



# Private and Semi-Private Wireless Networks

A closer look at Private Networks in 2020 and beyond  
A Disruptive Analysis thought-leadership eBook



**Disruptive Analysis**



# Table of Contents

<b>Introduction &amp; Executive Summary</b> .....	<b>3</b>
<b>Blurring the line between public and private networks</b> .....	<b>4</b>
<b>Evolving today's public / private infrastructure status-quo</b> .....	<b>6</b>
<b>New spectrum, new technologies for private wireless</b> .....	<b>8</b>
Private 4G/5G cellular enablers .....	8
Wi-Fi enhancements .....	9
Other private wireless options .....	9
<b>Shifting demand: Use-cases, building types &amp; verticals</b> .....	<b>11</b>
<b>New stakeholders and service providers for private wireless</b> .....	<b>13</b>
<b>Conclusions and recommendations</b> .....	<b>16</b>
The future of private and semi-private wireless .....	16
Convergence, divergence or both? .....	17
The future of private wireless in the post-pandemic world .....	17
Recommendations .....	19

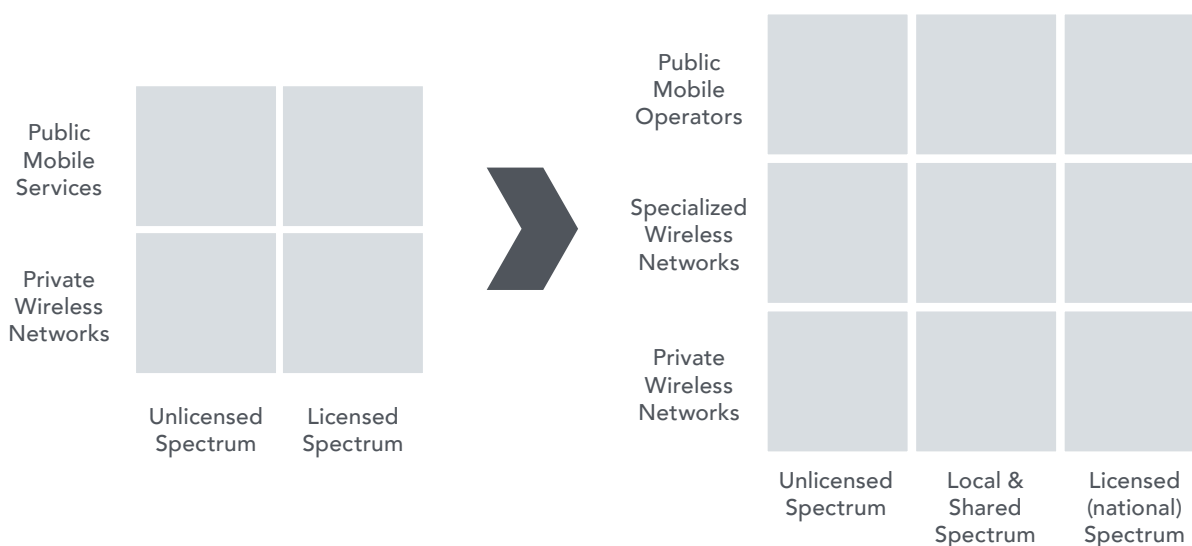
# Introduction & Executive Summary

The enterprise and in-building wireless world is changing. From a simple two-way divide between public cellular networks plus private Wi-Fi, the sector is now fragmenting into numerous new models and technological approaches.

This eBook follows on from previous iBwave publications that have considered CBRS, Private LTE and in-building network convergence. It considers various additional factors and trends including:

- The fast-evolving but distinct roles for 4G/5G and Wi-Fi in enterprises.
- Growing availability of localized and shared options for spectrum and small 4G/5G networks, at scales and prices suitable for businesses to deploy their own private cellular infrastructure. The previous binary choice of unlicensed bands vs. exclusive nationwide licences (suitable for public MNOs) no longer applies.
- The expanding universe of stakeholders and specialist service providers in enterprise wireless networks, including carriers, property companies, neutral-hosts, industrial automation and smart-building suppliers, as well as public safety agencies. These can enable “semi-private” networks and managed services.
- The need to distinguish between locations which need primarily human-focused wireless networks (for employees and visitors) vs. machine/IoT-focused.
- The complex ways that public networks and private networks will combine. For instance, MNOs may use “network-slicing” to create another class of semi-private networks, with some direct control by business customers.
- The impact and timelines for new spectrum and technologies, such as later versions of 5G (3GPP Release 16/17), Wi-Fi6E in the 6GHz band, and new vRAN/ OpenRAN architectures.
- Counterintuitively, Private 5G and Wi-Fi 6 will drive both convergence and divergence but at different layers of network and applications.
- Impact of the COVID-19 pandemic on the way in-building and on-campus wireless networks will be deployed and used in future. This will consider possible economic scenarios, shifts in sector/industry focus and priority, and possible new regulatory angles in future.

## New spectrum & new types of SP change the “private network” landscape



Source: Disruptive Analysis

# Blurring the line between public and private networks

In the past, there has always been a clear distinction between public and private wireless networks inside enterprise premises.

- **Public wireless networks** involve the delivery of cellular service from MNOs (also called carriers), mostly to smartphones carried by visitors and employees, for voice telephony and mobile data. Public safety agencies have generally used their own wireless networks, separate from the MNOs' systems. The 5G era makes public networks more important – but also harder to deliver.
- **Private wireless networks** – primarily using Wi-Fi today – are used for corporate and Internet data connectivity from a wide range of devices, including PCs and smartphones, as well as various IoT systems. Private networks are now becoming far more extensive and capable – and may include localized spectrum licenses suitable for private cellular.



There has been some overlap between these worlds, such as where MNOs provide public-access Wi-Fi hotspots in some buildings, linked to their cellular infrastructure for “offload” – but this has been comparatively minor overall.

Unlike utilities like energy and water – or even fixed-line telecoms – there is no clear “demarcation point” of responsibilities for wireless, as the vagaries of wireless signals mean that outdoor public-network signals work (partially) indoors, and indoor private-wireless can extend out beyond the walls.

## Wireless networks do not have clear “demarcation points”

**Variable demarcation  
between public vs. private**

**Clear demarcation between  
public vs. private**



Source: Disruptive Analysis



So there has always been an underlying tension and contradiction. Provision of public network services, such as normal 3G/4G mobile, on private property, introduces various types of complexity. Except where MNOs can provide those services purely with outdoor-to-indoor radio propagation from their macro networks, they have usually needed to rely on some privately-owned assets.

These can be thought of as precursors of the new domain of “semi-private” networks.

These public/private overlaps and tensions will only get deeper in the coming years, because of a number of trends occurring simultaneously:

- 5G brings new frequency bands and radio technologies, that need new approaches to on-premise wireless equipment, design and business models.
- Private cellular networks are becoming easier and more desirable to build.
- Campus networks spanning indoor and outdoor domains are growing in importance, blurring further the boundaries of the “private” domain.
- Diverse IoT use-cases and systems blend the wireless world with enterprise IT, industrial OT (operational technology) and new service-provider focus areas.
- Wi-Fi is becoming more sophisticated, business-critical – and yet sometimes congested. It is also evolving technically, with WiFi6 and the new 6GHz band.
- Public safety networks are shifting towards 4G/5G technology (sometimes dedicated, sometimes with an SP) – and indoor coverage is being regulated more.
- The COVID19 pandemic will create new drivers for – and economic brakes against – enterprise wireless, both public and private. Outcomes are as yet unknown.



Taken together, these trends mean that the historic separation of public and private networks is coming to an end. We will need to design, plan and invest for a future of hybrid on-premise networks that combine public and private connectivity in new ways.

# Evolving today's public / private infrastructure status-quo

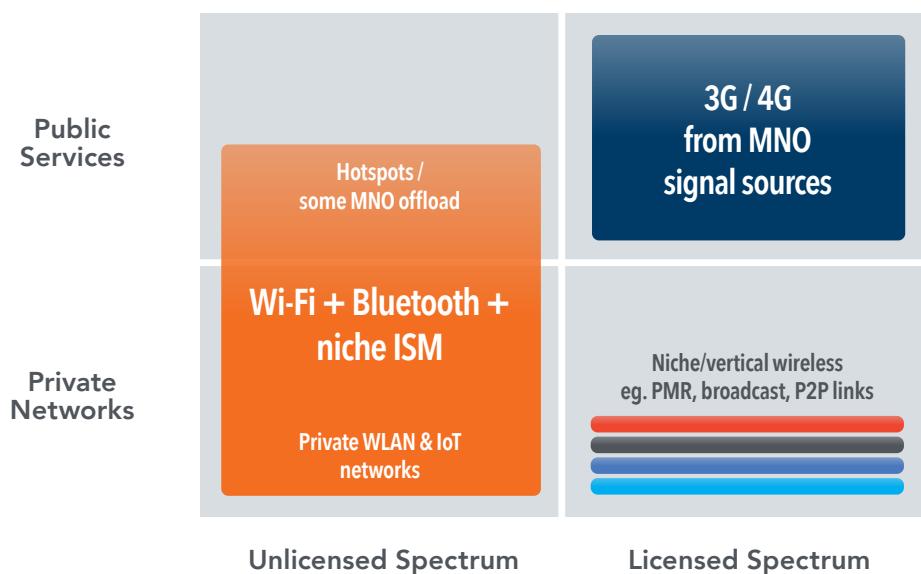
Today, a building owner may invest in a DAS (distributed antenna) system, Wi-Fi network, Fiber infrastructure – and the ducts and risers and power supplies – that support both public cellular services and its own private wireless system(s) and wired network. Sometimes a third-party service provider installs and operates a neutral system on the property company's behalf.

On-site mobile coverage generally uses the MNOs' own licensed spectrum and "signal source" (typically a base station or small cell), but the other physical infrastructure required is held on other companies' balance sheets. In certain instances, one or more carriers may directly deploy their own infrastructure, although this is rare. The use of MNOs' own spectrum means there is no clear single demarcation point between public and private realms, even with a DAS. There is always a risk of interference, or poor coordination, between indoor-originated and outdoor-macro signals.

This variable semi-private / semi-public hybrid leads to lengthy cycles for in-building wireless design, deployment and contracting, and a lack of standardisation in terms of business model and control. Sometimes carriers have paid for indoor/on-premise systems, while sometimes it is the owner or occupant's responsibility. Enterprises use a mix of capex and opex depending on the situation and involvement of third-party providers. Getting multiple MNOs to agree on sharing a system has been harder still. As a result, many systems have been one-off "special projects".

This model cannot work well in the future 5G world, or even some of the advanced 4G use-cases around IoT. Although the mobile industry is looking at enterprise as a core new source of revenues, scaling will be problematic. There are simply too many companies and sites, with too many urgent but diverse use-cases, to wait in line for carriers' processes and priorities.

## Today's indoor wireless: Licensed public mobile, plus unlicensed private Wi-Fi



Source: Disruptive Analysis

Meanwhile, Wi-Fi and some other wireless systems have been deployed as pure private networks much more broadly. Originally, Wi-Fi grew as an extension of wired ethernet LANs, paralleling the shift from desktop PCs to laptops, as well as with industrial handhelds such as barcode-scanners. It then took on the role of connecting visitors' laptops, followed by smartphones and tablets, and has become near-ubiquitous in all buildings from offices to hotels to schools.



Using unlicensed spectrum has meant that its installation has been “permission-less”, and a vast ecosystem of both network infrastructure and client/device products has emerged. This has meant that Wi-Fi has long bridged the gap between public and private domains – it can be either owned and run by an enterprise or building-owner directly, or it can be provided as a service-based model. Indeed, in many ways it is now an “amenity” – a fundamental part of the building’s infrastructure, just like power and air-conditioning.

But now we see two major shifts in both supply and demand, which will impact this landscape:

### Demand-side changes

- Growing range of applications & use-cases for indoor and enterprise-controlled private wireless
- Propagation characteristics of public 5G networks require enhanced indoor infrastructure

### Supply-side changes for private and semi-private wireless

- New tranches of shared and local spectrum (eg CBRS band in the US)
- New technologies for private networks, such as Wi-Fi 6, small cells and cloud-based 4G/5G core networks
- New classes of specialist SP for enterprise & indoor markets

These topics are further analysed in the next sections of this paper.



# New spectrum, new technologies for private wireless

Expansion of enterprise private and semi-private networks is now accelerating. A wide variety of “enabling innovations” is occurring concurrently, both in the technology itself and the way in which spectrum is being awarded and authorized for use by governments.

Product enhancements are happening across the board – relating to private 4G and 5G, Wi-Fi and other network technologies as well. There will not be a single “winner” here – most buildings and businesses will need multiple radio technologies, although we will see greater convergence and integration between them.

In addition, a growing number of options around “semi-private” cellular networks are emerging, where enterprises

control some aspects of their on-site wireless networks, but without complete ownership and operation. Both existing MNOs and new niche SPs are offering managed services, based on various strategies for spectrum, as well as exploiting the same innovations such as cloud-delivered networks.



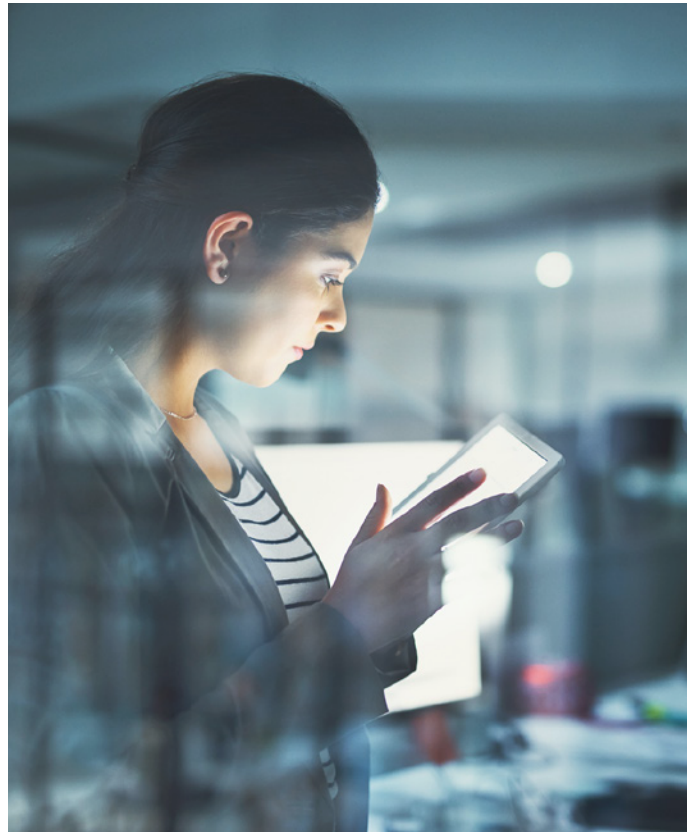
## Private 4G/5G cellular enablers

- **Spectrum:** In our previous eBooks on CBRS and Private LTE, we have discussed the growing availability of low-power local licenses or shared spectrum, suitable for indoor or on-campus private cellular usage. Numerous countries have freed up bands suitable for private 4G and 5G, for indoor or campus use by enterprises or niche SPs, as well as across wider areas in some cases. The US, Germany, UK, Japan, Taiwan and Nordic markets and others are all seeing a surge of interest in private mobile, sometimes for industrial facilities, and sometimes for venue-type locations. In coming years, we can expect 1,000s or even 10,000s of such deployments, although local rules vary by country.
- **New RAN approaches:** As well as spectrum, enterprises are benefiting from cheaper and more-available cellular network infrastructure, making private networks more “democratized”. In the past, only high-end deployments of Private LTE made economic sense – for example for utility companies, or major mines and oil-and-gas facilities. Now, major vendors have scaled-down their carrier-grade products, and a plethora of niche suppliers have targeted private LTE/5G. There are many suppliers of indoor small cells or advanced DAS platforms, along with a growing number of specialized integration and installation channels. Looking forward, a number of virtualized/cloud RANs approaches have promise, coupling cheap “white box” equipment with containerized functions and orchestration software, should further accelerate private cellular.
- **Cloud and core networks:** Some key components driving private/semi-private wireless are beyond the RAN itself. 4G and 5G networks need software-based cores for control, as well as further applications for managing SIMs, security, network operations, interconnect, voice/telephony and more. Historically these were complex, expensive and only available at scale. Now, they are being offered as cloud-delivered aaS functions, or “in a box” at costs suitable for enterprise on-premise deployment. In addition, existing national MNOs are focusing on the enterprise, offering on-premise connectivity, edge-computing and – in future – network slicing capabilities to create “virtual private” 5G networks.



## Wi-Fi enhancements

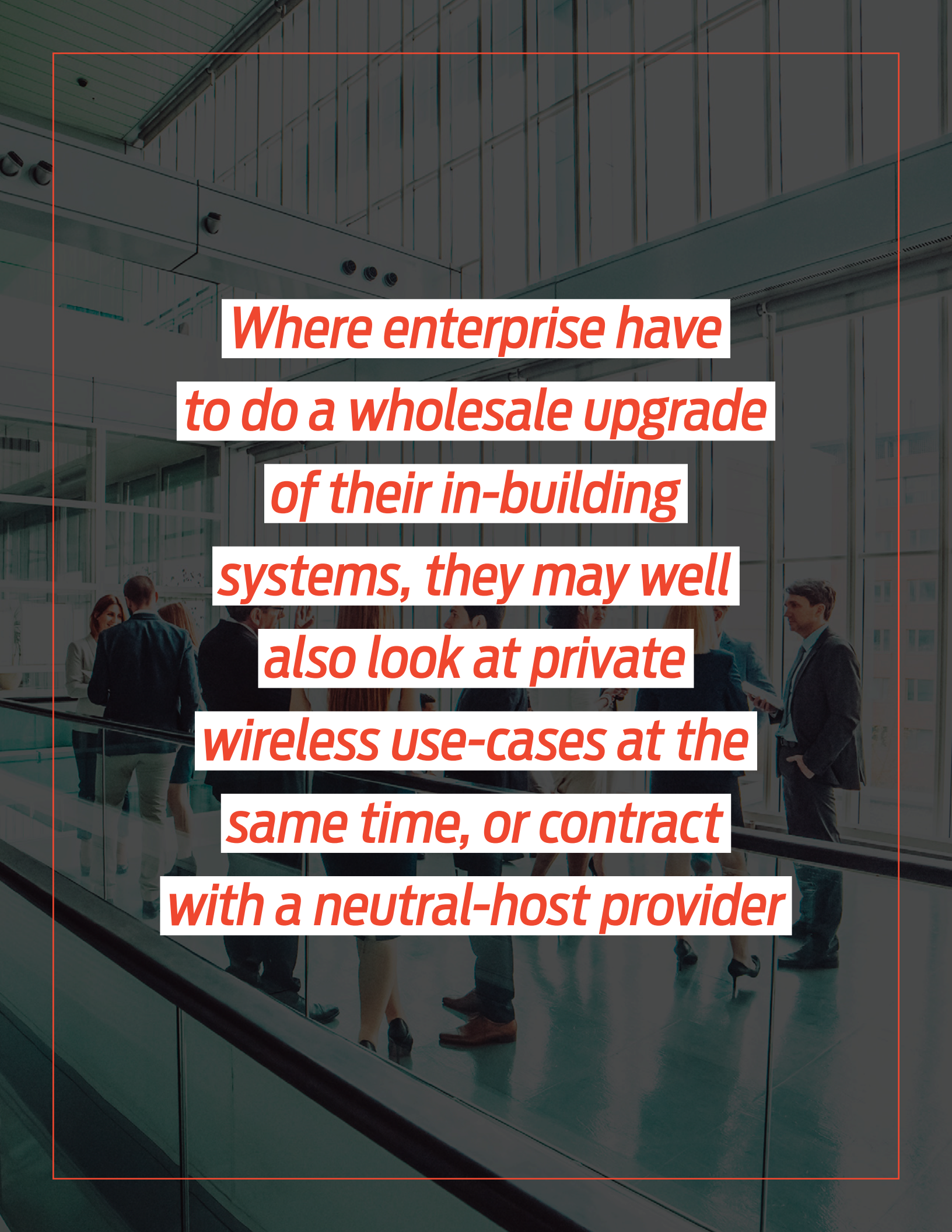
- **Wi-Fi 6 and beyond:** The latest version of Wi-Fi, based on 802.11ax standards and other enhancements, allows enterprises to create more-flexible private wireless deployments in unlicensed spectrum. Compared to earlier versions of Wi-Fi, it allows more fine-grained control of capacity, allowing differential levels of QoS to be created. It also permits higher densities of client devices, and allows power-saving in IoT by pre-scheduling connection times and delays.
- **6GHz:** In April 2020, the US FCC announced its intention to permit 1200MHz of spectrum in the 6GHz band for unlicensed use, suitable for Wi-Fi 6 and potentially 5G-U in future. This massively increases the potential capacity of Wi-Fi, allowing 2Gbps speeds and 2ms latency connections. The rules allow for different power levels of access-point, with “standard” power radios needing to work with an AFC (automated frequency coordination) system to avoid interference with (mostly outdoor) incumbent users such as point-to-point. European regulators are also expected to allocate part of the band – perhaps around 500MHz for unlicensed use, probably in 2021.



## Other private wireless options

As well as 4G/5G cellular and various generations of Wi-Fi, there are other options for enterprises building private wireless connectivity. Some are standardized, such as Bluetooth and ZigBee for low-power / short-range IoT devices such as sensors and smart-building controls. Then there are various proprietary industrial-wireless technologies, such as Siemens' I-WLAN and ABB's TropOS Mesh. There are even sonic and ultrasonic network systems for use where RF signals are prohibited.



The background image shows a modern office interior. In the foreground, there is a glass railing of a mezzanine or staircase. Several people in business attire are walking on the floor behind the railing. The office has large windows and a high ceiling with visible structural elements. The overall tone is professional and contemporary.

*Where enterprise have  
to do a wholesale upgrade  
of their in-building  
systems, they may well  
also look at private  
wireless use-cases at the  
same time, or contract  
with a neutral-host provider*





## Shifting demand: Use-cases, building types & verticals

As well as technology and spectrum shifts, which are permitting wider deployment of private cellular networks, there are parallel developments occurring on applications and use-cases.

At one level, private wireless demand is being driven simply by the need for indoor public 5G connectivity. Higher frequencies mean that existing outdoor-to-indoor or DAS solutions are no longer sufficient to deliver coverage. Most 5G deployments are in midband spectrum above 3GHz, or as dynamic-shared hybrid 4G/5G in 1-3GHz. Neither works effectively on most existing indoor infrastructure, and nor do the mmWave versions of 5G being used in a few markets.

These include:

- Site-specific personal mobile devices, such as barcode scanners and AR/VR headsets.
- Smart-building sensors and systems, from smart-lighting to environmental monitoring.
- Security cameras, digital displays, kiosks and other audio-visual equipment requiring high bandwidths.
- Industrial, medical and other technical equipment with requirements for low latency and high reliability
- Onsite mobile devices such as vehicles and automated guided vehicles (AGVs)

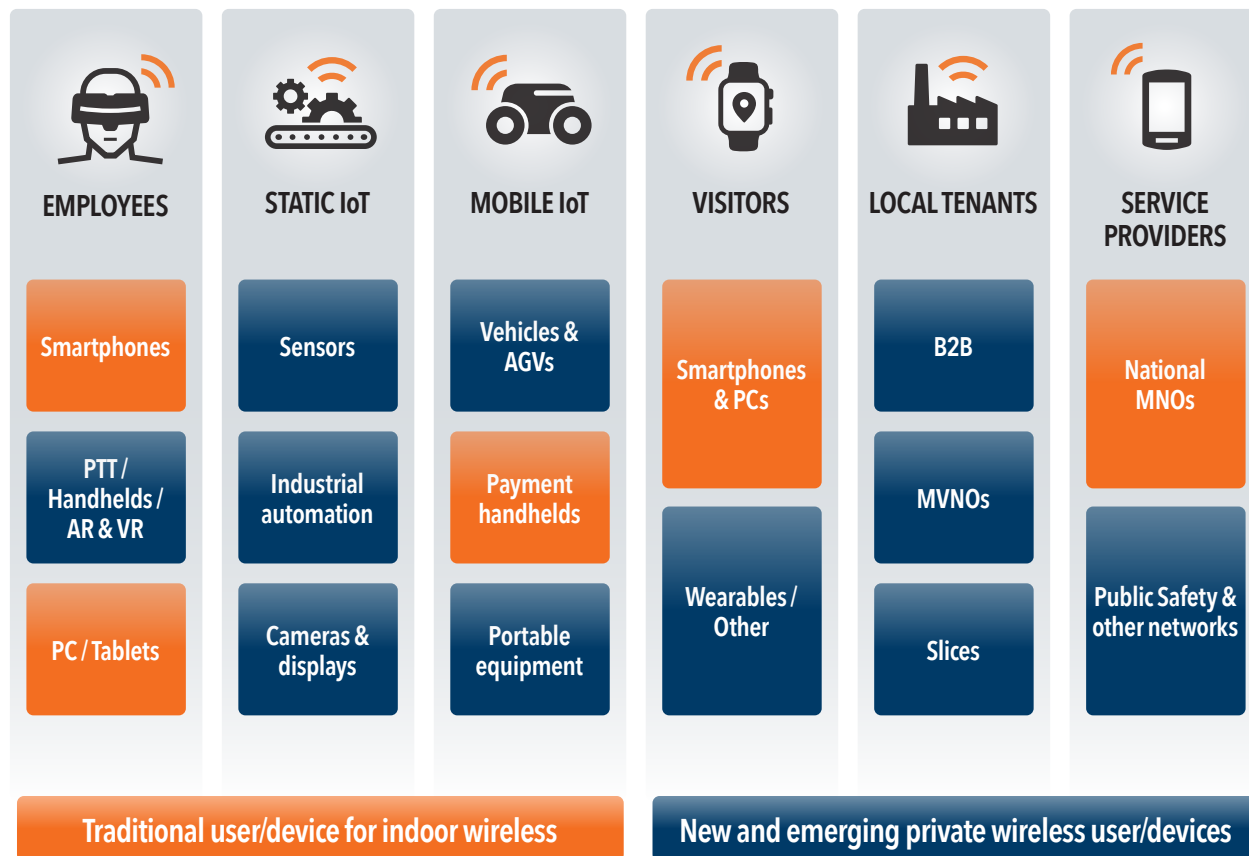
These types of systems are best-served by private networks of some form, as they involve economics, security or IT/OT integration that is specific to that enterprise. That type of application-specific connectivity is poorly suited to public

Where enterprise have to do a wholesale upgrade of their in-building systems, they may well also look at private-wireless use-cases at the same time, or contract with a neutral-host provider (see later section).

Moreover, the types of indoor or on-campus wireless applications are changing. While employees' and visitors' PCs and smartphones are still the focus for Wi-Fi (private) and indoor 4G/5G (public) respectively, many other devices and user classes are rising up the agenda.

networks' capabilities and business models. However, not all fit with Wi-Fi and unlicensed spectrum either – although the improved capabilities of Wi-Fi 6 and 6E will help in some cases.

## Future private wireless networks will cater to new classes of users and devices



Source: Disruptive Analysis

In addition, some “private” wireless environments start to look like miniature public networks, with their own on-site tenants served by the enterprise or venue owner. An airport authority may run its own wireless networks – but then provide connectivity services to airlines, catering firms and maintenance companies. A major property company running a wireless network across a business park may offer localized network-slicing and on-premise edge computing for its tenants. An entertainment, retail or sports location

may offer mobile “concessions” to companies and brands – almost like localized MVNOs. These types of business models probably could not work with the involvement of an external public network provider.

An interesting case study is German airline Lufthansa. It has announced two trials of private 5G – one with the enterprise and systems-integration arm of Vodafone, and one directly with Nokia as a purely private network.





## New stakeholders and service providers for private wireless

An important facet of the future private and on-premise wireless world is the fragmentation of the “service provider” space. Today, indoor wireless is primarily driven by venue owners – which could be property companies or major corporations with their own facilities.

Private wireless is mostly supplied through companies’ own Wi-Fi networks. For public wireless delivered onsite, they work with a limited range of SPs:

- ▶ Traditional MNOs and carriers, for provision of indoor public cellular services, as discussed above. Most countries have 2-4 major network operators.
- ▶ Some locations work with commercial Wi-Fi service providers, where the main target user-group is external visitors (for instance, in airports or conference centers). These may be owned or affiliated by MNOs or fixed telcos, or independent.
- ▶ A small number of sites have worked with in-building neutral-host providers, which have typically deployed DAS as a managed service.

Given the changes in technology, spectrum availability and demand for connectivity, a new set of SPs and stakeholders are emerging, which are helping to tip the balance towards private wireless, or at least semi-private managed services from non-telecom providers. The key new groups include:

- ▶ **Specialist and niche SPs:** A broad range of new providers are emerging to help enable fully-private wireless networks or provide and manage them for businesses on a “semi-private” or neutral-host basis. These organisations may be able to obtain their own spectrum on a local or leased basis, or else the venue/enterprise could itself apply for a license. In some cases, they may use unlicensed bands. A selection of the sub-types of SP involved includes:
  - ▶ **Tower companies** extending their footprint into in-building shared wireless infrastructure. They may derive revenues from the venue-owner, the MNOs, or both. Crown Castle, Cellnex and others fit into this category.
  - ▶ **Fiber companies** looking to extend their reach into enterprise offices with new propositions. They may bundle indoor wireless (perhaps with a wholesale neutral-host play) along with edge computing, voice/UC services and other offers. We may also see convergence between metro Fiber access and vRAN, with the provision of fronthaul direct to distributed antennas in-building, with baseband units consolidated in a local datacenter.
  - ▶ **Cloud providers** are trying to offer “Private Network as a Service”, tying together local spectrum licenses or CBRS database access, with cloud-delivered core networks, design tools, subscription management and interconnect. They would likely work with local installation/integration partners. CBRS SAS provider Federated Wireless is working with both Amazon AWS and Microsoft Azure, to offer “Private Network as a Cloud Service”

- ▶ **Wi-Fi hotspot SPs** are looking to add local cellular connectivity as well, typically as a neutral-host and offload platform for MNOs wanting better indoor coverage. Boingo is a good example here.
- ▶ **Enterprise-focused MNOs** are deploying private wireless networks for demanding campus or industrial environments, such as oilfields, mines, ports and airports. These are high-end use cases and sometimes justify directly leasing spectrum from national MNOs. Examples include Edzcom (formerly Ukkoverkot) in Europe, and Ambra Solutions, TampNet and EcoTel in North America.
- ▶ **Voice and UC/UCaaS** providers are extending their existing MVNO relationships with enterprise, to cover indoor private cellular as well. A number are looking at CBRS or other countries' local spectrum to deliver mobile PBX and conferencing, for instance, in contact centers or shared-office workspaces.
- ▶ **Property companies** are also stakeholders in this marketplace. Several major developers are realising that connectivity forms a central part of their value for tenants (business or residential) and are considering their own wireless infrastructure as part of construction or refurbishment capex. Many are investigating whether they can become wireless SPs, in the same way that some already offer and monetise broadband or Fiber connections. As it becomes easier to offer neutral-host wholesale capacity to MNOs needing on-premise coverage, we can expect this sector to grow. Some will obtain their own spectrum or use shared bands, if it is straightforward.



- ▶ **Existing MNOs:** Existing mobile carriers are increasingly focused on enterprises and are developing both 4G and 5G solutions for enhanced public, or semi-private networks. Technologies such as dedicated indoor coverage, or network-slicing, are enabling these propositions, often coupled with edge-computing or other services aligned to target industries. However, there is something of a divide emerging between:
  - ▶ **Public network extensions and slices** where an MNO provides an enterprise with improved coverage, essentially as an add-on to the macro network. The enterprise may be able to use its own core network or be given access to a private partition or slice, for customized configuration and security. Deutsche Telekom, Swisscom and various others are pitching "campus networks" of this type.
  - ▶ **Semi-private networks**, where the MNO facilitates a genuine private (isolated) network for the customer, with dedicated RAN and perhaps local spectrum. This may use different vendors to its macro RAN, with the MNO acting more as a systems integrator and managed service provider. Vodafone Business' work with Lufthansa is an example of this, while Telstra has set up a complete business unit called Mining Services, which has installed several above- and underground private LTE networks for resources firms.
  - ▶ **Component services**, where an MNO just provides specific elements of a private network to an enterprise. For instance, it could offer a multi-tenant "core network as a service", an interconnect or roaming capability, or even just installation and maintenance. The rest of the infrastructure is deployed and run privately.

➤ **Vertical systems providers:** Many modern industrial-automation, smart-building and other dedicated technology systems depend on wireless connectivity. These can sometimes rely on public networks, but are increasingly reliant on private or semi-private wireless of various types. Today, such systems often “bring their own” wireless connectivity – for instance a robot may connect to its control unit with a separate Wi-Fi network, rather than use the building’s main system. As IoT becomes more important and pervasive, as well as adopting 4G/5G connectivity, these systems may converge with the building’s wireless infrastructure. Siemens, Bosch, Motorola, Hitachi and many other have all discussed private cellular options for factories, warehouses, construction sites and other similar locations.



➤ **Public safety agencies:** There is a growing need for first-responders and other agencies to get access to reliable wireless networks indoors, for both voice and data applications. While various two-way radio / LMR systems have traditionally been used for fire, rescue or police, there is now a gradual shift towards 4G/5G under way in many regions of the world.



Some agencies are deploying their own private cellular networks, nationally or regionally, while others are working with MNOs (for example AT&T FirstNet, or BT's ESN). Regulations and safety-codes vary by country and even city/state about how these systems need to be supported in-building. Where enterprises are designing future private or semi-private wireless networks, they will need to consider how to accommodate public safety, which may have specific extra requirements such as fireproof conduits and risers for Fiber.

In addition to these direct stakeholder groups, various industry ecosystems are catalysing the market for private wireless deployments. In the Wi-Fi world, the role of the Wi-Fi Alliance is longstanding, including its central focus on equipment certification. But the private cellular world is extending far beyond that:

- The US CBRS Alliance has helped define use-cases, lobby governments, coordinate testing and certification, and raise awareness.
- In the UK, the Government has sponsored various 5G trials and testbeds for industrial and public-sector applications, while the regulator and other bodies such as the Spectrum Sharing Association have convened workshops and coordinated different stakeholders.
- The Small Cell Forum has helped pushed Neutral Host and private network models
- 5G Alliance for Connected Industries (5G-ACIA) focuses on private and semi-private networks for industrial automation and factories.

We can expect such groups to continue to proliferate in every country releasing local or shared spectrum, as well as each industry sector deploying private wireless at scale.



# Conclusions and recommendations

## The future of private and semi-private wireless

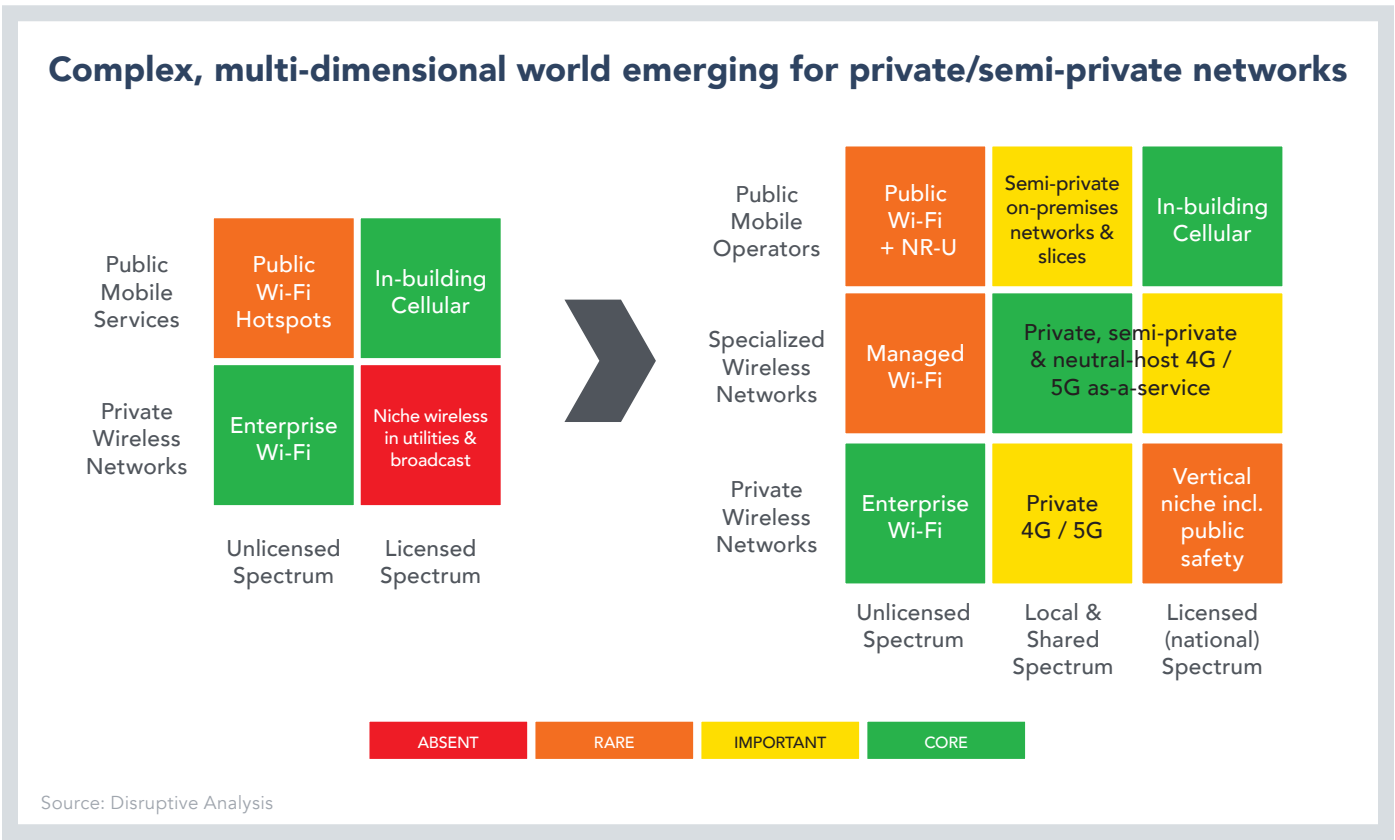
Enterprise wireless networks are evolving fast. Businesses are moving beyond connecting just smartphones and PCs, to a world of new on-premises mobile personal devices, many classes of IoT, automation, security and display systems, as well as mobile broadband for public-safety. At the same time, 5G makes many existing in-building systems look inadequate. Increasingly, these endpoints and the applications they service are better suited to private rather than public networks.

Against that backdrop of changing end-user needs, the industry is supplying better and more diverse wireless networks. Wi-Fi is improving rapidly with Wi-Fi 6 and additional 6GHz band spectrum. And cellular networks can now be deployed by both enterprises themselves as

fully-private systems, or by a new class of specialist service providers as semi-private managed services or wholesale neutral hosts.

New local and shared spectrum bands are key enablers, as are more “democratized” network infrastructure from small cells to cloud-based platforms.

Meanwhile, traditional MNOs are looking to compete, using customized enterprise-grade solutions of their own, offering enterprises a greater level of control, but without the same implementation and operational responsibilities as fully-private networks. That trajectory will continue with future iterations of 5G, bringing network-slicing and vertical-specific features in 3GPP Releases 16 and 17.





## Convergence, divergence or both?

In some senses, this increased range of approaches to networks could be characterized as “divergence”. There are more stakeholders, more business models, and more possible use-cases and applications. Organisations will need both Wi-Fi and cellular networks, and many will have to consider not just in-building but campus-wide coverage. They may have specific and valuable uses for private 5G, while still also needing to support normal use of public mobile networks when employees and visitors are indoors. There will be a need for new approaches to evaluating public/private wireless use-cases than in the past, and often a greater relevance for holistic network planning, design and operational tools that address both Wi-Fi and cellular domains.

And many more service providers and external stakeholders are becoming involved. As well as the normal mobile carriers wanting in-building coverage, new players also have important roles - from tower companies moving indoors, to cloud hyper-scalers pushing edge-compute and edge-networks for IoT. They create a new set of network operators, and new forms of “semi-private” models.

A previous iBwave eBook considered the trend towards convergence between different network types, as well as the underlying Fiber infrastructure. This trend still applies here – up to a

point. Given that many of these trends are taking place over periods of years, but with a different cadence, it will not be possible to combine everything into an elegant master-plan. It may be possible to combine midband 5G antennas with Wi-Fi access points – but then future shifts to mmWave may need additional units. Public-safety networks and associated regulations and codes are undergoing change, with different agencies involved and different speeds of adoption of broadband wireless. Some semi-private networks may be directly integrated with new IoT or industrial-automation systems, rather than linked to the existing wireless infrastructure.

We may also see convergence at a device or application level. A mobile AGV, or an employee with a smartphone, might switch from Wi-Fi to private 5G between buildings, or even bond both connections together for extra reliability. We can

expect various analytical tools to help optimise the wireless environment for coverage, application performance, security and even power consumption.

Perhaps a pragmatic vision involves “converge where you can, diverge where you have to” – and future-proof your designs and stress-test your assumptions, with as much rigour as possible. Business processes, vendor/integrator relationships, skill-sets and tools will need to reflect this extra complexity and nuance.



## The future of private wireless in the post-pandemic world

This eBook cannot ignore the impact of the COVID-19 pandemic. It will inevitably alter the world of wireless networks – public and private – in many ways. The world has changed immensely; workplaces and business venues will operate in different ways in the future. The economic fallout is likely to be significant, and potentially long-lasting.

As well as the terrible human and broad societal costs, there are narrower ramifications for networking generally, and for private wireless networks in particular. Businesses are

adjusting to the new environment, but there remains a need to update plans and strategy as far as possible. There is still a good – even accelerated - long-term future for private networks, in a post-pandemic world.

Clearly, there are many unknowns; the situation changes rapidly, so this can only be a snapshot. Further updates and analysis of the impact on the wireless industry – especially private cellular and smart buildings – will be posted on the author’s blog ([here](#)) and LinkedIn updates ([here](#)).

### Short-to-mid term: Now until early-2021:

- › Deploying private networks for utilities, mining, rail and public safety will likely be considered essential.
- › Flexible manufacturing, supply-chains (eg ports & logistics), utilities and medical sectors are likely to recover first, although top use-cases and priorities may change.
- › Airports/aviation, hotels, retail, sports and other consumer/indoor sectors will suffer the brunt of economic hardship and will be more likely to delay or cancel projects. Oil and gas sectors face problems because of oil prices.
- › Experimental / trial networks may be reassessed as urgent priorities by some enterprises, especially where non-essential tasks are halted.
- › Non-physical tasks such as private-network planning, design, training and software development will be conducted by staff working from home.
- › Governments and regulators are delaying some spectrum auctions and licensing functions.
- › Some national MNOs' 5G deployments may be delayed, especially enterprise-facing campus network and network-slicing offers. This may lead to greater focus on dedicated private and semi-private solutions for some verticals, including from niche SPs.

### Long-term: 2021-2025

Assorted scenarios can be described for the outcome of the pandemic, such as the success/failure to create viable vaccines, or the extent of economic damage and shape of the recovery. It is not possible to make accurate forecasts yet, but describing possible "future worlds" can help readers create coherent plans.

If we assume reasonable success at controlling the virus, plus a sharp-but-brief global recession with a sharp bounce-back, then we can make a guess at changed business and government priorities and social behaviours.

- › Most businesses will increase work on transformation and automation, although with more focus on "Just in Case" resilience and diverse supply chains. This could catalyse more private wireless networks, especially if connected to industry-wide federation or data-sharing for emergencies.
- › Governments may impose "stress test" and "adequacy" rules on public networks, similar to those on banks' financial health in the post-2008 financial crash era. This may drive more private cellular adoption alongside Wi-Fi and DAS systems.
- › Growing adoption of private 4G & 5G in industrial plants, factories and similar facilities, reflecting need for flexible processes, physical reconfiguration of manufacturing equipment etc. Also, higher requirements for remote monitoring and control, of onsite vehicles, fixed machinery and high-definition cameras.
- › There may be a reduced priority for deploying private cellular in offices, given permanent increase in working-from home.
- › We can expect a large focus by businesses and governments on "pandemic-proof" buildings, with more sensors and systems to manage occupancy, enforce social-distancing if another outbreak occurs, and improve infection-control and hygiene – for instance with disinfectant robots. These will all need improved indoor wireless systems. A full article on this scenario is linked here.
- › Slow recovery in travel, hospitality and retail sectors may dampen prospects for private networks, although indoor wireless coverage will remain important.

(Other scenarios, from dystopian nationalism, to near-utopian societal renaissance can also be explored – contact [information@disruptive-analysis.com](mailto:information@disruptive-analysis.com) for more details)

## Recommendations

Disruptive Analysis advises enterprises to consider the following actions:

- › Consider holistically all the current and likely future use-cases for wireless connectivity indoors and on-campus. Go beyond personal smartphone and PC use, to consider static and mobile IoT, visitor needs, public safety personnel and building/automation systems.
- › Engage with a long list of service providers (and current system suppliers that could offer managed services in future) to understand their relationship to public/private wireless connectivity, partnerships, and vision for the next 5 years.
- › Assess the current skills and readiness of IT and networking staff in the planning deployment and operation of wireless systems. Look to ensure that skills, tools, partners and infrastructure can span Wi-Fi and cellular domains.
- › Understand the myths and realities of 5G, especially with regard to indoor coverage and performance, as well as network-slicing and device support.
- › Keep abreast of new use-cases for private 4G/5G networks, and also Wi-Fi 6.
- › Examine recent and possible future regulatory trends for wireless, such as new rules on enterprise-suitable spectrum, plus also fire/safety codes and possible post-pandemic shifts in managing social distancing in emergencies.
- › Consider new business models emerging for private / semi-private wireless, such as neutral-host platforms from specialist providers, or the ability to operate as a local service provider for your own tenants or visitors.
- › Expect continued change over coming years, in terms of technology, spectrum, vendors and service-providers. Maintain up-to-date inventories of infrastructure and assess network performance in the light of new behaviours and applications.
- › Converge networks where you can – but diverge where it makes sense.



## About iBwave

iBwave Solutions, the standard for converged indoor network planning is the power behind great in-building wireless experience, enabling billions of end users and devices to connect inside a wide range of venues. As the global industry reference, our software solutions allow for smarter planning, design and deployment of any project regardless of size, complexity or technology. Along with innovative software, we are recognized for world class support in 100 countries, industry's most comprehensive components database and a well established certification program. For more information visit: [www.ibwave.com](http://www.ibwave.com).

## About Disruptive Analysis

Disruptive Analysis is a technology-focused advisory firm focused on the mobile and wireless industry. Founded by experienced analyst & futurist Dean Bubley, it provides critical commentary and consulting support to telecoms/IT vendors, operators, regulators, users, investors and intermediaries. Disruptive Analysis focuses on communications and information technology industry trends, particularly in areas with complex value chains, rapid technical/market evolution, or labyrinthine business relationships. Currently, the company is focusing on 5G, NFV, IoT networks, spectrum policy, operator business models, the Future of Voice, AI, blockchain & Internet/operator ecosystems and the role of governments in next-generation networks.

Disruptive Analysis attempts to predict and validate the future direction and profit potential of technology markets - based on consideration of many more "angles" than is typical among industry analysts. It takes into account new products and technologies, changing distribution channels, customer trends, investor sentiment and macroeconomic status. Where appropriate, it takes a contrarian stance rather than support consensus or industry momentum. Disruptive Analysis' motto is "Don't Assume".

For more detail on Disruptive Analysis publications and consulting / advisory services, please contact [information@disruptive-analysis.com](mailto:information@disruptive-analysis.com). For details about Private Cellular, Neutral Host and Horizon-Scanning workshops & publications, please see [www.deanbubley.com](http://www.deanbubley.com).

Website: [www.disruptive-analysis.com](http://www.disruptive-analysis.com)      Blog: [disruptivewireless.blogspot.com](http://disruptivewireless.blogspot.com)

Twitter: @disruptivedean      Quora: Dean-Bubley

## Intellectual Property Rights / Disclaimer

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, Disruptive Analysis Ltd.

Every reasonable effort has been made to verify research undertaken during the work on this document. Findings, conclusions and recommendations are based on information gathered in good faith from both primary and secondary sources, whose accuracy it is not always possible to guarantee. Disruptive Analysis Ltd. disclaims all warranties as to the accuracy, completeness or adequacy of such information. As such no liability whatever can be accepted for actions taken based on any information that may subsequently prove to be incorrect. The opinions expressed here are subject to change without notice.



