# Mission-Critical Push-To-Talk (MCPTT): A Brief Summary

Oregon SIEC Technology Committee

## Executive Summary

This white paper provides a brief introduction to the concept of cellular wireless-based push-to-talk (PTT) services and their use by public safety agencies. It is intended to be a vendor-agnostic presentation at a high level and does not endorse or recommend any specific vendor or product. The anticipated audience for this white paper is technicians, managers, and decision-makers at public or private organizations with a public safety nexus looking for basic information about push-to-talk services.

## Definitions

**Push-to-Talk (PTT)**: A function that mimics the near-real-time **one-to-many** and **one-to-one** voice communications found in modern public safety radio systems. For this white paper, we are specifically using PTT defined as a service over 3G/4G-LTE/5G cellular data networks, while recognizing that it can also be extended to applications on other wired and wireless networks.

**3rd Generation Partnership Project (3GPP)**: An international partnership composed of seven different national/regional telecommunication standards organizations. Originally formed in 1998 to develop technical standards for 3G Mobile broadband based on GSM cellular networks, the group continues to maintain and develop technical standards for evolving mobile broadband technologies. For more information on 3GPP and its various standards, please see: https://www.3gpp.org/

**Mission-Critical (MC)**: Colloquially, this term is used to describe services, hardware, and functions assigned to individuals and organizations with a core role in protecting people, property, and the environment. First responder communications are generally the primary example of "mission critical". More information on the full spectrum of mission-critical services embraced and advocated for by 3GPP can be viewed here: https://www.3gpp.org/news-events/3gpp-news/mc-services

**Mission-Critical Push to Talk (MCPTT)**: An application-specific standard, published by 3GPP in 2016, describing how a PTT system over existing cellular and Long-Term Evolution (LTE) networks should be implemented to serve the public safety and first responder community. MCPTT is designed to provide one-to-one and one-to-many communications identical to current **public safety** land-mobile radio (LMR) networks while also leveraging the wide-area coverage of Internet Protocol (IP) based networks. MCPTT is a subset of the larger IP-based PTT ecosystem.

**Land Mobile Radio (LMR)**: A generic term that describes one-to-one and one-to-many voice communications systems that operate over radio frequency (wireless) network. A catch-all term that includes simplex (person to person) operations, simulcast/multicast networks, and trunked radio systems. Encompasses nearly all public safety radios in use today.

**Gateway:** In radio engineering, a device that allows access from one network to another. Includes both voice/analog gateways, which take audio from one source/frequency and retransmit it on another source/frequency, and devices that convert analog (or digital encoded voice data) into data and transmit it over networks to other devices. A gateway, also known as an interconnect, is necessary to allow PTT applications on LTE networks to connect to existing LMR systems.

**Bring-your-own-device (BYOD)**: An IT service concept where a software application is made available to users on personally owned devices such as cell phones, tablets, or computers. BYOD solutions can be

cheaper and easier for organizations to implement, but bring challenges in information security and data retention that are not as easily controlled as with organization-provided devices.

## The Basics of PTT and MCPTT

### How Push-to-Talk works

PTT consists of an end-user application installed on mobile devices that then works with a cellular (3G/4G/LTE/5G etc.) data network. Audio signals and data (including multimedia, telemetry, and location services) are sent over the Radio Access Network (RAN) to a PTT core server. This core can be hosted by a cellular provider on their network or in the cloud by application service providers. Functionally, PTT services are just an extension of how smartphones normally work. For "mission critical" applications, the **core is often separate from the carrier's other network applications** and interconnected via virtual private networks (VPN). In the case of FirstNet, MCPTT operates on LTE Band 14, which is bandwidth dedicated to first responders and public safety. Figure 1 (below) illustrates a schematic of a typical PTT system implemented over cellular networks.

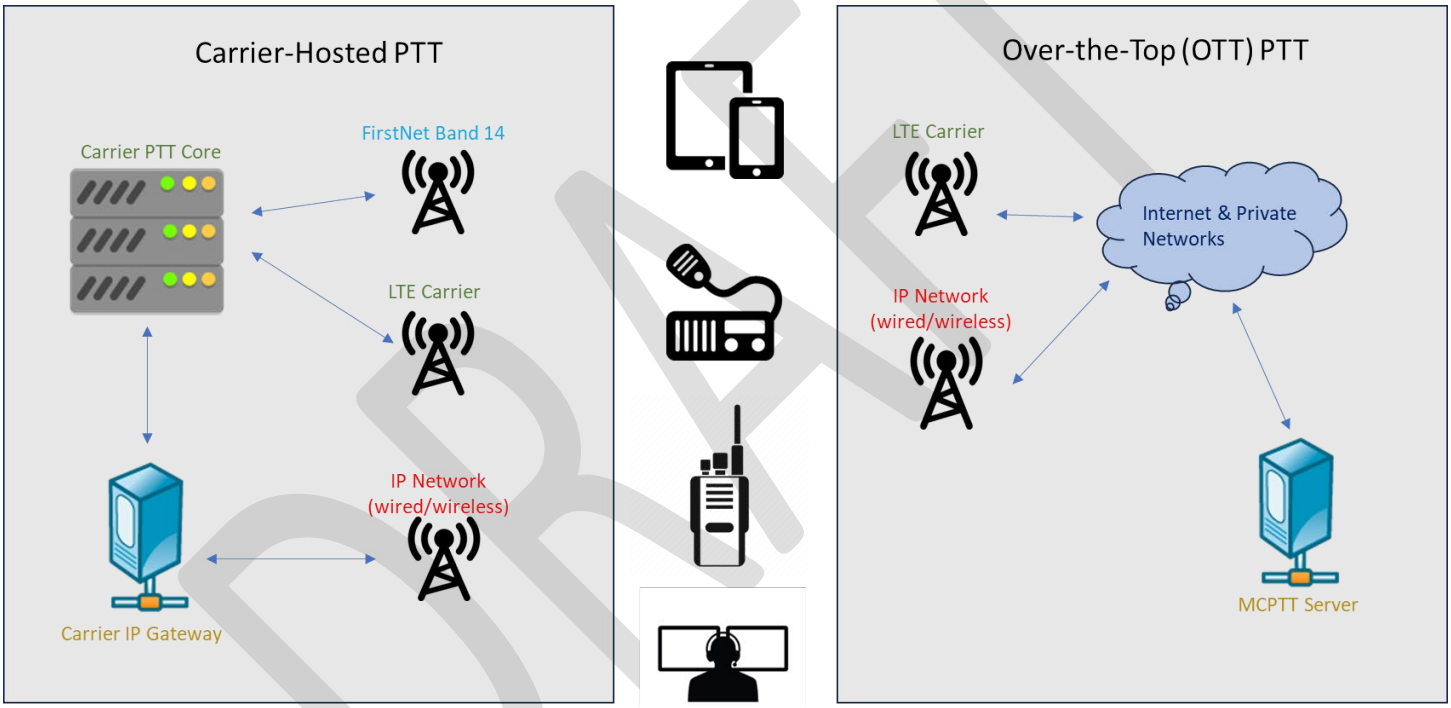


*Figure 1: Stylized description of typical LTE-based PTT messaging systems*

MCPTT was originally envisioned and marketed as a nationwide service on the National Public Safety Broadband Network (NPSBN), supported by FirstNet/AT&T. However, other wireless providers offer their own independent MCPTT solution that compete with FirstNet; these are often referred to as "carrier integrated" options. In addition, there are numerous commercial off the shelf (COTS) IP data-based PTT services that already exist that do not have the "MCPTT" label but can be provisioned as high availability services. These services support similar levels of voice, data, video, telemetry, and location awareness, and are colloquially referred to as "over the top (OTT)" services.

The advantage of carrier-based services is the ability to prioritize first responder traffic above all else on congested networks. The advantage of OTT services is that they are carrier-agnostic, and work on both commercial cellular networks and private/public wireless (WiFi, WiMAX, or mesh) networks. Enterprise Secure Chat (ESChat) is probably the most widely used "mission critical" OTT PTT service in use today in the United States.

## How MCPTT integrates with existing public safety systems

One of the key selling points of most MCPTT systems are the ability integration with existing LMR systems through several different interfaces, including:

- Audio gateways like JPS ACU-series gateways, tactical voice bridges, and others.
- Digital Radio over IP (ROIP) gateways like Icom's VE-PG4, JPS' Z-series, and others.
- System-level integration using the P25 inter sub-system interface (ISSI) or the Digital Mobile Radio (DMR) Application Interface Specification (AIS).
- Dispatch console patches from vendors such as Zetron, Catalyst, and others. Very useful when on-demand dynamic talk groups are needed.

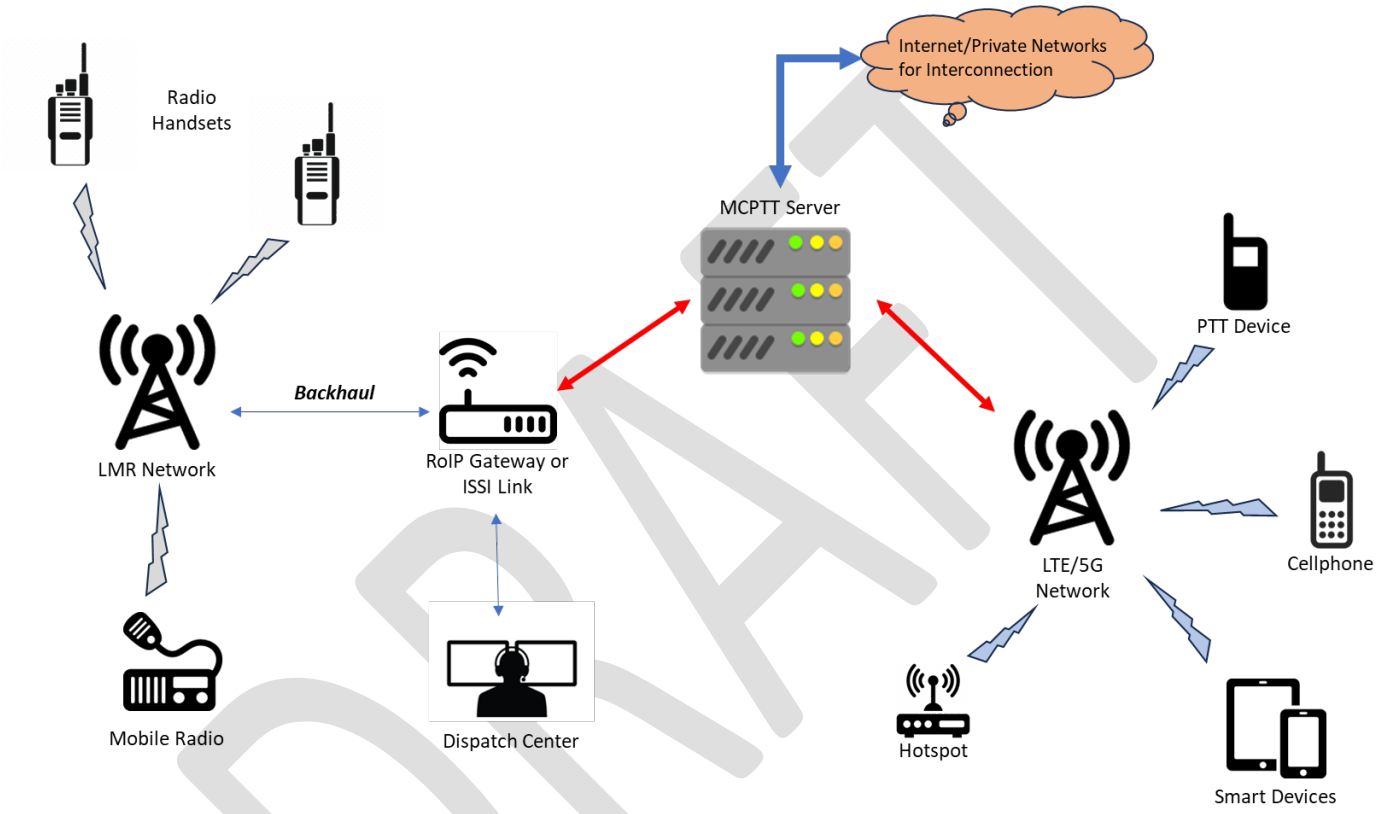


*Figure 2: Example network architecture diagram for a PTT messaging system integrated with LTE and private IP data networks.*

## Relevant standards

MCPTT was originally developed as a service specification by the Third-Generation Partnership Program (3GPP) to implement push-to-talk services over FirstNet; the specification is derived from an earlier standard from the Open Mobile Alliance (OMA-POC) that has been used in the past by wireless carriers. MCPTT, as defined by 3GPP, is an open standard like APCO's P25; it can be licensed and used by anyone.

## Known MCPTT Service Offerings (as of late 2024)

- FirstNet PTT (1st generation)
- FirstNet Rapid Response (2nd generation)
- Motorola WAVE and WAVE PTX, with or without Critical Connect interface.
- Verizon Push to Talk Responder (1st generation)
- Airbus AGNET
- T-Mobile Mission Critical PTT (formerly Sprint Direct Connect – marketed as for first responders)

- Southern Linc MC PTT
- Telus MCPTX (Canada)

### Known non-mission-critical PTT Service Offerings (as of late 2024)

- Motorola Kodiak Broadband PTT (used as the underpinnings of many third-party LTE-LMR bridge applications)
- Verizon Push to Talk Plus (business-class offering)
- T-Mobile Direct Connect (formerly Sprint Direct Connect)
- ESChat (carrier agnostic, T-Mobile, Tait TeamPTT)
- Android Team Awareness Kit (ATAK) and iTAK
- Harris/L3 BeOn
- Zello PTT (specifically Zello Work or Zello First Responder)
- Voxer Business
- Instant Connect Enterprise (formerly a Cisco offering)
- Orion PTT
- ISM band P2P messaging systems (GoTenna, Beartooth)
- ReadyOp (iDEN-based)
- Hytera (currently under import / sale ban in the United States)

Note that these lists are not comprehensive. First, applications with no potential for LMR integration were generally not considered for this white paper. Second, there are a plethora of smaller vendors and open-source projects that offer PTT voice services over data network on mobile devices; no attempt was made to categorize every single one. This white paper focuses on solutions currently in use and marketed largely to enterprise, government, and public safety customers.

## Advantages, disadvantages, and challenges

### Advantages

- Potential **cost savings** on devices, especially for secondary / occasional users for whom a public-safety grade LMR unit is not essential to their job functions.
- **Greater usage** of existing LMR systems without adding additional devices. Casual users can be added to existing talk groups on digital trunked radio systems without needing a radio handset.
- Inclusion of higher bandwidth services such as **data, telemetry, and streaming video**.
- Priority and pre-emption of voice and data communications on cellular networks (depending on carrier). The Federal Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) provide voice telephone call priority and pre-emption, but do not extend to data communications save Voice over LTE (VoLTE).
- Utilization of devices that nearly every first responder is intimately **familiar with and has at hand**. There is a significant training and efficiency value to extending the functionality of devices that are already core to many public safety functions.
- **Cost effective for buildout** of new network in areas with pre-existing dense cellular network coverage. It is possible that a MCPTT program could be significantly cheaper to stand up than a new public safety radio system or to replace an existing out-of-date one.

### Disadvantages

- **Yet another device** to provision, manage, and maintain, especially if an organization already has a mature LMR network.
- **Resilience** of handset devices, especially consumer-grade smartphones (Apple iPhone, Samsung Galaxy, Google Nexus). There are rugged LTE smartphones available, but their usage is in general

orders of magnitude less than consumer-grade devices. Precious few handset devices are intrinsically safe for use in hazardous environments, and most are both expensive and lacking features found in modern consumer-grade handsets.

- Effectively **no simplex mode** where one user can talk direct device-to-device; MCPTT only works when connected to the LTE network. Note that there is a Device-to-Device implementation described in the MCPTT standard, but it largely does not encompass "offline" usage, and as of 2023 few if any chipmakers have added it to their integrated radio modem controllers.
- **Cost recovery** for system owners and operators. For many organizations, the cost model for LMR radio systems involves an ongoing access fee to the network as well as either up-front device purchase or a monthly amortization and replacement fee. Cost recovery may have to follow a different model, especially in a bring-your-own-device (BYOD) environment.
- Reliant on a robust and operational **cellular data network**, including not only tower to tower but also backhaul connectivity to the Internet. If either the local or backhaul connection is broken, the service is unusable.

## Challenges

- **Incompatible solutions from multiple vendors**. For examples, MCPTT using FirstNet-centric solutions can only communicate with other users on the FirstNet Core; the system is not interoperable at the core network.
- **Resiliency of cellular network** in the face of natural and technological hazards. Providing robust backup power and backhaul resiliency is still a challenge in many locations.
- **Connecting conventional systems** not networked together via ISSI to LTE will often require additional hardware, including donor radios and RoIP bridges.
- Service-level (SLA) **uptime guarantees**.
- Longevity / **pace of technological advancement**. New communications services and technologies arrive on an annual basis, which is generally much faster than the planned life cycle for most organizations' communications systems.
- **Identity management** / credential authentication, especially with respect to data roaming between carriers. LMR users face similar issues such as sharing of system keys, enabling of roaming from network to network, and sharing of encryption keys.
- **Information security**, especially with mobile devices being a prime target for both cybercriminals and nation-states.
- **LTE and LMR roaming**, especially on deployable systems (COWs, COLTs). Field experience in Oregon during wildfire season has generally shown that deployables do not have carrier-agnostic roaming, limiting the use of non-carrier MCPTT to within a few hundred feet of the deployable where open WiFi is available.
- **Reliability of WiFi networks**, especially those built on consumer-grade technology in congested environments. These devices / networks may not have the reliability necessary to meet a "mission-critical" standard. In addition, many ad-hoc wireless networks set up on incident sites do not have network traffic management or quality of service (QoS) priority configured to ensure consistent application performance.
- Separation of professional and personal profiles on **responder-owned devices** in bring-your-own-device (BYOD) circumstances. This is a concern that is not just limited to MCPTT but is an issue that all organizations face where employees are not provided mobile devices for their work use.
- **Prioritization of device access**, i.e., LMR users versus MCPTT on a hybrid LTE-LMR network

## MCPTT Use Cases

### Surge Capacity

MCPTT devices give organizations an additional ability to deploy devices to an incident that can rapidly form one or more talk groups for an incident among personnel without having to distribute cache radios. It can allow access to LMR talk groups to smartphone users in a BYOD situation. PTT over LTE networks also gives responders a separate network on which to connect when/if existing LMR channels become saturated or oversubscribed.

### Integration with Interoperability Radio Channels

In a trunking system outage where conventional interoperability repeaters are in play, the ability to add cellular phones to interop command and tactical channels via either a Radio over IP (RoIP) or audio gateway is key. Some applications may require a donor radio, similar to traditional gateways like JPS' ACU series, while others utilize specialized hardware integrated at the radio site. MCPTT may also improve communications in confined-space environments like tunnels, airports, or high-rise buildings where bi-directional amplifiers (BDA) for LTE service have been installed but not for trunked or conventional LMR systems.

### Provisioning equipment for non-public-safety users

Give the ability to non-public safety, but still "mission-critical" users such as DOT / county roads, public utilities, emergency operations centers, logisticians, shelter workers and public health, access to LMR-specific talk groups without provisioning each with an individual radio.

### Alternatives to carrier-provided PTT (not necessarily MCPTT)

- Carrier-agnostic OTT services such as Zello, ESChat, Viber, and Voxer
- Microsoft Teams PTT functionality, for those organizations with a significant investment in the Microsoft Azure Cloud / Office 365 environment. A relatively inexpensive lift for organizations already paying licensing costs for Microsoft cloud applications. As of 2023 no LMR gateway is available.
- Google Meet PTT, for those organizations with a significant investment in the Google cloud. As of 2023 no LMR gateway is available.
- Existing secure messaging services like Signal, Telegram, and Wire operating over wireless data networks.
- Satellite PTT systems as offered by Iridium and Globalstar.

Note that, per 3GPP technical releases, few if any of these services meet the MCPTT standard. Any use in a public-safety environment should carefully evaluate whether system reliability, coverage, and interoperability will meet life-safety needs.

## Recommended Best Practices

### Key Messaging Points

1. MCPTT devices augment public safety LMR systems; they does not replace them. They offer a cost-effective way to increase the scope of an LMR network when mission requirements do not mandate portable or mobile radios.

2. MCPTT offers a way to extend LMR systems and bridge to the cellular LTE network world that allows scalability, surge capacity, and for the use of new types of communications applications.

3. MCPTT on cellular devices face challenges to resiliency based on the robustness of the LTE carrier infrastructure, including lack of backhaul redundancy and alternative power systems, that many LMR systems have already addressed.

4. There are carrier-specific, vendor-specific, and vendor/carrier neutral (OTT) services; carefully evaluate which will work best based on existing contracts, infrastructure, experience, and local requirements. As with LMR radio, one system may not fit all users.

5. As with P25 radio systems, while MCPTT is a known standard, various incompatibilities between different vendor offerings have the potential to compromise interoperability. The opinion of the SIEC Technical Committee is to prioritize PTT services that make interoperability with the widest possible mix of carriers, vendors, hardware, and software possible and do not lock the user into a vendor-specific solution.

### Implementation Strategies

1. The SIEC Technology Committee recommends starting with the Department of Homeland Security's best practices for LMR/LTE integration.

2. Include a detailed cost-benefit analysis, especially in the case of an environment with a well-supported and robust LMR network. This calculation should also account for new capabilities available through LTE/LMR integration and the use of PTT not previously available to first responders.

3. Design any MCPTT implementation with a cost recovery mechanism that mirrors what is done for the existing LMR system. Centralized billing, accounting, and provisioning is highly desirable.

4. Ensure your existing network infrastructure can handle the additional loads incurred by the inclusion of LTE-based MCPTT systems. Completing these calculations before bidding and implementing a MCPTT system will save both time and money in the long run.

5. In parallel with strategy #4 above, recognize that in general cellular networks will not meet the 99.999% reliability threshold that critical public safety users (police, fire, and EMS) need and are used to. These users should not be issued MCPTT as their primary device to replace LMR; rather, it should be issued as a secondary supporting device.

6. The MCPTT landscape continues to evolve daily. Ensure that any implementation includes a mechanism to adapt to technological change. Of particular importance are mechanisms to account for system obsolescence; cellular technology advancements tend to occur at a much faster pace than advances in the traditional LMR world.

7. Approach the issue of bring-your-own-device with caution; from an information security standpoint it is probably safer to issue organization owned devices utilizing mobile device management (MDM) systems. This does not preclude adding BYOD capabilities in an emergency.

## References


- 3GPP Mission Critical Push to Talk (MCPTT) Stage 1, Specification 22.179, published November 2019, last accessed January 2024: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=623

- 3GPP Specifications and Technology Releases. MCPTT is covered in releases Rel-13 (2016), Rel-14 (2017), and Rel-15 (2019); the current latest frozen standard is Rel-17 (2022), though Rel-18 is

approaching frozen in late 2024. Last accessed January 2024: https://www.3gpp.org/specifications-technologies/releases

- Land Mobile Radio/Long Term Evolution (LMR/LTE) Integration: Best Practices, SAFECOM and NCSWIC, February 2023, last accessed 11/7/2023: https://www.cisa.gov/sites/default/files/2023-02/Land%20Mobile%20Radio%20%28LMR%29%20Long%20Term%20Evolution%20%28LTE%29%20Integration%20Best%20Practices%20Whitepaper%20508C.pdf
- Mission Critical Push to Talk (MCPTT) Considerations for Interoperability Talkgroup Naming and Management, NPSTC Interoperability Committee, November 2018, last accessed 2/7/2023: https://www.npstc.org/download.jsp?tableId=37&column=217&id=4172&file=NPSTC_MCPTT_IO_TG_Naming_181214.pdf
- Interworking Mission Critical Push-to-Talk (MCPTT) between Long Term Evolution (LTE) and Land Mobile Radio (LMR), Catalyst Communications Technologies, 2019, last accessed 2/7/2023: https://www.dhs.gov/sites/default/files/publications/interworking-mission-critical-push-talk-between-lte-and-lmr-report_02142020.pdf
- Transforming public safety with wireless technology, T-Mobile For Government, 2022, last accessed 2/7/2023: https://www.t-mobile.com/business/government/public-safety
- LTE; Mission Critical Push to Talk (MCPTT) over LTE; Stage 1, 3GPP TS 22.179 version 15.2.0 Release 15, July 2018, last accessed 2/7/2023: https://cdn.standards.iteh.ai/samples/54830/83cba542b025424f8c957004decaafc4/ETSI-TS-122-179-V15-2-0-2018-07-.pdf
- Push-To-Talk over Cellular: Integrated LTE and LMR Communication Success in the Mainstream, Andrew Seybold Inc., March 2017, last accessed 2/7/2023: https://www.allthingsfirstnet.com/wp-content/uploads/2017/04/Whitepaper-Succcess-in-the-Mainstream2.pdf
- Push-To-Talk over Cellular: The Flavors of PTToC Carrier Integrated, Over the Top, and MCPTT, Andrew Seybold Inc., March 2017, last accessed 2/7/2023: https://allthingsfirstnet.com/wp-content/uploads/2017/04/Flavors-of-PTToC-FINAL.pdf