

Telecommunication and Public Safety Post 9/11

by Paul P. Josephson

Ever-evolving communications technologies present every person and organization with a bewildering array of choices among technologies, devices, providers, operating systems, features, speed, and cost structures. As soon as we think we have figured out the most effective and efficient technologies for our needs, another technological breakthrough reshapes the entire field. If not square one, we have to go back and figure out whether we need that new technology and how to pay for it.

These changes in modes, methods and the commercial terms of communications dominate the business news. They are reshaping industry after industry.

Leveraging these new communications technologies is perhaps nowhere more critical than for public safety and first responders—police, fire, EMS and others with mission-critical communications needs. First responders need fully interoperable communications systems that allow them to speak with each other in times of crisis, when the cell phone network is down or overloaded by civilian traffic. They need to be able to plug-and-play new technologies into those systems with minimal upgrade costs. They need to take advantage of new technologies as quickly as possible.

Today, the average citizen can shoot and post to the Internet video of a tornado or civil disturbance while it is in progress. It can be viewed worldwide, while it is happening, and can go viral within hours via Twitter, Facebook, and other social media platforms. But can police or fire units from different towns speak directly with each other when responding to that same incident? Can they send their own video back to a central command center for superiors to make critical decisions about how best to defuse that disturbance? Can a helicopter surveilling a disaster scene from above send video of the scene to responders on the ground to enhance their search and rescue efforts?

Just as the average consumer wants the newest smartphone with the latest features the public safety community wants and needs access to the latest communications technologies.

This race to embrace new technology has been especially important since the events of Sept. 11, 2001, when we discovered the need to improve voice and data communications among public safety agencies and their first responders, to allow public safety agencies to communicate with each other despite differing technology choices, and to be sure critical data in the government's possession can be accessed by public safety in real time.

These technologies are changing how police and other public safety officers work. Not so long ago, a typical police cruiser contained little more than a radio communications unit in the way of technology. An officer responding to a crime or pulling over a vehicle typically had to radio license plate information to a dispatcher to obtain information in the course of a traffic stop, and then either fill out a report in longhand with carbon copies or travel to the station to type a written report. Today, the typical police cruiser is packed with technology—license plate readers that can scan every plate around the cruiser as it rolls and alert the officer to vehicles that have been reported stolen or with outstanding violations, video recorders, wireless streaming of that video, GPS to track the cruiser or suspects, and laptop computers to document and generate reports on the scene. Each device can dramatically improve efficiency and accountability.

A 2011 survey by the Police Executive Research Forum¹ highlighted the number of national police agencies using the following technologies:²

- In-car video recording: 71 percent in some vehicles, 25 percent in all
- Wireless video streaming: 46 percent
- License plate readers: 71 percent
- GPS to track police vehicles: 69 percent

Likewise, firefighters now have access to technology that can give field commanders access to building plans and inspection reports that can prove invaluable to directing first responders in an emergency. In fact, the precise location of

individual firefighters within a burning building can be monitored on scene by commanders.

Each of these new public safety technologies is highly dependent on communications infrastructure to work effectively. No longer does public safety simply require a voice connection by radio; now officials need data connections with tremendous bandwidth to make effective use of these technologies. They need secure systems that will function as well in times of crisis as they do in ordinary day-to-day situations.

Society's burgeoning data demands have led to a scramble for spectrum to accommodate all of these technologies, in both the civil and public safety arenas. This scramble for communications spectrum is of vital importance to the public safety community, and also to the public entities that must make significant financial investments in the technology, hardware, and infrastructure that makes it all work.

Thus, attorneys representing public entities, as well as those representing technology vendors selling to the public sector, face a new set of challenges that law school did not prepare them for—what technologies to acquire, what communications platforms to select, and how to contract to obtain the hardware, software and communications infrastructure in a cost-effective manner.

Unfortunately, New Jersey's public procurement methods, like those in many states, especially at the local and county levels, do not provide the flexibility needed to quickly acquire these technologies, or to change course if technologies change while procurement is pending.

This article highlights key recent developments practitioners need to be aware of to help public safety clients respond to and manage rapid changes in the area of public safety communication technology.

Interoperability

Interoperable emergency communication is integral to initial response, public health, safety of communities, national security and economic stability. Of all the problems experienced during disasters, one of the most serious concerns is the lack of appropriate and efficient means to collect, process and transmit important and timely information. In some cases, legacy radio communication systems are incompatible and inoperable, not only within a jurisdiction but within departments or agencies of the same community. Non-interoperability can result from outdated equipment, limited availability of radio frequencies, isolated or independent planning, lack of coordination and cooperation between agencies, community priorities competing for resources, funding, ownership and control of communications systems.

Recognizing and understanding this need, Project 25 (P25) was initiated in 1989 by public safety agencies and manufacturers of digital radio communication.³ P25 is a collaborative project to ensure that two-way radios are interoperable. The goal of P25 is to enable public safety responders to communicate with each other and, thus, achieve enhanced coordination, timely response, and efficient and effective use of communications equipment.

P25 is an open-source standard that allows different radio communications systems across North America to speak with each other, adopted through the joint efforts of the Association of Public Safety Communications Officials International (APCO), the National Association of State Telecommunications Directors (NASTD), selected federal agencies including the National Telecommunications and Information Administration (NTIA), the National Communications System (NCS), the National Security Agency (NSA) and the Department of Defense (DoD). It was standardized under the Telecommunica-

tions Industry Association (TIA).

The P25 suite of standards involves digital land mobile radio (LMR) services for local, state and federal public safety organizations and agencies. P25 is applicable to LMR equipment authorized or licensed in the U.S. under NTIA and Federal Communications Commission (FCC) rules and regulations. (Europe has established an equivalent common standard, the European terrestrial trunked radio (TETRA) protocol, although TETRA equipment is not interoperable with P25 equipment.)

Although developed primarily for North American public safety services, P25 technology and products are not limited to public safety alone, and have been selected and deployed in other public services, as well as private system applications. Transportation and public works departments, public and private utilities, and transportation networks such as rail facilities are prime candidates.

Since Sept. 11, the federal government has made substantial funding available to the states through numerous grant programs to enhance the interoperability of public safety radio communications systems. The Public Safety Interoperable Communications (PSIC) Grant Program⁴ led to the award of \$968,385,000 to fund interoperable communications projects in the 56 states and territories. This represents the largest single infusion of federal funding ever provided for state, territory, and local agencies to implement communications solutions. In most cases, public entities relying on federal grants (or state grants funded by the federal government) today must procure P25-compliant technology and equipment.

New Jersey's P25 Network

Since the events of Sept. 11, New Jersey has been at the technical forefront of shifting to an interoperable, digital future. State agencies including the Office of Information Technology (OIT),

the State Police, the Office of Homeland Security and the Department of Transportation have, over the past decade, invested tens of millions of dollars in various federal grant funds the state received into a statewide radio communications network known as the P25 Network.

In 2012, OIT began deploying the P25 Network, a 700 MHz digital trunked radio communications network that provides 95 percent coverage statewide. One side of the network is designed to accommodate state agencies, while the other side can accommodate county and municipal users. The state has launched a website dedicated to the P25 Network.⁵

Together, the network represents perhaps the ultimate shared service arrangement undertaken by the state to date. In the past, counties and individual municipalities typically built and designed their own freestanding communications systems that might—or might not—be interoperable with neighboring entities. These systems, consisting of antenna sites, control centers, dispatch centers and associated equipment, typically cost tens of millions of dollars to properly design, build, operate, maintain and upgrade to the latest technology.

Now, counties and municipalities can avoid many of those infrastructure costs by participating in the statewide P25 Network. Significant cost savings can be expected from participating in the statewide network. Because it will be subscription-based, there will be far lower infrastructure costs to network participants. Municipalities will benefit from the economy of scale that can be leveraged with a single infrastructure, as well as ongoing technology enhancements and upgrades that will be procured by the state for the system. Participating municipalities and counties can add existing or new facilities to the statewide network to enhance coverage rates for their specific needs.

The P25 Network represents perhaps

the lowest-cost option for towns to become interoperable and to take advantages of the technology investments the state makes for the benefit of State Police, DOT and other first responders. While procurement methodologies are still being worked out, it is anticipated towns will be able to procure their equipment and installation services off current and pending state radio communications contracts, without the need to conduct their own procurements.⁶

In keeping with New Jersey's policies, home rule options remain, however. Counties or municipalities that have their own radio network can still maintain it while linking to the P25 Network to achieve statewide interoperability. Presently, local officials have been provided guidance by the state that such systems generally must be procured through the traditional low-bid methodology. The low-bid methodology is ideally suited for purchasing essentially identical commodity goods (paper, milk, etc.) and construction services. But when applied to procure complex technical systems, it can force a public agency to buy the cheapest system offered rather than the one that offers the best value and best suits the agency's specific needs. Of course, lowest cost does not necessarily mean best value when it comes to technology. Low bidding also prohibits cost and technical negotiations that can help refine bidders' proposals to best suit the agency's needs.

From a policy perspective, serious questions can be raised regarding whether low bidding should be required in these cases, given the advanced technical and professional skills associated with designing and installing these systems. Certainly the state does not use low-bid methodology for procuring its complex technology systems, as a consequence of state law that allows for vendors to be selected based on the best value to the state,

price and other factors.⁷

State law presently permits towns and counties, upon resolution, to use the 'competitive contracting' process, which permits award to the bidder who best satisfies evaluation criteria rather than merely the lowest price, in certain cases.⁸ These cases include professional services, 'special equipment for confidential investigation,' 'extraordinary unspecifiable services,' and 'operation, management or administration of data processing services,' and upon approval of the director of Local Government Services, other services.

Depending on the scope of engineering design services included in a contract for a radio communications system, as well as whether the operation of the communications system is to be outsourced as part of the contract, the agreement might be eligible for competitive contracting.

One solution is legislative amendments authorizing competitive contracting and negotiations for public entity communications technologies that provide local public agencies flexibility to seek competition among vendors and select the best technology, provider and terms for their specific needs.

Second, communities should consider retaining highly qualified communications consultants to guide them through the maze of technology options and to assist in developing procurement documents. Communities should also contact OIT and thoroughly investigate the significant advantages of joining the state's P25 Network before making any new communications investments.

FCC Spectrum Issues and FirstNet Authorization

The establishment of a national communication network for first responders is one of the final outstanding recommendation of the 9/11 Commission, which was led by two eminent New Jer-

seyans, former Governor Thomas Kean and former Attorney General John Farmer.

If the three most important factors in real estate are location, location, and location, the most important factors in radio and data communications are spectrum, spectrum and spectrum. Wireless carriers, broadcast radio and television operators, and public safety, public service and business users all compete for the same finite radio spectrum to provide for the nation's exploding digital data needs.

The FCC serves as the nation's communications traffic controller, assigning appropriate uses for various bands within the spectrum, and licensing individual agencies to use specific frequencies within those bands for their needs.

As noted above, public safety users have many new data-intensive technologies available to them. Obtaining the needed bandwidth to carry that data is critical to the success of the technology. Consider a football game at the Meadowlands where many fans are trying to send video of a play to their friends via smartphone; too many users competing for the same cell site will overwhelm the site, and users either cannot access the cell network or experience extremely sluggish response times.

While a delay in sending the latest Eli Manning triumph to friends can be tolerated, public safety cannot tolerate delays during emergencies.

For this reason, when the FCC moved over the air television broadcasting to digital, the commission dedicated portions of the 700 MHz radio band to public safety users, and allocated a total of 12 MHz for narrowband, P25 voice use.

With respect to public safety data needs, New Jersey was at the forefront of the broadband communications revolution. The state was one of a handful of jurisdictions nationally to secure a special Broadband Technology Opportunities Program grant (BTOP) to establish a

new broadband network for public safety data use on the 700 MHz band in Northern New Jersey, for 30,000 public safety users. Other BTOP recipients included Los Angeles; San Francisco; Charlotte, N.C.; Mississippi; and New Mexico. The state was awarded \$43 million for its broadband network efforts, and in 2011 received proposals for a new broadband system. But shifting federal policy has halted the state's procurement.

As a result of legislation enacted in Feb. 2012, Congress established the First Responder Network Authority (FRNA, or FirstNet) as an independent authority within NTIA to establish a nationwide, interoperable public safety broadband network.⁹ The legislation provides \$7 billion in funding for this network out of anticipated spectrum auctions in the future. As part of this law, each governor has the option to decide whether to opt in to the FirstNet system, or to develop and deploy its own broadband radio access network.

As part of this legislation, Congress reallocated the 10 MHz so-called 'D Block' to public safety data uses, to provide a total of 32 MHz of spectrum for public safety use. 20 MHz is reserved for broadband (data) use; the other 12 MHz is reserved for narrowband (voice) use.

The authorization of FirstNet, critical to advancing interoperability nationwide, has unfortunately had the negative impact of halting New Jersey's cutting-edge efforts to launch its regional broadband data network. The FCC has frozen the use of BTOP grant monies by jurisdictions like New Jersey until it decides how best to use those funds in light of the new FirstNet authority.¹⁰ FirstNet will take several years to launch; in the meanwhile communications leaders like New Jersey are pushing aggressively for federal guidance to allow them to use those monies to advance their public safety broadband efforts now.

The so-called D Block Spectrum Act

and FirstNet network have no impact on most existing public safety radio systems nationally, except that the act requires public safety users on the UHF T-Band between 470-512MHz (where digital television signals are now broadcast) to vacate that spectrum within approximately nine to 11 years.

This impact does affect New Jersey public safety users, many of whom are currently licensed and equipped to run their systems in the UHF T-Band. When digital television was mandated by the FCC, many public safety users in New Jersey who had been licensed to use the UHF band began to experience significant interference from digital television signals.

In seeking to acquire the newest interoperable technologies, communities licensed to use UHF spectrum between 470 and 512 MHz rather than the 700 MHz band must make a choice: whether it is better to invest in technology optimized for their current licensed UHF spectrum but likely to become obsolete within a decade, or move now to the 700 MHz band as part of upgrading their systems. Many of these users are choosing to move to the 700 MHz band.

By moving to the state's P25 Network, which also operates in the 700 MHz band, public agencies may be able to achieve considerable savings when upgrading their technology, and avoid obsolescence issues inherent in staying on the UHF T-Band.

Conclusion

The only constant in the field of communications technology is change. Public safety agencies and governing bodies need to plan for change just as they plan for emergencies, taking the time to understand the changing field to make the wisest communications investments. Qualified communications consultants can help them understand the best options for their current and anticipated voice and data needs.

As a place where so many historic communications breakthroughs were made, it should come as no surprise that New Jersey has been at the forefront of efforts to establish a framework for public safety communications in the digital world. The state's public safety and technology leadership recognize the need to be proactive but smart in the investments they make, evidenced by New Jersey's shared service P25 Network for voice communications.

Given the high costs of going it alone, any town or county trying to plan for the future should keep a close eye on the state's initiatives in the coming months, and give serious consideration to joining the state's communication systems as the cheapest and best way to access the latest technical advances for both voice and data needs. ↻

Endnotes

1. Founded in 1976 as a nonprofit organization, the Police Executive Research Forum is a police research organization and a provider of management services, technical assistance, and executive-level education to support law enforcement agencies.
2. Police Executive Research Forum, "Use of Technology in Policing: The Chief's Perspective," April 4, 2011. Over 70 police agencies with an average population of 531,011 responded to this survey. See www.policeforum.org/library/critical-issues-in-policing-series/perfpresentation.pdf.
3. See www.project25.org.
4. Created by the Deficit Reduction Act of 2005 (Public Law 109-171), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53) and by Public Law 111-96.
5. See www.nj.gov/911/p25.
6. See www.nj.gov/911/p25/index.shtml.
7. See N.J.S.A. 52:34-12; N.J.A.C. 17:12-2.7.
8. N.J.S.A. 40A:11-4.1, *et seq.*
9. See Middle Class Tax Relief and Job Creation Act of 2012, Public Law 112-96, Feb. 22, 2012. www.nita.doc.gov/category/public.saftey.
10. Police Networks Hit U.S. Roadblock, *Wall St. J.*, at A4 (July 30, 2012).

Paul P. Josephson is partner-in-charge of the regulatory and government practice group at Hill Wallack LLP in Princeton.