



16842 Von Karman Avenue, St.200,
Irvine, CA 92606
www.ipmn.com

PUBLIC VS. PRIVATE DATA SYSTEMS

Public networks seem like the easy way to affect mobile data communications quickly, easily, and cheaply. But first impressions can be deceiving.

While municipalities do not have to purchase radio infrastructure to operate on public networks, they do have to invest in hardware (the modems in the vehicle), and continue to pay for service over the life of the system. With the demise of the carrier's CDPD services, agencies are forced to transition to the new technology, often having to bear the cost of the new hardware required to operate on the new system. In addition, the recurring charges are typically much higher. Since the carrier's technology decisions are driven by consumer subscribers, the carriers are likely to force similar changes in the future. Private ownership ensures that technology migration happens when your schedule and budget allows, not by the carrier's timetable.

CONTROL

In times of emergency, you need guaranteed access to your mission critical data. With private systems, owned and operated by a public safety or municipal agency, you are in control. As the recent power outages in the North East United States and hurricanes in Florida demonstrated, public carrier systems are very susceptible to power failures and other natural disasters.

With a private radio system, an agency or municipality can make the system as redundant and fault tolerant as resources permit. IPMobileNet offers several options for enhancing system redundancy and reliability, including a hot-standby IPNC. Private radio tower sites are typically outfitted with emergency power sources (such as a UPS) that guarantee reliable voice and data communications in the event of power failure. Because cellular tower locations and construction are driven by consumer forces, there is little impetus for cell phone companies to upgrade their tower site infrastructure, or devote resources to redundancy.

Owning your own system also means owning your own frequency. When a wide-scale emergency strikes (such as earthquake, weather condition, breach in homeland security, etc.), people naturally reach for their cell phones to make sure their family and friends are safe. This kind of cellular traffic was seen during each of the Los Angeles earthquakes in the 1990's and Florida hurricanes of 2004. Frequencies quickly become congested with cellular telephone users, and no cell phone or data communications can get through. Even during a localized emergency, cellular antennas (including GPRS) become overloaded with requests to talk, and effectively shut down. Voice traffic has priority access in public carrier systems, and so public safety data will always lose to a voice user trying to get on the system. Private RF systems provide clear channels for mission critical communications.

COVERAGE

With public data systems, agencies and municipalities must accept the wireless coverage that is provided. Adding new cellular base stations can be difficult due to political and zoning issues. Additionally, cellular providers have no incentive to add a



tower in rural areas where there are few cell phone users. Police and fire however, require coverage in woodlands, lakefronts, and undeveloped lands. With private RF, base stations can be added to fill coverage holes in hard-to-reach areas.

The phenomenon known as “cell breathing” is perhaps the biggest coverage challenge for public networks. “Cell breathing” is the expansion and contraction of cell coverage from any given cell tower, depending on how many users (voice or data) are accessing the tower. As more voice and data users are on the tower, the area that the tower is able to cover shrinks significantly. In the event of an emergency, not only is public safety not guaranteed an open channel for data, the public safety vehicle may no longer be in range due to changing cellular coverage.

DATA RATES

There is a common myth that public data systems like GPRS have a higher data rate than private radio systems. This is simply not true. In a field test, as part of a competitive evaluation of mobile data products for a state contract, the IPMobileNet 19.2 Kbps system had significantly greater throughput than the local cellular network. In fact, the IPMobileNet system was determined to be faster than competitors, private and public systems, many of whom claimed higher than 19.2 Kbps data rates. Public network latency (the time a user requires to gain access to the channel) outweighs any signaling rate advantage for typical public safety dispatch operations.

IPMobileNet’s 32Kbps product provides increased data rates and significantly increased throughput. Importantly, the IP Series 32 mobile data products provide synchronous 32 Kbps uplink and downlink data rates. Other systems have high data rates for downlink (wireless communication from the base down to the mobile), but 19.2 Kbps uplink rates (from the mobile to the base station). The benefit of 32 Kbps uplink and downlink is that it increases the aggregate throughput of the system. The throughput for public systems is highly variable, depending on how many users are on the system at any given time.

CONCLUSION

The abandonment of CDPD is a hard lesson for many agencies. Agencies are forced to adhere to the carrier’s timetable, so the agency must find funding to either move to a private RF system or to purchase new modems for public networks. Don’t be left out in the cold. If public safety voice communications cannot rely on cellular networks for their critical communications, why should you risk your data communications to the same unreliable infrastructure?



Public and Private Network - Summary

Public

Not Secure

Shared facilities and control systems

Carrier-defined coverage and capacity

Designed for general use, open access

Vulnerable to scene of incident overload

Low start up cost

Carrier control of technology migration

High latency, erratic availability

Private

Secure

Dedicated facilities and control systems

Agency-defined coverage and capacity

Mission-critical design for access priority and security

Immune to scene of incident overload

Lowest life cycle cost

Agency control of technology migration

Low latency, high availability