, Mar. 2, 2007, http://news.com.com/Public+safety+bids+stir+spectrum+spat/2100-1033_3-6163654.html?tag=st.prev.

45. *See* Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, *Ninth Notice of Proposed Rulemaking*, FCC 06-181 (Dec. 20, 2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-181A1.pdf.

46. For one such proposal, see Joshua Marsh, *Secondary Markets in Non-Federal Public Safety Spectrum*, Telecomm. Pol'y Research Conf. (2004), http://web.si.umich.edu/tprc/papers/2004/384/tprc.pdf.

47. *See* News Release, FCC Improves Public Safety Access To The Latest Broadband Technology (Nov. 9, 2004), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-254117A1.doc (explaining that "public safety licensees [can now] use a single, low-cost device to access the 4.9 GHz band, the U-NII band, and the ITS band, allowing them to enjoy savings that are typically limited to the high-volume commercial market").

48. *See* TROPOS NETWORKS, METRO-SCALE VIDEO SURVEILLANCE: HIGH-PROFILE CRIMINAL TRIAL (Aug. 2004), http://www.tropos.com/pdf/peterson_casestudy.pdf

inherently modular and flexible, allowing different agencies to all interoperate while experimenting with different broadband access solutions.

Finally, a promising option for deploying broadband infrastructure is the use of mesh networking systems. Such systems can be called "infrastructureless" because they use distributed antennas—including ones on the relevant devices themselves—to transmit broadband communications. Indeed, mesh networking systems may well benefit from the broader introduction and use of smart radio technology.[49]

E. Information Accessible Through Rights Management

For most corporations using an enterprise architecture built around Internet technology, the key components of their network are: (1) local broadband access links; (2) an IP backbone network; and (3) "core application services" accessible to all authorized users. As noted above, this architecture does not necessarily require any reliance on the public Internet at all. Rather, by using Internet technology (or "Intranets," as they are sometimes called), corporations can connect their branch offices, partners, and customers. Any such network, however, would not make available all services to everyone with access to the network; supply chain partners, for example, would not have access to customer service records. To regulate who has access to what information, businesses use "rights management" technology to limit who can use particular services. In the context of public safety, for example, police officers would have access to a gang database, but fire fighters would not need such access.

The use of a rights management model for access to core applications is a classic feature of many Internet-enabled technologies. Notably, this platform is fundamentally different from (and superior to) today's specialized systems that provide little opportunity for customization,

---

(discussing Tropos' mesh networking wi-fi solution); IBM, *Alvarion to Deliver Wireless and WiMAX for Public Safety*, WIRELESS WEEK, May 11, 2006, http://www.wirelessweek.com/article/CA6333878.html?text=wimax (discussing Alvarion's solution using WiMAX).

49. As a review of the technological landscape explained:

> Since the cognitive radio technology enables the access to larger amount of spectrum, [cognitive radio] networks can be used for mesh networks that will be deployed in dense urban areas with the possibility of significant contention. For example, the coverage area of [cognitive radio] networks can be increased when a meshed wireless backbone network of infrastructure links is established based on cognitive access points (CAPs) and fixed cognitive relay nodes (CRNs). The capacity of a CAP, connected via a wired broadband access to the Internet, is distributed into a large area with the help of a fixed CRN. [Cognitive radio] networks have the ability to add temporary or permanent spectrum to the infrastructure links used for relaying in case of high traffic load.

Akyildiz, *supra* note 34, at 2135 (footnotes omitted).

evolution, or innovation. By so doing, it enables agencies to authenticate who is a permitted user and restrict their access to information—regardless of what underlying network they are using. Significantly, this model would allow considerable customization so that while the fire department might choose to share information with the local electric utility in one jurisdiction, it need not do so in another jurisdiction.

I recognize that rights management technology, as currently being used by commercial firms, is unlikely to meet all of the needs of public safety agencies. Consequently, once public safety agencies commit to use this architecture, there will be a need to drive the development of new standards to facilitate applications to meet their particular needs. Indeed, some efforts along these lines are already underway and, with an increased commitment to their use, others will progress much more effectively.[50] To be sure, the Department of Homeland Security's SAFECOM is encouraging such efforts by developing its Statement of Requirements,[51] but SAFECOM has tended to adopt a narrower conception of interoperability (as focused on the use of radios by traditional first responders).

To appreciate the opportunities for shared applications regulated by rights management technology, consider some of the initiatives underway in Maryland. At present, Maryland is prioritizing the development of technologies to enable electronic fingerprinting and biometric identification. This system, at least as envisioned, would enable state police officers to make criminal record checks from mobile data terminals in their cruisers as well as to transmit this information on an as needed basis.[52] If implemented on a shared network managed by rights management, however, this information could also easily be made available—on an as needed basis—to other agencies (say, local police).

---

50. One such effort underway involves a coalition of first responders working to develop an Extensible Markup Language ("XML")-based standard (i.e., the Emergency Data Exchange Language ("EDXL")). This system will enable a panoply of different agencies that might be called to the scene of an accident (i.e., public safety, transportation, and medical personnel) to share information with one another. Diane Frank, *First Responders Seek Common Lingo*, FEDERAL COMPUTER WEEK, Nov. 15, 2004, http://www.fcw.com/article84556.

51. *See* K.C. Jones, *Emergency Responders Can't Communicate, DHS Warns*, TECH WEB, May 11, 2006, http://www.techweb.com/wire/security/187202152 (noting that Department of Homeland Security "will set functional requirements and performance standards"). *See also* Press Release, U.S. Dep't of Homeland Security, Homeland Security First to Define Interoperability Requirements for Nation's First Responder Community (Apr. 26, 2004), http://www.dhs.gov/xnews/releases/press_release_0396.shtm.

52. Alice Lipowicz, *Buying Power*, WASH. TECH., Oct. 16, 2006, http://www.washingtontechnology.com/news/21_20/statelocal/29516-1.html.

The architecture described above—which is flexible, extensible, and based on IP technology—provides a far more effective means of ensuring both operability and interoperability than by simply providing more spectrum and more funds for traditional equipment. All too often, policymakers are addressing interoperability issues by looking in the rear view mirror, ignoring new technological opportunities, and failing to realize the underlying causes of interoperability. As Jon Peha has explained, "[o]ne cannot easily 'fix' interoperability as an afterthought to today's infrastructure, any more than one can easily 'fix' fuel efficiency on a racecar that was designed exclusively for maximum speed."[53] Unfortunately, as discussed in Part IV, developing and implementing appropriate technologies are only part of the solution, as the thousands of different agencies with jurisdiction to adopt unique information and communications technologies greatly complicates any efforts to improve interoperability.

IV. A FRAMEWORK FOR LEADERSHIP

Under the United States' governmental system, local agencies are both empowered—and indeed expected—to make individualized decisions about their information and communications technology needs. From the perspective of viewing public safety communications as an enterprise, the current model resembles a corporation where the marketing department adopts one email system while its legal department adopts another one, thereby complicating communications between the two and creating unnecessary inefficiencies.

To date, federal policy has yet to view public safety communications as an integrated system. Rather, policymakers have traditionally provided grants of money and spectrum to local agencies to use as they see fit—as opposed to using federal oversight to facilitate cooperation.[54] On account of the limited (if any) cooperation between different agencies, it should not be a surprise that the system of public safety communications infrastructure—designed by many thousands of independent decision makers—would produce "a tangle of systems that do not interoperate."[55]

In general, the current model in place for facilitating interoperability can be summed up with the mantra "more spectrum and more money" for local agencies. Indeed, the "Deficit Reduction Act of 2005," which is sometimes called the "plan of record" on public safety interoperability,

53. Jon M. Peha, *How America's Fragmented Approach to Public Safety Wastes Money and Spectrum*, Telecomm. Pol'y Res. Conf. (2005), at 15, http://web.si.umich.edu/tprc/papers/2005/438/Peha_Public_Safety_Communications_TPRC_2005.pdf.

54. *See* Peha, *supra* note 4, at 5.

55. Peha, *supra* note 8.

pursues just this strategy, providing more money ($1 billion for interoperability grants) and more spectrum (24 MHz of spectrum cleared as a result of the DTV transition) without addressing the more fundamental flaws of public safety communications. This strategy, however, will almost certainly ensure that we remain on the current path whereby public safety agencies are investing enormous sums of money into a technologically antiquated model. Fortunately, policymakers are increasingly appreciating the flaws of this model, recognizing that funding public safety agencies to the tune of $3 billion per year without developing a next generation technological architecture will leave public safety without the opportunities created by the Internet revolution.[56]

Equally important as developing an appropriate technological architecture is developing a framework for intergovernmental relations to spur coordination between a myriad of different agencies. To be sure, the use of IP networking provides a more flexible network architecture than the model used by current public safety radios. But that flexibility only *allows* firms to interoperate; it still takes leadership to *encourage* and *facilitate* interoperability. Indeed, without the proper leadership and incentives, local public safety agencies accustomed to making their own decisions are unlikely to cooperate and seek to interoperate with one another.[57]

The Alaska Land Mobile Radio system discussed above provides a vivid illustration of how cooperation and clear leadership about technology decisions can make an enormous difference.[58] Even though that system relies on digital trunking (and not the set of technologies championed above), the same success in facilitating coordination using that technology can be used to facilitate interoperability using new technologies. In that case, the major impetus for the project was federal money that was pegged to a coordinated system and leadership that believed in the project. Such pressures, as the ALMR case demonstrates, are necessary because people do lose some control when they cooperate and, other things being equal, will resist giving up that control without a fight.[59] Consequently, to drive

---

56. Lipowicz, *supra* note 52.

57. As numerous experts have related, "all the technology and money in the world will do little for interoperable communications unless the emergency responders are convinced that they should communicate with each other." Jackson, *supra* note 10.

58. In another promising effort, the Wireless Accelerated Responder Network ("WARN") project envisions allowing broadband access to a number of agencies and permitting interoperable, city-wide, real-time video tools for remote surveillance and detection. *U.S. Department of Commerce before the Committee on Homeland Security's Subcommittee on Emergency Preparedness, Science and Technology*, 109th Cong. (2006) (testimony of John M.R. Kneuer, Acting Assistant Sec'y for Commc'ns and Info. Admin.), *available at* http://www.ntia.doc.gov/ntiahome/congress/2006/Kneuer_interoperable_042506.htm.

59. As one observer stated with regard to new systems, "[p]eople are going to ask, 'Am

technology adoption, the federal government should use its control of money and spectrum more strategically, and states should be required to assume greater leadership in developing interoperability plans that will coordinate the information and communications technology needs of all relevant agencies.

A. The Federal Government

Traditionally, the federal government has viewed itself largely as an enabler of progress to be made at the local level. Consequently, the federal government has traditionally divided spectrum licenses into locality and agency-specific licenses and issued grants to the relevant agencies—as opposed to being managed or restricted by a statewide (or region-wide) program. In the case of spectrum, the decision to grant local licenses is particularly unfortunate in that it is coupled with a policy of forbidding the leasing of this spectrum, thereby creating the illusion that spectrum is free and reinforcing the notion that local public safety agencies should operate their own wireless networks. On account of such policies, as the House of Representatives Committee Investigating the Katrina Disaster concluded, "[s]tate and local governments [continue to be] responsible for designing and coordinating their efforts, and [have] failed to make meaningful progress *despite knowledge of the problem for years and the expenditure of millions in federal funds*."[60]

It is critical that the federal government recognize the need for strong incentives to encourage the embrace of a broader architecture that facilitates interoperability. As noted above, there is an understandable caution about relinquishing control and trying new technological approaches. But more than just this caution, there is a serious principal-agent problem that limits the attractiveness of the architecture described in Part III (or any architecture that would displace the traditional prerogatives of local agencies). In particular, the adoption of new technologies (such as those discussed in Part III) may clash with the self-interest of a local official who operates a public safety network and wants to continue doing what she knows well.

The federal government is well positioned to address the conflict of interest problems by dispelling the plausible reasons for sticking to the old technology and by providing incentives for states to forge a new path

---

I going to lose any power or control?' Everyone has a little less control but, overall, they have better capability. Once you get past the egos, it all makes sense." Jackson, *supra* note 10.

60. A Failure of Initiative: The Final Report of the Select Bipartisan Comm. to Investigate the Preparation for and Response to Hurricane Katrina, H.R. Rep. No. 000-000 at 174 (2006), *available at* http://www.c-span.org/pdf/katrinareport.pdf (emphasis added).

ahead. In terms of the objections to shared networks, a regular refrain of local public safety officials is that such networks (say, those using IP technology) often fall short on the reliability and security fronts. This objection, however, fails to appreciate that large numbers of critical mission networks rely on commercial off-the-shelf equipment and commercial networks that use Internet technology. Moreover, the flexibility of such networks, particularly when part of an extensible architecture that includes legacy equipment, promises levels of redundancy that far exceed the capability of current networks.

A recent Aspen Institute report highlighted that policymakers championing a next generation technology for public safety must overcome a "culture of resistance." In particular, the conference report (quoting Charlottesville Fire Department Chief Charles Werner), explained:

> the history of fiefdoms within the respective agencies obscures the "gains from cooperation." In many cases, managers of legacy radio systems tell chiefs that "you need to stick with the traditional land mobile radio system" or the system won't remain secure. To be sure, education and demonstration projects are part of the answer because there is a basic lack of understanding about how modern networks are designed and managed—for example, security stems from effective encryption, not physically separate networks. Yet education alone will not do the trick. As Chief Werner recounted from his experience, getting beyond the silo-based approach is starting to happen where incentives for cooperation—in the form of federal grants—create opportunities to bring together groups of distinct agencies and individuals through consensus-building leadership.[61]

Moreover, this report also emphasized that the failings in cooperation are not limited to public safety communications, but also cover related failings in government usage of technology (such as E-911 systems).[62]

The federal government's reorientation of its model for issuing interoperability grants and licenses for spectrum would be a crucial step in creating powerful incentives for agencies to adopt new technologies and facilitate interoperability. This change should be accompanied by the federal government's leadership in developing the technologies noted above and promoting state leadership and coordination to spur that transition, including the use of accountability metrics that ensure federal funds are spent effectively. Moreover, during the early stages of promoting

---

61. *See* Philip J. Weiser, Clearing the Air: Convergence and the Safety Enterprise 24–25 (The Aspen Institute 2006) *available at* http://www.aspeninstitute.org/atf/cf/%7BDEB6F227-659B-4EC8-8F848DF23CA704F5%7D/C&S%20FINALAIRSREP06.PDF.

62. *See id.* at 25. *See also* DALE HATFIELD, A REPORT ON TECHNICAL AND OPERATIONAL ISSUES IMPACTING THE PROVISION OF ENHANCED 911 (2002), *available at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513296239.

the new technologies, the federal government can play a critical role in supporting demonstration projects and publicity for best practices to encourage states to begin to embrace the opportunities available in public safety communications.

In terms of the federal government's leadership in developing new technologies, there is an increasing awareness that the federal government must assume a leadership role in spurring interoperability. For starters, there is an increased recognition that certain standards development activity should be supported at the federal level.[63] Similarly, there is a growing awareness of the value of investigating the potential of emerging technologies.[64] Indeed, the National Institute of Justice is already pursuing this course, as it "has made significant investments in new technologies such as SDR, cognitive radio, and satellite communications for rural agencies."[65]

To ensure that the federal government's technological leadership role is most effective, it should be guided by a basic reference model—based on the technologies discussed in Part III—that will guide the public safety communications systems of the future.[66] Such a model would outline the basic technological architecture (and set of technologies) that public safety agencies would use to communicate and manage their information needs. This system, moreover, would leave some discretion to state and local authorities, but would insist on certain requirements and components that are necessary to enable effective public safety communications. The model would, for example, emphasize that a broadband access link is critical, but it would not necessarily dictate what type of technology or strategy would be used to provide this link.

With a reference model in mind, the federal government should develop a hierarchy of critical steps for individual state-led systems to embrace. This hierarchy would take the form of a set of envisioned outcomes and specific metrics that would be used to measure progress. The federal government is well positioned to bring together the affected stakeholders to identify the currently available technologies and best

63. The National Emergency Management Reform and Enhancement Act of 2006, for example, would require that the Department of Homeland Security develop the necessary voluntary consensus standards in three years to facilitate a migration to a next generation architecture. Moreover, the bill would also call for enhanced state leadership—in the form of interoperability plans. *See* H.R. 5351, 109th Cong. (2d Sess. 2006).

64. Peha, *supra* note 4, at 15.

65. *The State of Interoperability: Perspectives on Federal Coordination of Grants, Standards, and Technology Before the Comm. on Homeland Security*, 109th Cong. 3 (2006) (statement of John S. Morgan, Assistant Dir. for Sci. and Tech., Dep't of Justice), *available at* http://www.ojp.usdoj.gov/ocom/testimonies/morgan_test_060425.pdf.

66. *See* Weiser, *supra* note 61.

practices that could inform such an action plan. Again, this action plan would not require an abandonment of legacy systems or a one-size-fits-all solution, but it would require the migration toward an overall flexible and extensible architecture that leverages technologies currently being used by commercial firms.

To do its part, the Federal Communications Commission ("Commission") should gear its spectrum policy decisions to spur the adoption of the architecture outlined above. First, the Commission should ensure that any decision to award spectrum licenses to local agencies is conditioned on participation in a state or regional plan to migrate to a next generation architecture. Such a step would dovetail nicely with the Commission's current practice of requiring the local public safety agencies to operate under the oversight of regional frequency coordinators, which seek to limit interference and facilitate cooperation. Second, the Commission should investigate possible strategies for facilitating the development of a next generation broadband interoperable architecture. Third, the Commission should investigate strategies for better organizing the planned assignment of additional safety spectrum in the upper 700 MHz band to enable broadband networking, either on spectrum dedicated to public safety alone or in a manner that would integrate with commercially available spectrum. Finally, the Commission should consider allowing secondary markets for public safety users, thereby allowing users to both access and lease spectrum pursuant to secondary market rules.[67]

B. Empowering State Leadership[68]

The federal government should no longer provide funds directly to local agencies. Such a strategy only invites and facilitates the lack of cooperation that has plagued public safety communications to date. Rather, the federal government should work directly with state governments to spur them to take a leadership role in ensuring greater levels of operability and interoperability among public safety communications systems.[69] Over time,

67. In particular, allowing public safety spectrum to be leased—say, on an interruptible basis—may raise additional revenue, create robust networks with enhanced functionality, and reveal the opportunity costs of leaving this spectrum inefficiently used. *See* Marsh, *supra* note 46.

68. This section largely reflects the discussion contained in the Aspen Report. *See* Weiser, *supra* note 61.

69. To be sure, some state governments are already moving in this direction (with support from the National Governors Association Policy Academy on Wireless Interoperability), but federal encouragement is critical to ensuring more consistent and effective leadership. *See* NASCIO, WE NEED TO TALK: GOVERNANCE MODEL TO ADVANCE COMMUNICATIONS INTEROPERABILITY 2–3 (Nov. 2005), *available at* http://www.nascio.org/publications/documents/NASCIO-InteropGovResearchBrief.pdf.

the money and spectrum provided to states should be conditioned on the development of a coordinated strategy and the effective management necessary to make it happen. By so doing, the federal government can create powerful incentives for states to empower an official—say, a state chief information officer ("CIO")—to facilitate cooperation and the development of an integrated strategy.

The federal government should publicize its findings as to state progress and ensure that states are held accountable by the court of public opinion. Over time, once some states begin to lead the way in migrating toward a new technological architecture, the federal government can act as a referee of yardstick competition between states and enable transparent assessments of how different states are progressing toward a next generation architecture. Thus, for example, when forty states have adopted IP backbone networks that connect all public safety agencies, E-911 calls, and others working in conjunction with first responders (say, ambulance dispatch services), it will put considerable pressure on the ten remaining states that have yet to do so. Moreover, the federal government should perform regular audits to evaluate which states are using communications and information technology effectively.

The critical role for state governments is to develop the skills necessary to oversee an integrated emergency communications strategy. Ideally, this strategy would take a broad view of emergency response, including the current state of E-911 technology. In any event, it would certainly commit to developing shared resources where appropriate and would ensure that all federal and state funds were invested to advance the migration to a next generation architecture.

Leadership at the state level can make an enormous difference in driving adoption of advanced technologies that will provide for greater functionality and affordable systems. To spur such effective leadership, each state should appoint a single official (say, the state CIO or an emergency management head) to oversee the development of a statewide plan to migrate toward a next generation architecture. Based on the efforts of some states to better leverage the use of information and communications technology through an empowered and centralized CIO (where all IT employees worked for a single agency), there are strong reasons to believe that such a model can succeed in this area.[70]

The challenge for ensuring effective emergency communications is that public safety agencies should act more like enterprise customers, requiring certain functionalities and not specifying particular technologies

70. *See, e.g.*, Tod Newcombe, *Leaving His Mark*, PUBLIC CIO, Nov. 8, 2005, *available at* http://www.public-cio.com/story.php?id=2005.11.08-97208.

that they must control and maintain. State or federal agencies can move to this model by developing Request for Proposals ("RFPs") and requirements documents that can be used by local agencies to procure the needed services and to take advantage of shared investments in information and communications technology. Increasingly, most local public safety agencies are ill-prepared to judge the potential of modern technology—let alone to integrate it in an effective fashion. Thus, even as to the deployment of broadband access networks (an inherently local task), most local agencies will be best served by following the strategies used by larger and more sophisticated entities (say, New York City) to the extent that their strategy for building out broadband networks can work for them.[71]

V. CONCLUSION

The current strategy for addressing the failings of public safety communications is essentially to make incremental progress through the implementation of digital trunking arrangements. To be sure, this step constitutes important progress and, as demonstrated in the ALMR case, can lead to important improvements. It represents, however, only a piecemeal solution to a problem that rests on the flawed foundations of a system of public safety communications that resists changes and implements solutions in a localized manner. The ultimate solution is to break away from the prevailing culture around public safety communications both with respect to its aversion to new technologies and to its resistance to oversight and accountability.

A number of emerging technologies promise to transform public safety communications into a system that is far more flexible and extensible than the current model. Unfortunately, over the last ten years, localities have spent tens of billions of dollars upgrading their communications capabilities by buying replacement equipment that, like its predecessors, was specialized and thus technologically limited. Over the next ten years, multimode radios, IP-based technology, broadband communications, cognitive radio systems, and rights management technologies all promise to transform public safety communications and to set it on a new path of technological development. In so doing, these technologies—which can be implemented alongside legacy systems—will afford agencies interoperable, secure, reliable, redundant, and high-performance communications systems.

71. Just recently, New York City announced its plan for a $500 million wireless broadband network that would facilitate the sharing of antiterrorism databases, fingerprints, mug shots, maps, and video. *See* Claudia Parsons, *NYC Orders $500 Million Emergency Data Network*, PERI, Sept. 12, 2006, *available at* http://www.riskinstitute.org/PERI/NEWS/NYC+Orders+500+Million+Emergency+Data+Network.htm.

The United States' commitment to localism and resistance to centralized authority is often a virtue. In the case of public safety communications, however, the lack of centralized oversight and coordination—at least on a state level—is highly problematic. Left to their own devices, local public safety agencies often live comfortably in an isolated and antiquated technological environment. Consequently, the federal government must spearhead an initiative where—backed by state oversight and responsibility—local agencies migrate to a new technological architecture and federal incentives (both grants and spectrum) spur them to do so. Ultimately, the power of this new architecture promises a far more functional and efficient public safety system. But many of the operators of the current system will not abandon the current model unless pushed to do so, and thus it is critical that the federal and state governments not engage in bottom-up leadership, but rather consult with local agencies as to their particular needs and incentivize them to adopt new technologies that will meet them.