# Mobile Policy Handbook

## An insider's guide to the issues

2019

Do you have
the knowledge?

Can you take
a position?

Will you lead
the debate?

# Mobile Policy Handbook

## An insider's guide to the issues

# About this Handbook

Ever since the introduction of the first digital cellular services for commercial use in the 1990s, mobile networks have spread, evolved and changed our world. Massive infrastructure investment and competition among mobile operators, supported by enabling policies and regulation, have led to continual improvements in network speed and quality and have extended the reach of mobile services to the most remote rural communities.

The GSMA believes that a country's citizens benefit most when the private and public sectors work together in a spirit of openness and trust, as policymakers and regulators create the conditions that can attract telecoms investment, encourage innovation and strengthen digital trust.

This is why we are committed to supporting governments and regulators in their efforts to introduce pro-investment telecommunications policies. The Mobile Policy Handbook: An Insider's Guide to the Issues is part of the GSMA's efforts to promote such collaboration. A unique resource that assembles a range of policy topics and mobile industry positions and initiatives under one cover, it acts as a signpost to regulatory best practice.

As the global trade association of mobile operators, the GSMA conducts and commissions research on policy trends and challenges in the fast-moving mobile communications market. This handbook draws on the association's unique insight into the mobile sector and presents it in a practical way for those who want to explore the issues and unleash the value of mobile technology in their own market.

In this seventh edition of the Mobile Policy Handbook, new policy topics and industry positions have been introduced covering areas such as 5G and spectrum sharing. Throughout the book, the content has been refreshed with up-to-date statistics, new resources and industry insights.

The online version of this resource — **www.gsma.com/publicpolicy/handbook** — offers an always up-to-date catalogue of the mobile industry's policy positions.

Readers are encouraged to contact the GSMA if they have any questions or requests for more information. E-mail us at **handbook@gsma.com.**

# World-Changing Trends

The world has pivoted towards digital technologies to enable seamless communication, connection, commerce and all manner of internet-enabled services and solutions. These technologies are indelibly changing the way businesses operate and the way people live, work and play.

Mobile networks are at the heart of this digital transformation, as the primary channel over which people communicate and access online applications and the internet. However, the industry itself is now going through a transformation as it looks to a future that will be opened up by fifth-generation, or 5G, mobile networks.

It will appear in cities first, where mobile data volumes are climbing fastest and where a return on investment is most readily achieved. And it will seamlessly coexist with earlier mobile generations, which will connect citizens to the mobile internet for years to come.

Many countries will host their first commercial 5G network deployments in the next three years. The digital economy needs 5G to respond to booming demand for mobile data, enable a massive Internet of Things (IoT) and make possible an array of services that require fast, dependable, low-latency connectivity.

Governments have embraced the vision of 5G as the catalyst for economic growth and beneficial services. However, significant new investment will be needed to fund equipment costs as well as spectrum access licences and regulatory costs. Governments as well as regulatory authorities will therefore play a crucial role in enabling efficient and timely deployment of next generation mobile networks while bringing down the costs for operators.

5G networks will be central to the realisation of an advanced digital economy and society, but supportive policy and regulations must be deployed to make 5G a reality. We hope this handbook will prove useful as a compass to help navigate the policy and regulatory challenges that lie ahead on the path to the next generation.

## #BetterFuture



## Mobile For Development



## Capacity Building



## Mobile Initiatives

## Business Environment



## Spectrum Management and Licensing



## Consumer Protection



## Appendix

# #BetterFuture

The UN's 2030 Agenda for Sustainable Development details 17 Sustainable Development Goals (SDGs) that act as the world's to-do list to end poverty, reduce inequalities and tackle climate change.

With its unprecedented scale and growing impact on daily lives, mobile is a powerful tool for achieving the SDGs. Countries with high levels of mobile connectivity have made the most progress in meeting their SDG commitments — put simply, quality of life improves as people gain access to mobile technology.

The GSMA has reviewed the industry's contributions towards achieving the goals in three in-depth reports since 2015. The 2018 edition of the Mobile Industry Impact Report highlights that the industry is continuing to build on the positive impact it is having across all 17 SDGs.

The strongest overall impact is on SDG9 — industry, innovation and infrastructure. Mobile is enabling innovation and new business models such as the sharing economy, mobile savings and credit, and pay-as-you-go solar models to access clean energy. It also allows businesses to expand trade and enhances the productivity of industry.

The report highlights that, out of all the goals, the mobile industry's impact on SDG13 (Climate Action) and SDG11 (Sustainable Cities and Communities) has improved most from its 2015 baseline. A key driver of this increased impact is the use of mobile phones to provide essential humanitarian assistance during epidemics and natural or climate-related disasters. Since committing to the SDGs, the mobile industry has played a much larger and increasingly expanding role in humanitarian response. In 2017, the response efforts of mobile operator signatories and humanitarian partners in the Humanitarian Connectivity Charter reached more than 30 million people affected by crisis and disasters.

There are three specific characteristics — covered in greater detail overleaf — that explain how the mobile industry continues to increase its contribution across all SDGs: deployment of infrastructure and networks; access and connectivity; and enabling services and relevant content.

Furthermore, new and emerging areas — such as IoT, Big Data and artificial intelligence — are demonstrating their potential to have transformative impacts on peoples' lives.

The industry has a clear incentive to drive improvements beyond 'business as usual' and accelerate activities that contribute to the SDGs. The reason is that the SDGs not only ensure a healthy and viable society but also offer new and substantial commercial opportunities, through more inclusive and prosperous societies, dynamic and inclusive marketplaces, reliable regulatory frameworks and thriving ecosystems. Detailed over the next six pages is a small selection of ways in which the industry is driving these improvements.

# Improving the industry's impact on the SDGs

Three underlying trends explain much of the improvement in the industry's impact on the SDGs since 2015:

### Deployment of infrastructure and networks

The mobile industry drives impact through the provision of, and investment in, high-performing mobile networks, which provide the foundations for the digital economy and act as a catalyst for a diverse and innovative range of services. More than four-fifths of the world's population — around 6.9 billion people — are now within reach of a 4G network, while overall 3G coverage rose to more than 91 per cent in 2018. In addition, wider coverage as well as improved network quality and resilience enables the industry to play a critical role before and during epidemics, conflicts and natural or climate-related disasters.

Improvements

**Population coverage**

3G 80% 2015 → 91% 2018 More than **6.9 billion** people covered

4G 48% 2015 → 81% 2018 More than **6.2 billion** people covered

Source: GSMA Intelligence

**Network quality**

Average mobile broadband download speed

14 Mbps 2015 → 22 Mbps 2017

57% increase

Source: Based on analysis by Ookla® of Speedtest Intelligence® data for 2015 to 2017

### Access and connectivity

Operators continue to connect the unconnected, adding 795 million unique new subscribers from 2015 to 2018, bringing the total to 5.1 billion. An increasing number of people are moving beyond voice to take up mobile internet services, enabling them to participate in the digital economy. During the same period, there were 851 million new mobile internet subscribers, bringing the total to 3.5 billion. Mobile technology also increases productivity and the efficient use of resources in industry, for example via industrial Internet of Things (IoT) and smart energy grids. From 2015 to 2018, there were 649 million more cellular IoT connections, bringing the total to 969 million.

Improvements

**Unique mobile subscriber penetration**

62% 2015 → 67% 2018

**5.14 billion** subscribers

795m new subscribers

Source: GSMA Intelligence

**Mobile internet subscriber penetration**

36% 2015 → 46% 2018

**3.5 billion** mobile internet subscribers

851m new mobile internet subscribers

**Cellular IoT connections**

320m 2015 → 969m 2018

203% increase

### Enabling services and relevant content

Mobile technology has enabled a range of life-enhancing services such as mobile financial services, mobile agriculture and mobile health. In 2017, there were 690 million registered mobile money accounts worldwide, and mobile money platforms were processing more than $1 billion a day, helping to expand financial and social inclusion. Meanwhile, new and emerging areas such as IoT, Big Data and artificial intelligence are demonstrating their potential to have transformative impacts on lives. For example, the implementation of IoT and Big Data solutions for improved environmental monitoring is helping reduce the adverse environmental impact of cities.

Improvements

**Active mobile applications available on smartphones**

3.5m 2015 → 5.8m 2017

65% increase

Source: Appfigures

**Including**

Education 62% increase

480,000 2015 → 780,000 2017

Health 66% increase

165,000 2015 → 275,000 2017

**Use of mobile-enabled services**

In 2017, **850 million subscribers** (more than 15% of total) used mobile to access government services

In 2017, **1 billion subscribers** (20% of total) used mobile to access health services

In 2017, **1.2 billion subscribers** (25% of total) used mobile to access education services

Source: GSMA Intelligence

Case Studies

### How mobile is contributing to achieving SDG targets

Since committing to playing a leading role in delivering on the Sustainable Development Goals, the industry has increased its impact across all 17 goals. Below are four practical examples that highlight how the industry is making a difference.

#### Latin America: Bringing school to life in the Amazon

Over one million children in Peru live too far from a school to get access to the best education. As a result, only 10 per cent of girls and boys understand what they read. Telefónica is helping to address this by bringing digital learning to the most remote parts of the Amazon rainforest via its Mobile Classroom. The project supplies a portable teaching station to schools. This includes a computer (which also acts as a network server), monitor, multimedia projector, speakers and educational resources. There are also laptops for the students and a power source so the laptops can be charged. The Mobile Classroom is allowing teachers to take advantage of the latest innovative teaching methods and giving students access to exciting educational resources.

#### Asia: Mobile apps boost birth registration

In Pakistan, approximately 60 million children remain unregistered, with registration rates lowest among girls, children from rural areas and those from the poorest households. Registering a birth can be difficult, in some cases nearly impossible — especially for children born at home, in remote locations or in displacement.

UNICEF, Telenor and the Punjab and Sindh provincial governments collaborated to create and deploy a mobile app which allows health workers and marriage registrars to send birth data directly to authorities. Officials use a PC-based dashboard to review information and monitor progress.

The four-month pilot project doubled registration rates in the target districts. A renewed project targets an additional 700,000 registrations over two years in nine new districts.

#### North America: Drone-mounted cell sites boost humanitarian response

Following Hurricane Maria, 90 per cent of Puerto Rico's telecoms infrastructure was damaged, costing an estimated $1.2 billion.

In response, AT&T deployed a drone-mounted cell site to provide data, voice and text services. These provided wireless connectivity to customers and recovery teams in an area up to 40 square miles, flying 200 feet above the ground.

The ability of these airborne cell sites to extend coverage further than other temporary cell sites makes them ideal for providing coverage in remote areas. Although this was the first time a drone-mounted LTE cell site was successfully deployed to connect residents after a disaster, it still managed to carry dozens of gigabytes of data, facilitating thousands of calls and texts.

#### Africa: Apps and SMS help improve nutrition

In Uganda, poor nutrition is linked to deaths from diarrhoea, malaria and pneumonia for children, and from anaemia for pregnant women. Some 29 per cent of children under five years old are considered to be stunted.

Non-governmental organisation Living Goods Uganda has responded by deploying a network of door-to-door community health workers (CHWs) who guide families towards improved health and well-being. They use an app called SmartHealth to record household information and make health assessments. A separate SMS service sends customers life-saving maternal and newborn health information.

Some 82 per cent of users who had a consultation with a CHW and received SMS on this topic reported to be exclusively breastfeeding their babies — a 32 per cent improvement of over non-users.

Resources:
GSMA Report: 2018 Mobile Industry Impact — Sustainable Development Goals
GSMA Report: 2017 Mobile Industry Impact — Sustainable Development Goals
GSMA Report: 2016 Mobile Industry Impact — Sustainable Development Goals
GSMA Handbook: Champions for a Better Future
GSMA App: Sustainable Development Goals — The SDGs in Action
Case for Change website

# Big Data for Social Good

The mobile industry is harnessing Big Data to help public agencies and NGOs tackle infectious disease, disasters and environmental impacts. Protecting privacy remains at the core of Big Data developments — and the mobile industry is committed to the responsible use of data and the protection of privacy. By aggregating and anonymising the data collected by their networks, mobile operators can provide insights into human movement patterns without comprising individuals' privacy. When this data is enriched with third-party data sources — such as hospital intakes, death counts and weather data — it can enable relief agencies to make decisions on when, where and how to deploy resources.

The GSMA's Big Data for Social Good programme is developing consistent methodologies and sustainable approaches that mobile operators can use to share relevant insights from this data with public agencies and NGOs, while building an ecosystem to support timely planning and response. The initiative is now backed by 20 operators, accounting for over two billion connections in over one hundred countries. From the start, the Big Data for Social Good initiative established a robust code of conduct to ensure all activity respects and protects individuals' privacy.

## First Wave of Projects — Health

The first wave of the programme's collaborative projects leveraged Big Data for health via three initiatives: one in Brazil, one in India, and the final one across three countries: Thailand, Bangladesh and Myanmar.

Air pollution kills thousands each year in Brazil's cities. In response, mobile operator Vivo collaborated with São Paolo municipalities to predict air quality. Deploying new sensors or carrying out surveys to predict pollution levels is both costly and labour intensive. Instead, Vivo harvested data from existing sensors and combined it with anonymised mobile traffic and location data to predict high-pollution zones up to 48 hours in advance. This armed municipalities with the information they needed to take action.

Across India, tuberculosis kills hundreds of thousands of people each year, but the government aims to end the disease entirely by 2025. Mobile operator Bharti Airtel supplied anonymised, aggregated mobile data from 280 million people to be combined with health and disease data from multiple other sources. The idea is to predict tuberculosis hotspots and locate hidden cases. This in turn will allow health services to understand where best to deploy mobile clinics and vaccination programmes or to launch awareness campaigns.

In Southeast Asia, malaria-causing parasites travel fast, ignore borders and are increasingly immune to anti-malarial drugs. If resistance spreads beyond the region, it could massively increase malaria deaths worldwide. Mobile operator Telenor had already partnered with the Harvard School of Public Health to fight dengue. This time, they are using mobile Big Data and adding Thailand's Mahidol Oxford Tropical Medicine Research Unit as a partner. The goal is to model the population movements that spread multi-drug resistant malaria around Thailand, Bangladesh and Myanmar.

## Second Wave of Projects — Disaster Preparedness

The next wave of the programme will tackle disaster preparedness and response, with early stage projects across Japan, Colombia, Russia and Turkey. In Japan, three operators are working to produce live displacement maps linked to seismic activity. In Colombia, Telefonica is working on models to predict flooding and climate impact. In Russia, MegaFon is gestating plans to use Big Data to help people displaced by natural disasters. In Turkey, Turkcell wants to use Big Data to prepare and recover from earthquakes.

Resources:
Big Data for Social Good website
Big Data for Social Good video
Telefónica Case Study: Predicting Air Pollution Levels 24 to 48 Hours in Advance in São Paulo, Brazil
ITU Blog: How AI and Big Data are Tackling the Health Impacts of Urbanisation

# Mobile for Development

The transformative power of mobile is most apparent in emerging markets where it is usually the most widespread and reliable infrastructure. Isolated populations in these countries are often underserved by basic services, so this puts the mobile industry in a unique position to help connect them to key infrastructure, as well as to health and financial services.

Mobile for Development (M4D) is a dedicated global team within the GSMA, which brings together our mobile operator members, tech innovators, the development community and governments, to harness the power of mobile in emerging markets. The team identifies opportunities and helps deliver innovations in financial services, health, agriculture, digital identity, energy, water, sanitation, disaster resilience and gender equality.

A key part of M4D's strategy involves taking advantage of the synergies between the different strands of the team's work to amplify the overall impact of the programme. For example, it works to identify ways to leverage mobile money payments alongside machine-to-machine communication to help improve access to energy, clean water and sanitation in emerging markets. Correspondingly, it promotes the use of digital identity solutions to support the registration of newborn babies via mobile phones, which can then boost the effectiveness of maternal health programmes.

The programme continues to demonstrate impact across a number of important areas. For example, mobile money services have helped to greatly reduce financial exclusion over the past decade, as there are now 690 million mobile money accounts across more than 90 countries. Furthermore, the mHealth programme reached just under 1.6 million women and households with lifesaving maternal and health information in eight sub-Saharan countries over the last two years.

Via its Mobile for Humanitarian Innovation Fund, the GSMA is also helping allocate grants to innovators whose activities bolster crisis response, while its Ecosystem Accelerator Innovation Fund is supporting start-ups in Africa and Asia Pacific with non-equity funding, mentorship and technical assistance to help them create commercially sustainable products and services.

Through these activities and more, M4D's work seeks to test the feasibility of new ideas, support the spread of those with the most potential and scale those projects that have proven their worth. This section details how these efforts are translated into real projects with meaningful socio-economic impact.

# Connected Society

## Background

During 2018, an additional 270 million people connected to the mobile internet, bringing the total number to 3.6 billion globally.[1] Despite this achievement, more than four billion people remain offline. This is known as the 'digital divide'. It includes one billion people who are currently not covered by mobile broadband networks (representing the 'coverage gap'), and three billion people who live within the footprint of a network but are not accessing mobile internet services (equating to the 'usage gap'). In developing markets, mobile is the cheapest and often only way of accessing the internet. This means that accelerating mobile internet connectivity and usage is critical to supporting the growth of the digital economy and ensuring no-one is left behind. In that context, digital inclusion has become a key facilitator for a range of essential mobile-enabled services in the areas of healthcare, education, utilities and financial services.

## Programme Goals

The GSMA's Connected Society programme focuses on accelerating digital inclusion. It works with the mobile industry and key stakeholders to increase access to and adoption of the mobile internet, spotlighting underserved population groups in developing markets. The programme supports the mobile industry in its efforts to extend network coverage and address consumer barriers to mobile internet adoption in order to unlock the significant socio-economic benefits of increased digital inclusion.

## Public Policy Considerations

Significant progress has already been achieved but, based on current trends, almost 40 per cent of the world's population will still be offline by 2025. The reasons for the mobile digital divide are complex and rooted in a range of social, economic and cultural factors. Accelerating mobile internet adoption will require deliberate and strategic efforts by the mobile industry, policymakers and the international community, particularly for rural populations, women and other underserved groups.

The following areas will require particular attention:

**Enabling rural broadband expansion.** Offline populations typically have low income levels and live in sparsely populated, rural areas that lack enabling infrastructure such as electricity and high-capacity fixed communications networks. All of these factors adversely affect the business case for mobile network expansion in these locations. Policymakers should acknowledge that the mobile industry cannot close the coverage gap without the government's support. Instead, they can enhance incentives to invest in rural infrastructure by aligning key policies around best practices. These include adopting coverage-driven spectrum allocation and pricing, implementing investment-friendly tax policies, facilitating access to public infrastructure, reducing red tape for deploying mobile infrastructure, and encouraging voluntary infrastructure sharing.

**Breaking down barriers to mobile internet usage.** The majority of people who remain unconnected to the mobile internet are already living in areas with network coverage. Closing this 'usage gap' will require stakeholders to tackle issues in four key areas: affordability, usability and skills, relevance, and safety. Key considerations for governments include:

- Avoiding the introduction of distortionary or disproportionate taxes on mobile handsets as they negatively impact the affordability of these devices, which remains a key barrier for many people in developing markets.
- Prioritising digital skills in formal education and through government supported training programmes.
- Developing e-government services to help drive an increase in the amount of relevant content and services available to citizens and, in turn, improve the accessibility and efficiency of government service.
- Strengthening action against internet-related abuse and harassment, including through legal and policy measures, to build trust around the mobile internet, particularly among women.

[1] Source: All figures quoted are GSMA Intelligence, Q4 2018 estimates unless otherwise stated.

Resources:
GSMA Connected Society Website
GSMA Mobile Internet Skills Training Toolkit
GSMA Report: State of Mobile Internet Connectivity 2018
GSMA Report: Enabling Rural Coverage — Regulatory and Policy Recommendations to Foster Mobile Broadband Coverage in Developing Countries
GSMA Report: Rural Coverage — Strategies for Sustainability
GSMA Report: Unlocking Rural Coverage — Enablers for Commercially Sustainable Mobile Network Expansion
GSMA Report: Accelerating Affordable Smartphone Ownership in Emerging Markets

# Connected Women

### Background

Mobile connectivity has grown rapidly, but it is not reaching everyone equally. Many women are being left behind in today's increasingly connected world. Women in low- and middle-income countries are 10 per cent less likely to own a mobile phone than men on average[1], which translates into 184 million fewer women owning mobile phones.[2]

Even those women who do own a mobile tend to use it less frequently and intensively than men, especially for more transformational services such as mobile internet and mobile money. Women are on average 26 per cent less likely to use mobile internet than men and 33 per cent less likely to use mobile money.[3]

Barriers to both access and use of mobile products and services often disproportionately affect women. These barriers include network coverage, the cost of handsets and services, concerns around security and harassment, and a lack of technical literacy and awareness of relevant products and services.

Closing the gender gap in mobile phone ownership and usage can substantially empower women, opening up access to information and life-enhancing opportunities — such as health information, financial services and employment opportunities — often for the first time.

The gender gap won't close on its own. The social, economic and cultural barriers driving it can only be overcome with intervention by all stakeholders — including policymakers — collaborating with the mobile industry.

### Programme Goals

The GSMA Connected Women programme focuses on accelerating digital and financial inclusion for women. Its mission is to reduce the gender gap in access and use of mobile internet and mobile money services in low- and middle-income countries.

It works with mobile operators and their partners to address the barriers to women's use of these services, unlock this substantial market opportunity for the mobile industry, deliver significant socio-economic benefits and transform women's lives. By July 2018, 36 operators had committed to reducing the gender gap in their mobile internet, their mobile money customer base or both by 2020.

### Public Policy Considerations

To address the gender gap, policymakers and regulators should take a holistic approach to the issue that respects both local and cultural sensitivities. Strategies, policies and budgets that explicitly address women's needs, circumstances, capabilities and preferences are essential if governments are to truly make progress. The adoption of clear targets around women's access to mobile internet and mobile money is encouraged, along with the implementation of proper accountability structures to ensure these targets are met.

Creating a supportive policy environment is an essential first step to making progress towards three objectives. Such an environment will help address issues of gender equality and social norms. It must ensure that mobile devices and services are accessible, affordable, usable, safe and relevant for women. It must also ensure that women have the skills and confidence to use them.

For example, it is important to ensure appropriate policy and regulation is in place to lower cost and access barriers for customers. This can be achieved by reducing mobile-specific taxes, supporting voluntary infrastructure sharing among licensed operators and releasing sufficient spectrum at affordable cost.

Furthermore, governments can consider strategies for increasing mobile and digital skills through changes to school curriculums and having training programmes for women who lack digital skills. It may also be appropriate to address harassment via mobile phones and the mobile internet through awareness campaigns or legal and policy frameworks.

Targeted regulatory interventions can also play a key role in addressing the challenges that disproportionately affect women. In the context of mobile money for example, the adoption of flexible agent regulation and of tiered know-your-customer (KYC) requirements can go a long way in driving mobile money adoption among women.

Data is critical to help regulators and policymakers better understand the barriers women face. Demand-side data in particular can be an invaluable source of insights and also tends to be more reliable than supply-side data. Policymakers are encouraged to adopt creative approaches to ensure accurate sex-disaggregated data is available. This allows decision-makers to inform their own policies, monitor the gender gap and support operators and others in developing customer-centric approaches focusing on women.

1 According to the GSMA's 2018 Mobile Gender Gap Report.

2 'Mobile' or 'mobile phone' ownership refers to personally owning a SIM card, or a mobile phone which does not require a SIM; and using it at least once a month.

3 According to the World Bank's 2017 Findex Report.

*We call for immediate measures to achieve gender equality in internet users by 2020, especially by significantly enhancing women's and girls' education and participation in ICTs, as users, content creators, employees, entrepreneurs, innovators and leaders.*

— UN General Assembly, WSIS+10 Outcome Document

Resources:
GSMA Connected Women website
Broadband Commission Working Group on the Digital Gender Divide — Recommendations for Action: Bridging the Gender Gap in Internet Access and Use
GSMA Report: The Mobile Gender Gap Report 2018
GSMA Report: Triggering Mobile Internet Use Among Men and Women in South Asia
GSMA Report: Bridging the Gender Gap — Mobile Access and Use in Low-and-Middle-Income Countries

# Digital Identity

## Background

The ability to prove that you are who you say you are and have this information authenticated when interacting with the state or private companies is critical to accessing basic services such as healthcare, education and employment, as well as exercising voting rights or benefiting from financial services. Yet World Bank estimates from 2018 indicate that at least one billion people lack any form of officially recognised ID, either paper or electronic.[1] This problem disproportionally impacts rural residents, poor people, refugees, women, children and vulnerable groups; and is most pronounced in Africa and Asia. The international community has recognised this so-called 'identity gap' as a critical barrier to achieving inclusive and sustainable social and economic development. Indeed, the ninth target of UN Sustainable Development Goal (SDG) 16 aims for everyone to have a legal identity by 2030.

The identity gap is both a symptom of slow economic development and a factor that makes development more difficult and less inclusive. The problem is particularly stark when it comes to birth registration, with Unicef figures showing that one in four children under five lacks a legal identity simply because their birth wasn't registered. World Bank research in sub-Saharan Africa indicates that more than half of the population lacks an official identity, yet more than two-thirds of residents in the region have a mobile phone. These figures highlight the transformative potential of mobile to bridge this identity gap and catalyse greater socio-economic impact in emerging markets.

## Programme Goals

The GSMA Digital Identity programme is working with mobile operators, governments and the development community to demonstrate the opportunities and value of mobile as a scalable and trusted platform to enable robust digital identity solutions for the underserved, leading to greater social, political and economic inclusion.

Mobile operators are ideally placed to play a leading role in the development of a digital identity ecosystem because they have:

- Immense reach — they connect more than five billion unique subscribers worldwide.
- Extensive networks of agents that can be used for face-to-face verification.
- A local presence that is bound by local licences and laws.
- The ability to access unique customer attributes through network management tools.
- Experience in partnering with governments and service providers.

## Public Policy Considerations

Digital identity has the power to increase digital, social and financial inclusion, drive economic growth, support more efficient and transparent processes and prevent fraud. Mobile operators can play a number of roles in advancing digital identity ecosystems and accelerating governments' digital transformation strategies. For example, they could leverage their nationwide reach to support residents' enrolment into new digital identity systems.

They could also validate people's existing identity credentials against government databases, where these exist, to strengthen 'know your customer' (KYC) processes.

To enable mobile-based digital identity solutions, policymakers should consider investing in and promoting e-government services.

Furthermore, an enabling regulatory environment needs to be put in place if mobile is to deliver digital identity solutions to the underserved. Governments must first ensure consistency between the different legal and regulatory instruments that affect the management of digital identity. They must also work to break down any legal, policy and regulatory barriers that may inhibit the roll out of mobile identity services.

For example, in at least 147 countries mobile operators are already subject to identity-related requirements, such as mandatory SIM registration and KYC obligations for mobile financial services. Taking an integrated policy approach to these requirements would boost momentum towards mobile-based digital identity. It is also important for policymakers to ensure that a critical mass of citizens has had the opportunity to access an official form of ID before imposing any requirements on mobile operators to disconnect users who failed to register their SIM using an ID. Consideration should be given to the needs of underserved and vulnerable groups including refugees, those in remote areas or those with disabilities.

Governments also carry a responsibility to foster a trusted environment where consumers' privacy is respected, by adopting data protection and privacy frameworks based on international best practices. Finally, governments should also actively engage with mobile operators, key stakeholders and the wider identity ecosystem to help drive interoperability and innovation.

[1] World Bank: Identification for Development (ID4D) global data set.

Resources:
GSMA Digital Identity Programme website
GSMA SIM Registration website
GSMA Report: Access to Mobile Services and Proof of Identity
GSMA Policy Note: Enabling Access to Mobile Services for the Forcibly Displaced

# Ecosystem Accelerator

### Background

The mobile industry has had a hugely positive impact on the lives of citizens in developing nations because it has delivered a wide range of innovative services at unprecedented scale. However, many opportunities remain untapped because innovative start-ups in emerging markets face challenges in establishing partnerships with mobile operators and vice versa.

For example, start-ups commonly report fundamental issues related to differences in organisational goals, business language or technical limitations around incompatible application programming interfaces (APIs). Conversely, operators report a lack of market insight, a scarcity of appropriate partners and a dearth of clear business models when attempting to partner with local start-ups. Operators are also struggling to identify the best candidates for collaboration because they are flooded with requests for partnerships from a large number of start-ups.

As a result, mobile operators miss out on new innovations and commercial opportunities — including potentially disruptive ones — at a time when other players are becoming increasingly influential within the ecosystem. This is highlighted by GSMA research carried out in March 2018, which found that there were around one thousand active tech hubs in Africa and emerging markets in Asia Pacific. Of these hubs, half report a partnership with at least one tech giant — such as Microsoft, Google and Amazon — but only 10 per cent were partnering with a mobile operator.[1]

### Programme Goals

In emerging markets, mobile operators have reached the scale that start-ups lack, while start-ups are developing the local innovation mobile operators need. The GSMA Ecosystem Accelerator works to bridge the gap between mobile operators and start-ups, enabling strong partnerships that support the growth of commercially sustainable mobile products and services. By kickstarting dialogue between start-ups and mobile operators, the programme helps create synergies and expand the scale of the most promising ideas. This, in turn, helps the industry deliver the most impactful mobile solutions to the people and places that need them the most.

Through the Innovation Fund in particular, the programme leverages public sector capital to provide funding and tailored support to competitively selected start-ups in emerging markets that can deliver strong socio-economic impact.

The Innovation Fund supports start-ups in Africa and Asia Pacific with non-equity funding, mentorship and technical assistance, as well as by facilitating partnerships with mobile operators. As of July 2018, the programme has committed £5.5 million, and funded startups have tripled this money from other sources. During its lifetime, the programme will award over £7 million to help start-ups in Africa and Asia-Pacific realise their commercial and social potential.

Since it started in 2016, the fund has received more than 1,650 applications globally from start-ups across multiple verticals, focused on leveraging mobile technology to tackle the UN Sustainable Development Goals. As of August 2018, 24 start-ups from 15 markets have received funding from the GSMA Ecosystem Accelerator Innovation Fund, positively impacting some 1.5 million people.

The Ecosystem Accelerator programme is supported by the UK Department for International Development (DFID), the Australian Government, the GSMA and its members.

### Public Policy Considerations

The innovative ideas and nimble working practices that start-ups bring to business mean they often have a huge impact on both economies and societies.

As a result, governments now have a duty to implement policies that help start-ups act and move quickly. For example, governments can help by reducing bureaucratic barriers, improving access to capital, encouraging talent development and fostering a culture of innovation where risk-taking is not punished.

Governments can also have an impact by becoming more involved in supporting local tech hubs, given their potential to facilitate the creation of new jobs and to develop solutions that tackle social challenges and positively engage young people. Promoting investment in local start-ups also helps broaden the available range of locally relevant content and services. This can help drive the uptake of the internet and digital services among the broader population. Multilateral and non-government organisations also have a role to play in the emerging tech innovation landscape, particularly in providing technical support and a platform for collaboration.

Key ecosystem stakeholders also need to collaborate to ensure that new mobile-based solutions achieve scale and sustainability. For example, mobile operators can help by opening up APIs to third-party developers and start-ups. This will encourage even more innovation in the mobile ecosystem.

[1] From the GSMA Blog: 1000 Tech Hubs are Powering Ecosystems in Asia Pacific and Africa.

Resources:
GSMA Innovation Fund website
GSMA Ecosystem Accelerator Innovation Fund Portfolio
GSMA Ecosystem Accelerator Insights

# Mobile Agriculture

## Background

Agriculture contributes around 23.7 per cent of GDP in the world's least developed countries[1], with over 450 million smallholder farmer households depending on agriculture for their livelihood. However, smallholder farmers are increasingly vulnerable to volatile climate patterns affecting their yields. In addition, farmers, cooperatives and agribusinesses in agricultural value chains face many inefficiencies. The largest of these is the predominance of cash transactions, but there is no shortage of other issues. These include a lack of knowledge of the latest farming practices, of visibility into the value chain overall and of the agricultural assets available to farmers, like tools, inputs and equipment.

With mobile penetration across the world's developing regions expected to reach 68 per cent by 2025, mobile can deliver efficiencies and improve the business performance of both large- and small-scale agriculture operations.

Mobile can deliver the critical economic and climatic information that smallholder farmers need to improve their decisions. In addition, mobile offers a pathway to financial inclusion for mostly unbanked smallholder farmers. The digitisation of agricultural payments for the sale of crops via mobile money can support the formation of a financial identity and thus enable access to a range of services including credit, savings and insurance.

The GSMA forecasts that between 2017 and 2025 across sub-Saharan Africa, South Asia, East Asia and Latin America, some 350 million people will get their first mobile phone. Provided that mobile operators and other mobile money providers are able to operate in an enabling environment, a significant share of these people (many of whom are farmers) could be added as new mobile money customers. The main opportunities for digitisation within agricultural value chains are business-to-person and government-to-person transfers, which the GSMA estimates as worth around $2 billion and $202 million of revenue each year.

Evidence of the social impact of mobile services suggests that mobile-based information services targeting smallholder farmers in the developing world are driving behavioural change and livelihood benefits. Active users of mobile information services have reported significantly more on-farm changes than comparable non-users. This includes planting, land management and harvesting. For instance, in Pakistan active users of GSMA-supported services are 1.9 times more likely to report an increase in income than non-users.

## Programme Goals

The GSMA mAgri programme forges partnerships between mobile operators, technology providers and agricultural organisations. It supports scalable, commercial mobile solutions that impact smallholder farmers and the agricultural industry at large. As of March 2018, the GSMA mAgri programme had supported 12 projects, which had reached over 13.3 million smallholder farmers across Asia and Africa with mobile agricultural and nutritional services to improve their yields.

## Public Policy Considerations

In some cases, national Ministries of Agriculture have been important for the success of information-based mAgri services, for example by providing validation for the content that mobile network operators send to farmers.

However, there are also some challenges that need to be addressed, such as:

**The need for proportional know-your-customer (KYC) rules:** Complex due diligence processes impede mobile money service uptake in rural areas, since many farmers and agents are unlikely to have the official documentation needed to sign up for a mobile money account. Those seeking to enable uptake of mobile money services in rural areas must strike the appropriate balance between relaxing due diligence requirements and maintaining financial sector integrity. Where national ID schemes are particularly weak — including Fiji, Somaliland and parts of India — some financial service regulators have allowed providers to open mobile money accounts using alternative forms of documentation, including reference letters from village elders, employers and government officials.

**Mobile money transaction value and account size limits:** In many countries, the mobile money transaction value and account size limits mandated by financial sector regulators are not able to handle the size and value of payments for the sale of crops from agribusiness to farmers.

Business-to-person payments in agricultural value chains are the most likely entry point to financial inclusion for farmers, so it is imperative that service providers and regulators understand the unique nature of the agricultural sector. Failing to do so risks cutting off the full breadth of opportunities in the digitisation of agricultural payments. In countries such as Ghana, Haiti, and Sri Lanka, where mobile operators are digitising agricultural last mile payments for the procurement of key cash crops, the transaction value and account size limits mandated by regulators have posed challenges to the implementation of digital payments.

**Supporting mobile Internet of Things (IoT) for climate resilience:** Mobile IoT and Big Data are crucial for bridging the data gap in weather monitoring and forecasting. To enable innovation in this space, national governments must allow public-private partnerships between domestic meteorological agencies, commercial weather service providers and mobile operators. Many governments view meteorological data as state-owned and so have prevented private providers from disseminating weather alerts. This has been a roadblock to leveraging the potential of mobile technology for weather monitoring and forecasting.

[1] According to World Bank data.

Resources:
GSMA Report: Creating Scalable, Engaging Mobile Solutions for Agriculture
GSMA Report: Prerequisites to Digitising the Agricultural Last Mile
GSMA Report: Opportunities in Agricultural Value Chain Digitisation — Learnings from Cote D'Ivoire
GSMA Report: Opportunities in Agricultural Value Chain Digitisation — Learnings from Ghana

# Mobile For Development Utilities

## Background

Rapid network expansion means mobile now reaches further than the electricity grid, piped water networks and sewerage networks in most emerging markets. For example, while mobile coverage has grown extensively to cover more than 95 per cent of the world's population, 2.4 billion people still lack access to improved sanitation solutions.[1] The result is a widening gap between access to mobile and access to basic utility services. In fact, by 2015 mobile networks covered more than 855 million people without access to electricity, more than 373 million people without access to clean water and 1.97 billion without access to improved sanitation, according to the GSMA's Mobile for Development (M4D) programme.

This shortfall of affordable and sustainable utility infrastructure has a profound impact on people's lives. For example, according to figures from charity WaterAid, nearly 300,000 children under the age of five die each year due to diarrhoeal diseases caused by poor water and sanitation. Poorer people living off the electricity grid in emerging markets also often end up relying on expensive and harmful energy sources, such as kerosene, which suffer from fluctuating prices. As a result, a middle-class family in Europe can pay less for energy than a poor family in a country such as Bangladesh.[2]

However, by leveraging the enormous reach of mobile — as well as innovative mobile technologies and services, including machine-to-machine (M2M) communication and mobile money — the industry is well positioned to help bring the life-changing benefits of energy and clean water and sanitation to huge numbers of people in emerging markets.

## Programme Goals

Challenges to providing universal access to energy, water and sanitation services include last-mile distribution, operation and maintenance costs, as well as payment collection.

The GSMA Mobile for Development (M4D) Utilities programme focuses on leveraging mobile network technology and infrastructure to help solve these challenges in emerging markets.

The programme was established in 2013 with funding from the UK's Department for International Development. The programme has also launched the M4D Utilities Innovation Fund, which aims to accelerate the development of promising mobile technologies and business models that target improved access to energy, water and sanitation services. By July 2018, the fund had given grants to 53 organisations spread across four continents. The $12 million granted has unlocked a further $275 million from the private sector and benefited 4.5 million people in total.

The key goals of the programme include:

- Supporting the Innovation Fund grantees and their mobile operator partners to help them deliver on the promise of their trials.
- Demonstrating the commercial viability of improving energy, water and sanitation access using innovative mobile technologies.
- Driving further industry interest and support for increasing access to improving energy, water and sanitation services through mobile technology.

## Public Policy Considerations

Governments should recognise and support the role mobile can play in improving access to energy, clean water and sanitation in emerging markets. Mobile technologies are increasingly becoming a key strategic element of the models used by Water, Sanitation and Hygiene (WASH) and energy providers to support service delivery.

For example, many energy and water providers employ mobile M2M technology to support the delivery of their services. M2M technologies can be used to monitor water pumps remotely and trigger repair call-outs automatically when a fault occurs, reducing down time. Governments should ensure that taxation levels on M2M connections are set at appropriate rates to encourage these types of innovative solutions.

Equally, several companies offering home solar power kits in emerging markets rely on mobile money to make these kits affordable to low-income populations via pay-as-you-go financing. Governments should ensure supportive regulation is in place to allow mobile money services to thrive and continue to sustainably provide these much-needed affordable financing schemes.

Furthermore, in developing markets, affordability is critical to increasing the use of mobile phones and associated services such as mobile money. Mobile-specific taxes raise barriers to mobile phone ownership and usage. Governments can play a key role by ensuring consumers do not face higher taxes on mobile handsets and services than on other goods and services.

1 Defined by the United Nations as separated faeces from human contact, via latrine, flush or other means.
2 According to the GSMA's 2013 report Sustainable Energy and Water Access Through M2M Connectivity.

Resources:
GSMA Mobile For Development Utilities website
GSMA Mobile for Development Utilities Innovation Fund website
GSMA Connected Society Programme website
GSMA Toolkit: Mobile Money Payment Toolkit for Utilities Providers
GSMA M4D Utilities Annual Report

# Mobile for Humanitarian Innovation

## Background

Mobile networks, and the connectivity they provide, are now seen as a lifeline in humanitarian emergencies because they support critical communication and access to services for humanitarian agencies, affected populations and the international community.

Over the past several years, a proliferation of new coordination and response strategies have been built around mobile platforms and mobile-derived insights.

The impact of the 2017 Caribbean hurricane season — as well as the ongoing global displacement crises, which affect nearly 69 million people around the world[1] — provide recent examples of the critical importance of access to communication and information for populations affected by disaster and crisis.

Humanitarian responses are becoming increasingly reliant on mobile technologies. These include innovations as diverse as connectivity and information access for displaced populations to mobile money-enabled humanitarian cash transfers for communities impacted by disaster. The digital humanitarian ecosystem is also maturing, creating new services, partnerships and business models to support the evolving use of mobile-enabled technologies in these contexts.

Recognising the importance of these developments, 148 mobile network operators have signed up to the GSMA Humanitarian Connectivity Charter, representing networks covering 106 countries. The Charter consists of a set of shared principles adopted by key players in the mobile industry to support improved access to communication and information for those affected by crisis in order to reduce the loss of life and positively contribute to humanitarian response.

The role of mobile in disaster preparedness and response continues to grow, and as the ecosystem becomes more complex, there is a need for a better understanding of how the global mobile communications community can support continued access to communication and information. There is also a need for further understanding of how mobile network data can be used in privacy-friendly ways to derive helpful insights and how the mobile platform can be used as a delivery channel in the wake of humanitarian emergencies. Equally important are efforts among stakeholders to ensure that crisis-affected communities have access to mobile services, including collectively addressing barriers such as the ability to meet know-your-customer (KYC) requirements.

## Programme Goals

The GSMA Mobile for Humanitarian Innovation programme works to accelerate the delivery and impact of digital humanitarian assistance. This will be achieved by building a learning and research agenda to inform the future of digital humanitarian response, catalysing partnerships and innovation for new digital humanitarian services, and advocating for enabling policy environments. The programme also runs an Innovation Fund to help catalyse new mobile-enabled solutions that can benefit those affected by, or responding to, humanitarian crises. The programme is supported by the UK Department for International Development.

## Public Policy Considerations

The GSMA has developed a set of recommendations for governments, regulatory bodies and mobile operators to follow during times of crisis.

The key elements of these recommendations are that governments — along with relevant multilateral agencies — and operators should agree a set of regulatory or policy guidelines that can be adopted to best respond to, and recover from, an emergency and ensure broad access to mobile services for those affected. The guidelines should:

- Set out unambiguous rules and clearly defined lines of communication between all levels of government and operators in emergency situations.
- Provide the flexibility for operators to adjust to unforeseen circumstances rather than insisting that rules designed for non-emergency situations apply no matter what the circumstance.
- Help improve communication and coordination among various government entities involved in responding to an emergency and facilitate a timely and efficient response.
- Clarify what proof-of-identification is acceptable for forcibly displaced persons (FDPs) to access mobile services: this should include forms of identity that most FDPs have access to, for example United Nations High Commission for Refugees (UNHCR)-issued identification.
- Allow some flexibility in the applicability of certain rules at times of emergency, for example enabling lower, tiered thresholds of KYC requirements to allow FDPs to open basic mobile money accounts, particularly in emergency contexts.
- Adopt and promote robust privacy and data protection principles when dealing with people's personal data, particularly in the absence of relevant legal frameworks.

[1] According to the UNHCR's Global Trends Report.

Resources:
GSMA Mobile for Humanitarian Innovation website
GSMA Humanitarian Connectivity Charter website
GSMA Report: Enabling Access to Mobile Services for the Forcibly Displaced: Policy and Regulatory Considerations for Addressing Identity Related Challenges in Humanitarian Contexts
GSMA Report: The State of Mobile Data for Social Good
GSMA Report: Mobile is a Lifeline: Research from Nyarugusu Refugee Camp, Tanzania
GSMA Report: Refugees and Identity: Considerations for Mobile-enabled Registration and Aid Delivery
GSMA Report: Mobile Money, Humanitarian Cash Transfers and Displaced Populations
GSMA Case Study: Italy Earthquake Response and Recovery
GSMA Report: Mission Critical Communications
GSMA Report: The Importance of Mobile for Refugees: A Landscape of New Services and Approaches

# Mobile Health

## Background

Developing countries continue to grapple with low investment in public healthcare, which has a negative effect on access, quality and cost of healthcare services, ultimately leading to poor health outcomes. More than 400 million people do not have access to essential healthcare services, mostly in Africa and South Asia.[1] There is also a significant shortage of health professionals, as staffing levels are below World Health Organization (WHO)-recommended levels in many developing countries.[2]

Mobile's wide reach makes it an ideal tool for strengthening health systems and enabling improved healthcare delivery in countries where there is a large, unmet demand. Many developing nations have over 90 per cent 2G coverage, which allows the delivery of health information services via basic mobile channels such as SMS, Unstructured Supplementary Service Data (USSD) and Interactive Voice Response (IVR). The coverage of 3G networks has also increased to over 80 per cent of the population. As a result, mobile operators have a key role to play as ICT and digital service partners for governments, health providers and health tech companies.

## Programme Goals

The mNutrition Initiative, funded by UK Aid and implemented by the GSMA mHealth programme, aims to boost maternal and newborn child health (MNCH) via mobile solutions that promote the adoption of improved health and nutrition practices. By December 2017, mHealth services under the mNutrition Initiative had reached over 1.59 million users across eight markets in sub-Saharan Africa — Ghana, Malawi, Mozambique, Nigeria, Kenya, Tanzania, Uganda and Zambia.

The programme emphasises supporting partners to develop sustainable, user-centred mHealth services. There are four key areas of focus:

- **Product development:** The GSMA supports product owners with user-centric research, business intelligence analytics and monitoring and evaluation research to inform the product design and optimisation. The research also aims to inform pricing strategies and define the value proposition of the mHealth services to the end-users and other digital health stakeholders as well as potential funders of the solutions.
- **Content development:** The GSMA, with its global content consortium, developed locally tailored, open source nutrition content for each market. Messages were translated into local languages, tested among key target audiences and validated by the Ministry of Health for each market.
- **Industry engagement:** The mHealth programme works closely with health and mobile players across both the public and private sectors to ensure that services not only become commercially sustainable, but also deliver positive public health outcomes.
- **Insights generation:** The GSMA mHealth programme delivers thought-leading publications showcasing best practice and learnings from our work in the digital health sector.

## Public Policy Considerations

Digital health is taking its first steps in some African, Asian and Latin American countries. The number of initiatives is growing, and there is widespread belief that digital health can help address key healthcare issues if it reaches scale.

There are three main areas where digital health can have a significant impact:

**1. Access:** Digital health can widen the reach of healthcare services, as some (such as patient monitoring and diagnostics) can be delivered and managed remotely. It also allows for greater and faster patient access to health information delivered via mobile.

**2. Quality:** Digital health enables faster and more effective coordination of care and health professionals, and supports timely data sharing.

**3. Cost:** The transition from paper to digital ensures that available health resources are used effectively where and when they are needed the most. Mobile networks can also be a platform for solutions that strengthen monitoring systems and help prevent the spread of infectious diseases.

Unfortunately, few digital health and mobile health pilots are currently followed by full-scale implementation due to a lack of sustainable financing. In developing countries, venture capital activity is limited and private sector healthcare provision is underdeveloped. As a result, government is likely to be the largest funder of digital health initiatives in these nations.

Governments can play a key role in the development and success of the solutions by providing more stable government investment to help drive scale. Ministries of Health can also encourage the implementation of national digital health plans by aligning them with ICT and broadband plans. Key enablers include setting outcome-based objectives to drive execution and track progress; and policy and regulation that promote investment for digital health solutions.

At the same time, digital health stakeholders need to stimulate government investment by demonstrating how digital health solutions help address national healthcare issues, especially in terms of broadening access, which is a key challenge for emerging nations.

[1] According to the World Health Organization's 2015 report Tracking Universal Health Coverage.

[2] The WHO's critical threshold is 23 doctors, nurses and midwives per 10,000 inhabitants.

Resources:
GSMA Report: Creating Mobile Health Solutions for Behaviour Change
GSMA Report: Scaling Digital Health in Developing Markets
GSMA Report: mHealth Design Toolkit
GSMA Report: Mezzanine's Stock Visibility Solution
GSMA Report: Living Goods Uganda
GSMA Report: Kilkari: A Maternal and Child Health Service in India

# Mobile Money

## Background

Mobile money has done more to extend the reach of financial services in the last decade than bricks-and-mortar banking has in the last century. This has been possible because mobile money leverages the ubiquity of mobile phones, along with the extensive coverage of mobile operators' networks and retail distribution channels, to offer customers a more secure and convenient way to access, send, receive and store funds.

As a result, mobile money has transformed the financial services landscape in many developing markets, by both complementing and disrupting traditional bricks-and-mortar banking. Mobile money platforms now process more than $1 billion a day and over 168 million additional accounts became active during 2017. As a result, the number of registered customer accounts rose from 554 million in 2016 to reach 690 million by December 2017.

Globally, the percentage of providers who offer mobile money services through a smartphone app has increased from 56 per cent in 2015 to 73 per cent as of June 2017. Market figures clearly support the fact that mobile money is expanding financial inclusion. Services are now available in 85 per cent of countries where the vast majority of the population lacks access to a formal financial institution, while in 19 markets there are more mobile money accounts than bank accounts.

Furthermore, the mobile money industry has proven to be both viable and sustainable: as of 2017, there were 276 services in 90 countries.

## Programme Goals

According to the World Bank's Findex database, about 1.7 billion people remain unbanked, without access to safe, secure and affordable financial services. The GSMA Mobile Money programme helps mobile operators and industry stakeholders enhance the utility and sustainability of mobile money services to increase financial inclusion for these people.

The programme is working to develop a robust, highly-interconnected mobile money ecosystem where transactions are digitised for sectors including retail, utilities, health, education, agriculture and transport. Diversifying mobile money customer usage patterns to go beyond merchant payments and draw in transactions such as cross-border remittances and bulk disbursements can accelerate network effects and broaden the payments ecosystem.

To truly transform the financial lives of underserved people, mobile money must become a central monetisation mechanism that can be used to carry out a diverse range of digital transactions. Making mobile money more central to the financial lives of users can help achieve greater financial inclusion, economic empowerment and economic growth.

## Public Policy Considerations

Regulation has a major impact on the uptake of mobile money services. Evidence from the Findex and GSMA studies shows that enabling regulatory frameworks accelerates the development and adoption of digital financial services.

When banks and non-bank providers, especially mobile operators, are allowed to deploy mobile money services and establish partnerships that make commercial sense, mobile money can be a catalyst for financial sector development. It significantly expands financial inclusion through lower transaction costs, improved rural access and greater customer convenience. It can also provide the infrastructure to support a broad range of financial services including insurance, savings and loans.

There is a strong opportunity for mobile money providers to analyse personal data to develop innovative services for consumers and ensure the long-term sustainability of the industry. Appropriate data privacy frameworks will be critical to safeguard consumers' personal data and promote trust. Enabling frameworks that support cross-border data flows, while protecting personal data, will also become increasingly important to the growth of the industry.

Mobile money can also help governments achieve their policy objectives of safe, secure and efficient payment systems. It also reduces the vulnerability of a country's financial system by lowering the risks caused by the informal economy and widespread use of cash. For example, it helps to bring more people from the informal to the formal economy, which means that governments can increase transparency and make more informed economic policy decisions.

Governmental bodies can also benefit in multiple ways from using mobile money for government-to-person (G2P) and person-to-government (P2G) transactions. These include lower cash-handling costs, reduced security risks, minimal theft of funds, increased transparency, instant transfers and improved operational efficiencies.

For mobile money to succeed, a level playing field must be established via an enabling policy and regulatory framework that allows non-bank mobile money providers to enter the market.
Regulators should:

- Embrace reforms to enable operators to launch and scale mobile money services.
- Allow market players to determine the timing, technical model and commercial model for all forms of interoperability.
- Allow market-led solutions to be implemented at the right time for consumers and providers.

It is also important that governments refrain from imposing discriminatory taxes that target mobile money customers, as these types of taxes are likely to increase consumer costs and generate a headwind against this promising, socially beneficial service.

Resources:
GSMA Mobile Money Programme website
GSMA Mobile Money Regulatory Guide website
GSMA Report: 2016 State of the Industry — Mobile Money

# GSMA Capacity Building

The GSMA Capacity Building programme offers an extensive range of free training courses for policymakers and regulators. Since its launch in 2013, it has rapidly established itself as the world's premier provider of specialist telecoms regulatory training. With over 70,000 hours of training delivered to regulatory professionals from over 150 countries around the world, it has already achieved unparalleled scale and reach.

Our courses help students understand and keep track of the latest policy and regulatory developments around the world. By zooming in on real-world examples of regulatory good practice from different regions, they walk students through the implications of various policy and regulatory approaches and the impact these have on the delivery of mobile services in their country. Core areas covered include spectrum, competition policy, rural coverage, as well as emerging topics such as 5G and how to leverage mobile technology to help governments achieve their Sustainable Development Goals (SDGs) targets.

Our in-house policy experts, who develop and teach our courses, come from a wide range of backgrounds within telecoms, law and financial services and many hold advanced academic qualifications. Through their work with the GSMA, they are in constant contact with governments and regulatory authorities around the world. As a result, they have a unique understanding of the most pressing issues facing regulatory authorities today.

Our courses further benefit from the support of the GSMA's own research arm, GSMA Intelligence, which draws on the expertise of a global team of researchers, forecasters and analysts. This input helps ensure our courses are packed full of the latest, robust market statistics, analysis and insights. Our training materials are also accredited by the United Kingdom Telecommunications Academy.

The combination of engaging and interactive courses, expert trainers and in-depth research and analysis, make our programme a leader in training and professional development for policymakers and regulators across telecommunications and related areas. Ultimately, our goal is to help policymakers and regulators positively shape the development and reach of mobile services in their country, ensuring these services deliver the most benefit to citizens.

Our courses are offered in English, French and Spanish, and are suitable for professionals at any stage of their career. Available both as face-to-face and online training, they provide policymakers and regulators with maximum flexibility in how they study.

Our face-to-face courses are between one and three days long, while our online courses last between three and six weeks.

To learn more about our training or to register for a course visit:

**www.gsmatraining.com**

## Courses

- 5G — The Path to the Next Generation
- Advanced Spectrum Management for Mobile Telecommunications
- Bridging the Mobile Gender Gap
- Children and Mobile Technology
- Competition Policy in the Digital Age
- Digital Identity for the Underserved
- Internet of Things
- Leveraging Mobile to Achieve SDG Targets
- Mobile Money for Financial Inclusion
- Mobile Sector Taxation
- Mobile Technology, the Environment and Climate Change
- Principles of Mobile Privacy
- Radio Signals and Health
- Responding to Disasters and Humanitarian Crises
- Unlocking Rural Mobile Coverage

## How We Deliver Our Training

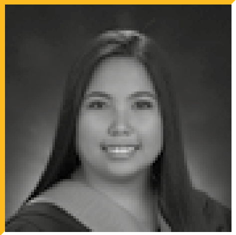
**On-Site**
If your organisation or department has a sufficiently large number of staff that could benefit from our training, we can deliver our courses on-site. This allows your employees to receive their training at the same place where they practice their skills and reduces or eliminates travel and accommodation expenses.

**Online**
All of our courses are available via our online portal, placing students in control of their own learning. Using this platform, students are able to study our courses anywhere in the world, progressing at their own pace and scheduling coursework around work and family life.

**Via local partners**
The GSMA also delivers its courses through a range of strategic partnerships with academic institutions, development organisations, regulatory bodies and training specialists. This ensures we have the flexibility to deliver courses at a location near you.

**"The [Internet of Things] seminar was very well attended by more than 50 senior level officers from DoT, BSNL, MTNL and CDOT. It was well appreciated by the participants in terms of content as well as delivery… the speakers' depth of understanding of the subject, and their ability to present the subject in an interesting way were key factors in meeting the objects of the seminar… we look forward to conducting many more such seminars on topics related to the latest telecoms technologies in collaboration with GSMA."**

Dr. Rajesh Sharma, Deputy Director General, Department of Telecommunications, Ministry of Communications, India



## Anna Teresa Aguilar

Planning Officer, Department of Information and Communication Technology, The Philippines

**What made you want to take your first GSMA Capacity Building course?**

After one of my colleagues finished a course, and then took another, I was determined that I would also take my first course and fit it around my tasks here at the office. Also, I find that taking the courses offered by the GSMA is a great way to refresh my knowledge and skills as an Electronics and Communications Engineer. They also help me to contribute to our team as we develop policies.

**What do you enjoy most about the courses?**

I really enjoy taking part in the different online chat sessions where I can ask the mentor questions about the topic, especially those that I have trouble understanding. Also, using the forum in the online portal, I can exchange ideas and learn from my classmates on the course. I find it interesting when they share information about things they are already implementing in their country.

**How have you used what you have learned during the courses?**

I used my learning from the courses as support for the technical research I have conducted while formulating different ICT policies.

**Can you give an example of how what you have learned relates to issues affecting the mobile telecommunications sector in your country?**

Telcos are having difficulty putting up base stations in subdivisions because some people fear that mobile radiation may pose a health hazard to humans, but as I learned in my first GSMA course, Radio Signals and Health, there are no significant effects on humans.

**What would you say to a regulator or policymaker that was thinking about taking a course with us?**

I would recommend that they go ahead with their plans to take courses with GSMA because the knowledge they will gain from the courses will help them perform effectively in their role.

## Glennert Riedel

Technical Affairs Officer, Bureau Telecommunicatie & Post (BT&P), Curaçao

**How did you find out about the GSMA's online courses?**

I saw the courses online and subscribed after my colleague recommended the Advanced Spectrum Management course.

**What made you want to take your first course?**

I wanted to gain more information about the mobile side of spectrum management as we needed to plan spectrum allocations, and the course was exactly what I was looking for. It was useful for my daily work and I was able to put what I had learned from the course into use.

**What did you like most about the experience?**

I was pushed to get involved and be active in the course. For some courses, all you do is listen, but you have to be proactive on GSMA Capacity Building courses. The dedication of the GSMA team pushed the course forward. I also liked having context and in-depth answers to the topics at hand.

**Were there any challenges you experienced while taking this course online?**

I had to get used to the accents! The course is also intensive, so I had to manage my time between my work and the course.

**Can you give an example of how what you have learned relates to issues affecting the mobile telecommunications sector in your country?**

I used the knowledge gained on the course to help prepare for conferences (I used my knowledge at a conference in Cuba, for example) and other aspects of my work, including planning spectrum allocations.

**What would you say to a regulator or policymaker that was thinking of taking a course with GSMA Capacity Building?**

Definitely take the course, it is time well spent. You learn more about the context, meet more people in the field, and understand the challenges other countries are facing. Thank you to the GSMA team for delivering these courses as it is an effective way to learn, especially for smaller countries that do not have the same access to industry knowledge.

# Mobile Initiatives

Innovation and investment by the mobile industry continue to have an enormous impact on the lives of billions of people around the world. Mobile doesn't just deliver connectivity, it empowers people through an ever-growing range of mobile-enabled services.

Currently there are over five billion unique mobile subscribers globally, which means that more than two-thirds of the global population is now connected to a mobile service. By the end of the decade, almost three-quarters of the global population will have a mobile subscription, with around one billion subscribers added over this period.

The GSMA leads several programmes in key growth areas that present significant benefits for consumers and clear opportunities for mobile operators. From supporting the development of mobile identity solutions to helping operators prepare for a 5G future, these initiatives are laying the foundations of an increasingly connected, mobile world.

Each of the initiatives covered on the following pages has its own public policy considerations and relates to one or more of the public policy topics presented in this handbook.

# Future Networks

The mobile industry is currently laying the groundwork for the transition to fifth generation (5G) technology. Building on the achievements of 4G, future 5G networks will help the mobile industry capture the huge opportunity presented by the Internet of Things (IoT), usher in an era of even faster mobile broadband and pave the way for ultra-reliable, ultra-low latency services, which may include exciting technologies such as tactile internet, augmented reality and driverless cars.

As operators begin to launch 5G networks, there is a need for close collaboration between industry, policymakers and regulators to deliver on the promise of this next-generation technology.

The GSMA is playing its part via its Future Networks programme. It provides guidance on key innovations such as network slicing in 5G, while also working to boost population coverage of high-speed broadband and reduce the capital intensity required for the rollout of 5G technology. The programme's work on infrastructure sharing and improvements to radio networks, for example, has already helped to identify a potential four per cent reduction in the capital intensity requirements for 5G. These reductions will be vital in helping the industry achieve its target of making 5G available to a third of the world's population by 2025.

Governments and regulators also have a crucial role to play. By adopting national policy measures that encourage long-term, heavy investments in 5G networks and by making sure sufficient harmonised spectrum is made available for 5G services, they can ensure future 5G infrastructure delivers significant benefits for their citizens. The decisions being made now will have long lasting impacts for the future and the technology's ultimate success will depend on governments and regulators prioritising its rollout.

In tandem with their exploration of 5G technologies, network operators are also continuing to upgrade their existing networks and transition to all-IP based services. This is important, not just to ensure consumers and business can gain the maximum benefit from today's advanced services, but also because IP-based networks and services will ultimately act as the launch pad for 5G services.

# 5G — The Path to the Next Generation

## Background

Mobile telecommunication has had a phenomenal and transformational impact on society. Starting from the earliest days of first-generation analogue phones, every subsequent generational leap has brought huge benefits to societies around the world and propelled the ongoing digitisation of more and more segments of the global economy. The mobile industry is now preparing to embark on the transition to fifth generation (5G) technology, which will build on the achievements of 4G while also creating new opportunities for innovation.

A range of industry, research, academic and government groups across the globe are working to define the technology for 5G. The next generation mobile technology will need to provide higher throughput, lower latency and higher spectrum efficiency.

Between now and 2020, the year when 5G is expected to become commercially available, the mobile industry will continue to take steps towards achieving these goals by evolving existing 4G networks. Despite these enhancements to 4G, there is still a need for 5G to meet the demands of future services and platforms. By 2025, 5G could account for over one billion connections and 5G networks are likely to cover one third of the world's population. The impact on the mobile industry and its customers will be profound.

But 5G is more than a new generation of technologies: it will usher in a new era in which connectivity will become increasingly fluid and flexible, as 5G networks will adapt to applications and performance will be tailored precisely to the needs of the user.

Currently, there are three key areas of focus for 5G development and innovation:

**Internet of Things (IoT).** There is a need for 5G to capture the huge opportunity presented by IoT. Conservative estimates suggest that by 2025 the number of IoT devices will be more than double the number of personal communication devices. As the ecosystem grows, the mobile industry will be expected to support bespoke services across industry verticals and develop next-generation services that are not achievable with 4G networks.

**Mobile broadband.** With each generational leap in mobile technology there is a natural progression to faster and higher-capacity broadband. Mobile broadband services using 5G technology will need to meet and exceed customers' expectations of faster and more reliable access.

**Ultra-reliable, ultra-low latency services.** Superior speed, very high reliability and reduced latency will see 5G nurture new services that cannot be supported on existing 4G networks. Some of the services being considered include tactile internet, virtual/augmented reality, driverless cars and factory automation.

The GSMA aims to play a significant role in helping to shape the strategic, commercial and regulatory development of the 5G ecosystem, including areas such as the identification and alignment of suitable spectrum bands.

Working closely with the mobile operators pioneering 5G, the GSMA is also engaging with governments and vertical industries (such as the automotive, financial services, healthcare, transport and utilities sectors) to develop business cases for 5G.

## Public Policy Considerations

The GSMA regards 5G as a set of requirements for future mobile networks that could dramatically improve the delivery of mobile services and support a variety of new applications. The mobile industry, academic institutions and national governments are currently actively investigating what technologies could be used in 5G networks and the types of applications these could and should support. The speed and reach of 5G services will be heavily dependent on access to the right amount and type of spectrum.

Additional new spectrum will be required for 5G services, especially in very high frequency bands, in order to support significantly faster data speeds and deliver enhanced capabilities. However, progressive refarming of existing mobile bands should also be encouraged to support wider area 5G services. Governments and regulators can enable refarming and encourage heavy investment in 5G networks by supporting long-term technology neutral mobile spectrum licences with clear renewal procedures.

The GSMA believes that three key frequency ranges are needed for 5G to deliver widespread coverage and support all use cases: sub-1 GHz, 1-6 GHz and above 6 GHz. Higher frequencies — especially above 24 GHz — will be needed to support superfast speeds in hotspots. Governments will need to support these new higher frequency mobile bands at the World Radiocommunication Conference taking place from October to November 2019. Lower frequencies will be needed to support wider area broadband access and IoT services. Exclusive licensing remains the principal and preferred regime for managing mobile broadband spectrum in order to guarantee quality of service and network investment. However, the licensing regime in higher frequency bands, such as above 6 GHz, could be more varied than in previous mobile technology generations, to suit more flexible sharing arrangements.

Resources:
GSMA 5G website
GSMA Blog: Five Things to Know About 5G
GSMA Report: The 5G Era: Age of Boundless Connectivity and Intelligent Automation
GSMA Report: 5G in China: Outlook and Regional Perspectives
GSMA Report: Smart 5G Networks: Enabled by Network Slicing and Tailored to Customers' Needs
GSMA Public Policy Position: 5G Spectrum

# IP Communication Services

## Background

IP communication is increasingly recognised as a natural evolution of core mobile services, and therefore a basic requirement of doing business in the future. The IP Multimedia Subsystem (IMS) has emerged as the preferred technical means for transferring core mobile operator services to an all-IP environment because of its flexibility, cost-effectiveness and support for IP services over any access medium. With 670 mobile network operators having launched Long Term Evolution (LTE) networks, and LTE coverage currently reaching just under 80 per cent of the world's population, the industry is now in a realistic position to make a global, interconnected IP communications network a reality. IP communications is comprised of Voice over LTE (VoLTE), Video over LTE (ViLTE), Voice over WiFi (VoWiFi) and Rich Communication Services (RCS).

- **VoLTE.** This offers an evolutionary path from circuit-switched 2G and 3G voice services to all-IP packet-switched voice and includes a range of enhanced features for customers, such as high-definition audio quality and shorter call connection times. As of July 2018, 145 operators offer voice over LTE services commercially in 69 countries.
- **ViLTE.** This enables operators to deploy a commercially viable, carrier-grade, person-to-person video-calling service. Like VoLTE, it is based on IP Multimedia Subsystem (IMS) technology.
- **VoWiFi.** This allows operators to offer voice calling over WiFi, providing many of the same benefits of VoLTE. As of July 2018, there were 61 VoWiFi services commercially available in 35 countries.
- **RCS.** This marks the transition of messaging from circuit-switched technology to an all-IP world, leveraging the same IMS capabilities as VoLTE and ViLTE. RCS incorporates messaging, video sharing and file sharing, enriching the communication experience of consumers. As of July 2018, RCS was being offered by 55 mobile operators in 34 countries.

The GSMA, via its Future Networks programme, is working with leading operators and equipment vendors to accelerate the launch of IP-based services around the world. The work of the Future Networks programme covers the development of specifications, assisting operators with the technical and commercial preparations for service launches and resolving technical and logistical barriers to interconnect.

## Public Policy Considerations

To support the exponential growth in IP traffic, large-scale investments in network capacity are required. Financing such investments depends on predictability and the existence of a stable regulatory environment. Where such an environment exists, future communications capabilities that are operator-led can be well aligned with the regulatory requirements related to mobile telecommunications, and mobile network operators have the systems in place to ensure compliance.

**Open standards.** VoLTE, ViLTE, VoWiFi and RCS are currently specified, through a process of industry collaboration, as industry standards for IP-based calling, messaging, file and video-sharing services, based on IMS technology.

**Interconnect.** VoLTE, ViLTE, VoWiFi and RCS support interconnection of these services between customers on different mobile networks. In the case of voice, they also support interconnection with customers on fixed networks.

**Lawful intercept.** Mobile network operators are subject to a range of laws and licence conditions that require them to be capable of intercepting customer communications (and sometimes also retaining certain data, such as the time and content of the communication, as well as the location, numbers or IP addresses of the participants) for disclosure to law enforcement agencies upon request. The specifications for IP communications are being developed so they support the capabilities needed to meet lawful interception obligations.

Resources:
GSMA Report: Building the Case for an IP-Communications Future
GSMA All-IP Business Guide website
Greenwich Consulting Report: The Value of Reach in an IP World

# Voice over Long Term Evolution

## Background

Consumers expect seamless carrier-grade voice services from mobile operators, irrespective of the type of technology used.

Since the introduction of digital mobile technologies in the early 1990s, carrier-grade public mobile voice services have been delivered via the circuit-switched capabilities of 2G and 3G networks.

To keep pace with growing demand, mobile operators are now upgrading their networks using a fourth-generation IP-based technology called Long Term Evolution (LTE). LTE networks support a new carrier-grade voice capability called Voice over LTE (VoLTE) that offers an evolutionary path from circuit-switched 2G and 3G voice services. VoLTE includes a range of enhanced features for customers, such as high-definition audio quality and shorter call connection times.

Some operators now have LTE networks that offer full national coverage and are using VoLTE for voice calls. Other operators still only have partial LTE network coverage.

In most markets, achieving full LTE coverage will take a number of years, thus requiring partial reliance on legacy voice services. For voice services, the transition is facilitated by the fact that VoLTE has been designed to support the seamless handover of calls to and from 2G and 3G networks.

VoLTE has a number of characteristics that distinguish it from internet-based voice services. These include carrier-grade call quality and reliability, support for emergency calls, and universal interconnection with other 'carrier-operated' voice services across the globe. By contrast, the majority of internet-based voice services are not managed for service quality and may be restricted to closed user groups.

In some jurisdictions, interconnection of carrier-grade mobile voice services is unregulated and carried out pursuant to a range of different commercial agreements. In other jurisdictions, regulated mobile call termination rates apply. These rates typically use a time-based charging mechanism and their levels are set using a number of different cost-oriented methodologies.

## Public Policy Considerations

Voice over Long Term Evolution (VoLTE) is a carrier-grade mobile voice service, making it distinct from other internet-based voice services.

Carrier-grade mobile voice services have a number of specific characteristics. For example, the use of mobile phone numbers from national numbering schemes means that customers can make calls to, or receive calls from, any other phone number in the world. Carrier-grade mobile voice services also use dedicated network capabilities (technically known as bearers) to assure end-to-end service quality and reliability.

VoLTE is an evolution of carrier-grade mobile voice services that have historically been provided using the circuit-switched assets of 2G and 3G networks. As such, regulators should not apply additional, or specific, regulations to VoLTE services.

In markets where mobile voice call termination is subject to regulatory control, the same approach should be adopted for VoLTE, with a single rate applied across 2G, 3G and 4G/LTE voice call termination.

Resources:
GSMA Future Networks — Voice over LTE website
ECN Magazine: VoLTE — What Makes Voice over IP 'Carrier-grade'?

# Internet of Things

The Internet of Things (IoT) is set to have a huge impact on our daily lives, helping us to reduce traffic congestion, improve care for the elderly, create smarter homes and offices, increase manufacturing efficiency and more.

IoT involves connecting devices to the internet across multiple networks to allow them to communicate with us, applications and each other. It will add intelligence to devices that we make use of on a daily basis and in turn deliver positive impacts to both the economy and broader society.

We are set to see rapid growth in IoT over the coming years. According to GSMA Intelligence, the number of licensed cellular IoT connections is expected to exceed three billion by 2025. However, this will still represent a small portion of the overall market, as the total number of IoT devices will have grown to 25.2 billion by 2025.

The GSMA, through its IoT programme, is encouraging the development of the nascent IoT ecosystem by working to define industry standards, promote interoperability and encourage governments to create a supportive environment that will speed the growth of IoT globally.

# Connected Drones (UAVs)

## Background

The development of Unmanned Aerial Vehicles (UAVs), commonly called drones, has advanced at a rapid pace in recent years. Military use was the early focus of these developments, but the potential for drones to be used within a civilian context for innovation in both new and existing services is now widely recognised.

Use cases range from filming for news reporting and entertainment, to inspecting key infrastructure such as power plants, roads, buildings, cell towers and power lines. In agriculture, drones are already being used to produce timely crop surveys to help boost yields.

The rapid development of this market means regulators are struggling to keep pace. However, regulatory efforts are now focused on the creation of frameworks that will allow the sector to continue to develop and innovate, but at the same time limit risks related to safety, privacy and data protection. The fact that drones fly across borders adds an additional layer of complexity to these efforts.

Mobile operators are a key enabler for drones, helping to unlock their potential. By providing the connection between drones and their control centres they ensure reliable communication with the drone on its flight path and support the transfer of data between the drone and its control centre.

## Public Policy Considerations

New regulatory frameworks for drones should ensure that they can, where required, be equipped with SIM cards and a communications modem so the drone ecosystem can benefit from mobile connectivity.

This would deliver many benefits to the drone industry:

- Mobile networks provide a global, interoperable and scalable platform that allows the drone market to develop and benefit from the existing mobile ecosystem.
- Many mobile operators already run 4G LTE networks which meet very high-bandwidth, low-latency requirements, while at the same time offering huge scalability and exceptional quality of service.
- The mobile industry already works collaboratively with Internet of Things (IoT) partners throughout the value chain to embed privacy and security into IoT technologies. As a result, the drone market can benefit from existing initiatives such as the GSMA's Security Guidelines and Privacy by Design Toolkit.

Mobile connectivity can help establish the controlled and safe operation of drones by ensuring secure, high-quality connectivity between drones and their control centres. This connectivity delivers a number of capabilities that can benefit the drone ecosystem:

- Mobile connectivity can form part of unmanned traffic management solutions and enable no-fly zones.
- A mobile-based solution could be an effective way to enable drone identification and authorisation services, as identity verification and management is already a key component of mobile services.
- Mobile connectivity can assist law enforcement by enabling identification and tracking of drones.
- The mobile industry has a strong track record of implementing privacy and data protection measures.

In order to ensure existing licensed mobile spectrum is available for drone connectivity, regulatory authorities responsible for spectrum and regulators responsible for drones need to cooperate to remove barriers that could hinder the use of existing licensed mobile spectrum for drone connectivity.

Resources:
GSMA Internet of Things — Drones website

# Connected Vehicles

## Background

The automotive world is about to undergo the single greatest revolution since its inception. Autonomous vehicles and Intelligent Transport Systems (ITS) are set to transform the efficiency, comfort, safety and environmental impact of road transport.

The first fully autonomous-capable cars have been launched and according to data from Machina Research the number of factory-fit connected vehicles worldwide is expected to reach 366 million by 2025. In Europe, eCall regulation means that, as of March 2018, all new models must now support eCall. In the event of an accident, an eCall-equipped vehicle automatically calls the nearest emergency centre and sends the exact location of the crash site, allowing for a rapid response by emergency services.

Through its IoT programme, the GSMA is actively engaging with vehicle manufacturers, mobile network operators, SIM vendors, module makers and the wider Cooperative Intelligent Transport System (C-ITS) ecosystem to facilitate the development of current and future connected-vehicle solutions.

The primary platform for these activities is the Connected Vehicle Forum. Established by the GSMA, it promotes dialogue across all stakeholders in the automotive and C-ITS ecosystem and looks to find innovative ways mobile technology can be leveraged by these sectors.

One example of this is remote provisioning of the GSMA's Embedded SIM Specification. This provides a single mechanism for the remote provisioning and management of machine-to-machine (M2M) connections, allowing 'over-the-air' provisioning of an initial operator subscription, as well as subsequent changes of subscription from one operator to another.

Mobile technology is also set to play a vital role in ITS by providing Cellular Vehicle-to-Everything (C-V2X) services. Standardised by 3GPP, C-V2X supports connectivity between devices (whether in vehicles, roadside infrastructure or mobile devices) as well as between devices and networks. C-V2X is being developed within the traditional mobile ecosystem and brings all the advantages and capabilities that traditional cellular networks offer: security, privacy, interoperability as well as an innovation-oriented and future-proofed ecosystem (5G technology). The 5G Automotive Association (5GAA) — whose 60 members include the main vehicle manufacturers — support C-V2X.

## Public Policy Considerations

Connected vehicle and intelligent transport applications have the potential to bring substantial benefits to consumers, including making travel safer, reducing congestion and providing real-time information to passengers.

Connected vehicle applications and services have a number of distinctive features. They need to operate globally, support very long 'device' lifetimes, integrate with local intelligent transport solutions and comply with local security, data protection, privacy and emergency regulations.

Policymakers and regulators must appreciate and understand these differences if they are to implement policies that allow global business models to develop and ensure that those rules apply consistently to all players in the value chain.

As ever more cars become connected, spectrum policy related to intelligent transport systems will become increasingly important in the future. In many countries around the world regulators have set aside a portion of spectrum for ITS, typically in the 5.9 GHz band. This generally includes a dedicated portion for safety-related communications between vehicles, infrastructure and people.

Regulators should adopt a technology-neutral approach to this spectrum, rather than mandating or preferring one approach. Equally, it is important that technology-neutral spectrum licences are adopted as this will allow existing mobile bands to be refarmed for 5G, enabling lower-latency connectivity, and thus improved response times for emergencies.

Furthermore, spectrum in the 3.4-3.8 GHz range should not be set aside for safety-based vehicle-to-vehicle communications, as this spectrum is critical for future commercial 5G services in many countries around the world. This also highlights the need for regulators to work with the mobile industry to support connected vehicles in future spectrum planning. For example, it is essential that sufficient spectrum below 6 GHz is made available as this spectrum travels further and is better suited to the wide-area connectivity required by connected cars.

Resources:
GSMA Report: Safer and Smarter Driving — The Rollout of Cellular V2X Services in Europe
GSMA Report: Cellular Vehicle-To-Everything (C-V2X) — Enabling Intelligent Transport
GSMA Report: Automotive IoT Security: Countering the Most Common Forms of Attack
GSMA Report: Mobilizing Intelligent Transportation Systems
GSMA Transforming the Connected Car Market website
GSMA Case Study: EE Brings Safer Driving to the UK's Roads

# Privacy and Data Protection for IoT

## Background

The Internet of Things (IoT) offers significant opportunities and potential for data-driven innovation to achieve economic, social and public policy objectives, and ultimately improve people's daily lives. For example, the IoT will enable a raft of new applications and services that will empower consumers to monitor their health, manage their energy consumption and generally benefit from smart home and city solutions. These applications have the potential to drive a range of positive outcomes, including improved traffic management, lower pollution levels and healthier lifestyles.

Many IoT services will be designed to create, collect or share data. Some of this data (e.g., data about the physical state of machines or weather conditions) may not impact on consumers' privacy and as a result won't be considered personal data.

However, IoT services aimed at consumers are likely to involve the generation, distribution and use of detailed data about those consumers. For example, a smart home appliance may use data about a person's eating or exercise habits to draw inferences about that person's health and steer them towards healthier lifestyles, or develop a profile based on their shopping habits to offer them personalised money-off vouchers.

These types of IoT services and devices have the potential to impact people's privacy and may be subject to general data protection and privacy laws. Where IoT services are provided by mobile operators they will also be subject to telecommunications-specific privacy and security rules. Nevertheless, as consumer IoT services gain in popularity, more consumer data will be created, analysed in real time and shared between multiple parties across national borders. Therefore, companies throughout the IoT ecosystem have a responsibility to build trust among consumers by ensuring their privacy is respected.

## Public Policy Considerations

To realise the opportunities that the IoT offers, it is important for consumers to trust the companies who are delivering IoT services and collecting the data generated by them. The mobile industry's view is that consumer confidence and trust can only be fully achieved when users feel their privacy is appropriately respected and protected.

There are already well-established data protection and privacy laws around the world. Where these data protection regulations and principles exist, they can also be applied to address privacy needs in the context of IoT services and technologies. It is vital that governments apply these frameworks in ways that promote self-regulation and encourage the adoption of risk management-based approaches to privacy and data protection.

Most importantly, protections should be practical, proportionate, and designed into IoT services (privacy by design) to encourage business practices that provide transparency, choice and control for individuals.

IoT services are typically global in nature and a mobile operator is often only one of many parties in a delivery chain that may include a host of others, such as device manufacturers, search engines, online platforms and even the public sector. Therefore, it is key that privacy and data protection regulations apply consistently across all IoT providers in a service- and technology-neutral manner. This will help ensure a level playing field for all industry players so they can focus on building trust and confidence for end users.

Resources:
GSMA Report: The Impact of the Internet of Things
GSMA Report: Safety, Privacy and Security Across the Mobile Ecosystem
GSMA Report: Privacy Design Guidelines for Mobile Application Development
GSMA News: U.S. Senate Subcommittee — Respect for Privacy Vital for Growth of the IoT

# Smart Cities and IoT

## Background

The world's population is increasingly concentrated in cities, with more than half now living in urban areas, according to data from the World Health Organization (WHO). This trend is set to continue, as the WHO forecasts that the global urban population will grow approximately 1.63 per cent per year between 2020 and 2025 and 1.44 per cent per year between 2025 and 2030. This will put additional stress on city infrastructure and services through increased congestion, pollution and higher costs of living. The infrastructure of today's cities is typically not designed to deal with continued increases in population densities. As a result, it is very difficult to redesign existing cities in most parts of the world to cope.

This is why national and local governments are increasingly interested in developing smart cities that use mobile communications technology and the Internet of Things (IoT) to solve many of the challenges cities face today. For example, smart city technology can to tackle traffic congestion, improve public transport infrastructure, create safer streets with better lighting, and add intelligence to utilities infrastructure via smart meters and smart grid solutions. It also opens up new commercial and investment opportunities for cities.

Mobile operators are at the heart of this change, offering solutions based on mobile IoT networks that are specifically designed to serve these ambitions. By supporting low-cost, connected devices that offer long battery life and can be rolled out at huge scale, mobile operators are able to serve the next generation of cities and offer solutions that make it easier to add connectivity and control to critical infrastructure.

## Public Policy Considerations

Policymakers and regulators looking to foster an environment that encourages investment in smart cities should:

- **Adopt an agile institutional framework and governance mechanisms.** A smart city needs an institutional framework that ensures coordination and support throughout the lifetime of each project. The smart city agency will have to be agile and, ideally, independent from traditional city departments. It should, however, be accountable to a governance body on which the city institutions are represented.

- **Appoint a chief information officer (CIO) or smart city director with strategic vision.** A strong vision and strategy is key to the success of smart city projects. A CIO or smart city director should be a project leader with cross-functional skills, capable of defining a long-term strategy.

- **Communicate effectively the objectives and benefits of smart city projects.** Establishing a dialogue with the local community is an essential step to ensure the design and functionality of effective smart city services. Digital media can help involve citizens in each step of the service lifetime and highlight tangible benefits that a smart city project will deliver.

- **Promote technology investment in open and scalable systems.** A smart city should avoid relying on proprietary technologies tied to a single provider. Standards-based solutions are an essential foundation for the long-term evolution of a smart city.

- **Comply with privacy and security best practice, rather than defining new service-specific rules.** To safeguard privacy and security, smart cities need to draw on industry best practice and comply with national laws. Local city managers should resist the temptation to define their own data privacy and security standards for services they launch and adopt in their own city.

- **Make city data available to promote transparency and stimulate innovation.** While protecting individuals' privacy, city managers should look to make data accessible to promote transparency and stimulate the creation of innovative services. Some cities already have portals that make data available in accessible formats.

- **Explore new models of funding.** Smart city projects require significant initial investment. Smart city managers should explore public-private partnerships or alternative finance mechanisms, such as municipal bonds, development banks or vendor finance. IoT technologies and smart city applications can generate substantial socio-economic benefits for citizens and businesses. Policymakers should make the most of this opportunity, by designing and implementing smart city projects with a long-term vision, that are defined around citizens' needs, are managed through agile governance structures, are based on open and scalable systems and promote a culture of openness, innovation and transparency.

Resources:
GSMA Smart Cities website
GSMA IoT Knowledgebase: Smart Cities
GSMA Report: Maximising the Smart Cities Opportunity — Recommendations for Asia-Pacific Policymakers
GSMA Report: Keys to the Smart City
GSMA Video Case Study: Smart City Tainan

# Identity

Digital content, services and interactions have become a part of daily life for billions of people, driven by expanding access to broadband and increasingly affordable mobile devices. The use of data and user authentication are requisite elements of being online. As a result, it is becoming increasingly important that users have a digital identity to be able to securely authenticate themselves online in order to carry out tasks such as accessing their accounts and subscriptions or making purchases.

The digital economy is predicated on trust. Interactions — whether they be social, commercial, financial or intellectual — require a proportionate level of trust in the other party or parties involved. Today consumers are seeking secure and seamless access to digital services, while safeguarding their privacy. As a result, online service providers must reduce friction in digital transactions, while still maintaining a seamless, secure user experience. Increasingly, governments are regulating for and demanding electronic identity solutions that leverage global standards to ensure interoperability, privacy, scale and cost effectiveness.

To this end, the mobile industry is developing a consistent and standardised set of services for managing digital identity, putting mobile at the heart of the digital identity management ecosystem. With mobile operators' unique advantages — such as the SIM card, the registration processes, contextual network information and fraud mitigation processes — they have the ability to provide strong customer authentication and interoperable, federated identity management solutions to enable consumers, businesses and governments to interact in a private and secure environment.

The GSMA is working with network operators and other mobile ecosystem players, as well as governments, banks and retailers, to help roll out mobile identity solutions. The GSMA is also working with industry standardisation bodies such as the Open ID Foundation to ensure support and interoperability for global standards.

Together, mobile operators are bringing mobile identity solutions to market. These solutions support huge scale, via a set of consistent technologies that benefit from low barriers to entry right across the digital identity ecosystem. These solutions also offer a seamless consumer experience that is scalable, safe and secure and puts users in control of their data and personal information.

Advantages of mobile operators in providing a digital identity service

| | |
|---|---|
| Flexibility to innovate | Flexibility to provide multiple authentication factors and the ability to add consumer functionality such as 'add to bill' or 'click to call'. |
| The mobile device | Ubiquitous, personal and portable; sensitive to location and capable of being disabled and locked. |
| The SIM card | Real-time strong authentication; encryption for storing certificates and other secure information. |
| Know your customer (KYC) standards | Strong registration and fraud-detection processes in place. |
| Robust regulatory requirements | Established systems to handle personal data safely. |
| Customer service | Sophisticated customer care processes and billing relationships. |
| Verified subscriber data | Ready for mobile identity. |
| The network | Secure by design, a mobile network can disable a device's SIM card and flag the device as lost or stolen in a global database. |
| Business processes | Ensures that the user has a way to report events, such as lost/stolen devices or an account compromise/takeover. |

# Mobile Connect

## Background

Mobile Connect is a secure digital identity framework developed by the GSMA in cooperation with leading mobile operators. Simply by matching the user to their mobile phone, Mobile Connect allows them to log-in to websites and applications quickly without the need to remember passwords and usernames. It is safe, secure and no personal information is shared without permission.

The key benefits of Mobile Connect include:

- Ease of use, as it employs the user's mobile phone for authentication, there is no requirement to use passwords.
- Secure and strong customer authentication (as there are no passwords to steal, it improves the user experience).
- Adds security and trust into digital transactions (as it confirms the user's location, identity and usage).
- Protects privacy (as the operator confirms credentials and the user gives consent for sharing of this information).
- Simple and cost effective to deploy.

To date, 60 operators have deployed Mobile Connect across 30 countries, making it available to nearly three billion customers.

Mobile Connect is supported by the GSMA Identity programme. The programme's strategic goal is to enable operators to play a significant role in the digital ecosystem through the provision of interoperable and commercially sustainable mobile identity services via Mobile Connect.

The GSMA's public policy activities assist the GSMA Identity programme via advocacy and pilot initiatives to support the use of Mobile Connect in regulated sectors, such as finance, e-government and e-health.

For example, in February 2018, the GSMA completed the second phase of a pilot that used Mobile Connect within the framework of the EU Regulation on Electronic Identification, Authentication and Trust Services (eIDAS). The report, issued upon completion of the trial, provides insights into operating within eIDAS and offers recommendations on how Mobile Connect can support the growth of these services.

In keeping with the priorities of many governments, Mobile Connect solutions focus on privacy and preserving citizens' trust. For example, in line with the EU General Data Protection Regulation (GDPR), Mobile Connect adopts the principle of privacy-by-design, as it seeks to ensure that an individual's identity attributes are used by digital services in a secure way that respects and protects their privacy.

Another key focus of the programme is aligning Mobile Connect with the requirements of the EU's revised Payment Service Directive (PSD2). This requires banks to open their APIs to authorised financial technology companies and use strong customer authentication for digital payments.

## Public Policy Considerations

Mobile identity services inevitably involve multiple devices, platforms and organisations that are subject to differing technical, privacy and security standards. Increasingly governments are using mobile technology as a key enabler to deliver identity services in their digital plans, thereby accelerating inclusion and reducing the digital divide. However, for mobile identity solutions such as Mobile Connect to achieve wide adoption and the greatest impact on the economy, a number of public policy issues must be addressed:

- Identify and assess existing legal, regulatory and policy challenges and barriers that affect the development of mobile identity services.
- Leverage best practice and advances in technology to foster the deployment of wide-scale mobile identity services and transactions.
- Engage with mobile operators and the wider digital identity ecosystem to facilitate greater collaboration between the public and private sectors and encourage interoperability and innovation.

Governments and regulators should create a digital identity plan that acknowledges the central role of mobile in the digital identity ecosystem. The mobile industry is committed to working with governments and other stakeholders to establish trust, security and convenience in the digital economy.

The mobile industry has a proven track record of delivering secure networks and has developed enhanced security mechanisms to meet the needs of other industry and market sectors. The implementation and evolution of these security mechanisms is a continuous process. The mobile industry is not complacent when it comes to security issues and the GSMA works closely with the standards development community to further enhance the security features used to protect mobile networks and their customers.

In summary, the mobile industry, via Mobile Connect, offers an identity and authentication experience that is aligned with best practice in the private sector, but uses mobile technology to leapfrog legacy infrastructure and economic barriers to deliver secure digital transactions.

Resources:
Mobile Connect website
GSMA Identity website
GSMA Report: eIDAS Pilot
Mobile Connect Privacy Principles
Mobile Connect: High Security Authentication
GSMA Report: Mobile Identity — A Regulatory Overview
GSMA, World Bank & SIA White Paper: Digital Identity — Towards Shared Principles for Public and Private Sector Cooperation

# Business Environment

All over the world, mobile network operators are providing the essential connectivity that people and businesses expect. In recent years, the industry has adapted to major changes brought about by the convergence of technologies and services, and by the emergence of internet platforms and services. Telecommunications markets have broadened and competition has increased as a result.

In most countries, however, mobile operators are still subject to regulations designed for the 'voice era'. These rules and obligations restrict their ability to innovate, invest and compete on equal terms in the digital ecosystem.

Policymakers should strive to create an enabling business environment that fosters competition and protects consumers without impeding commercial activity or economic progress. This will require a fresh look and a revision of regulations so they better reflect today's technologies and markets.

The following pages contain a number of policy topics that affect mobile operators, laying out the key points of debate and formally agreed industry positions. As the mobile industry continues to roll out 4G networks and initiate 5G trials, the need for pro-investment policies and modernised regulatory regimes has never been greater.

# Policies for Progress

### Resetting policy and regulation to drive the digital economy

From shopping and entertainment to managing household finances, digital technologies have fundamentally altered human behaviour, and consumers presented with the opportunity have been quick to integrate digital tools into their daily life. Many governments, recognising the value of mobile to society, have implemented bold policies to cultivate the digital economy, while extending connectivity to underserved communities.

A holistic policy framework that reflects the changing digital landscape while reducing costs and barriers to network deployment will deliver the best outcomes for society and the economy. If regulatory policies and institutions fail to adapt, markets can become distorted in ways that harm competition, slow innovation and, ultimately, deprive consumers of the benefits of technological progress.

Figure 1 identifies four areas of policy action related to network investment, regulation, promoting the digital economy and demonstrating digital leadership.[1]

Regulation — to focus on the area most applicable to this handbook — needs to be rethought for the digital and mobile age. However, reform has not kept pace with the converged and highly dynamic digital ecosystem. Emerging technologies are driving new business models, blurring the boundaries between once-distinct markets. Regulatory systems developed during the early years of mobile telecoms are still in place in many countries, and such regulation can actually do harm by slowing innovation and technological and market advances today.

The good news is that policymakers recognise the need to change. In many jurisdictions, such as the European Union, reforms are underway that will protect competition and consumers without impeding social and economic progress. We must not allow tomorrow's technologies to be stifled by yesterday's regulations. By updating the regulatory framework, policymakers can ensure that government and industry are aligned to create a growing and inclusive digital society for all.

**Figure 1 — Policy levers to promote an inclusive digital economy**

**Encourage Network Investment**

- Implement a broadband policy with clear goals
- Support infrastructure deployment
- Focus on spectrum allocation and use, not auction revenues

**Modernise Regulation**

- Adopt functionality-based, technology-neutral regulation
- Favour ex-post approaches over ex-ante prescriptive regulation
- Apply regulations consistently across the digital ecosystem

**Promote Digital Economy**

- Support data security and privacy
- Push digital literacy and lifelong learning
- Encourage the digitalisation of companies

**Demonstrate Digital Leadership**

- Encourage the use of digital IDs
- Support digital financial infrastructure
- Introduce digital government services

1 GSMA Report: Embracing the Digital Revolution — Policies for Building the Digital Economy (February 2017)

# Base Station Siting and Safety

## Background

Mobile services are a key enabler of socio-economic development, and achieving ubiquitous access to mobile services for citizens is a major government policy objective in most countries. Mobile operators often have roll-out obligations in their market area to ensure widespread national coverage.

To deliver continuous mobile coverage in dense urban areas and across rural expanses, mobile network operators must build and manage an array of base stations — free-standing masts, rooftop masts and small cells — equipped with antennae that transmit and receive radio signals, providing voice and data services to their customers in the area. The deployment of 5G will include the greater use of small cells to provide high-capacity and low-latency connectivity.

A variety of requirements and conditions, including electromagnetic field (EMF) exposure limits, must be met to secure permits for base-station deployment. Requirements can be defined at the local, regional and national level, even though the local authority (e.g., the municipality) is typically the point of referral. The process in some countries leads to significant delays and cost variances.

## Debate

*What antenna permitting processes should governments implement to avoid undue delay in infrastructure installation?*

---

*What reference point should be used by governments to define safe EMF exposure limits?*

---

*How can a balance be struck between national objectives for mobile connectivity for citizens and the decisions of municipalities?*

---

*Can processes be streamlined for the approval of small cell antennae and modifications to existing sites to achieve the necessary network densification?*

---

## Industry Position

**Governments that enable mobile network investment and remove barriers to the deployment of network infrastructure will accelerate the provision of mobile services to their citizens.**

By defining explicit, nationally consistent planning approval processes for mobile base stations, governments can avoid lengthy delays in network deployment. We support mechanisms that reduce bureaucratic inefficiencies, including exemptions for small installations, colocations or certain site upgrades, 'one-stop shop' licensing procedures and tacit approval. Governments can lead by example by improving access to government-owned land and buildings.

Base-station exposure guidelines should be aligned with international standards as recommended by the World Health Organization (WHO) and International Telecommunication Union (ITU). Additional arbitrary restrictions related to environmental impact should be avoided.

Infrastructure costs place a high threshold on entry into the mobile sector. If policies are short-sighted, and if taxes and licence fees are not in keeping with actual market dynamics, then operators may not have the means, or the will, to roll out new technologies and to reach rural areas. Such policies delay the social and longer-term economic benefits experienced by citizens.

Resources:
GSMA EMF and Health website
GSMA Base Station Planning Permission in Europe website
World Health Organization Electromagnetic Fields website
FCC Initiative: Leading the World Toward a 5G Future
ITU-T K.Suppl.9 on 5G Technology and Human Exposure to RF EMF
ITU-T K.Suppl.14 on The Impact of RF-EMF Exposure Limits Stricter than the ICNIRP or IEEE Guidelines on 4G and 5G Mobile Network Deployment
GSMA Report: 5G, the Internet of Things (IoT) and Wearable Devices: What do the New Uses of Wireless Technologies Mean for Radio Frequency Exposure?
GSMA: Arbitrary Radio Frequency Exposure Limits — Impact on 4G Network Deployment
GSMA Video: Mobile Networks Are Necessary to Deliver a Better Connected World
GSMA Report: LTE Technology and Health
GSMA Report: Improving Wireless Connectivity Through Small Cell Deployment
GSMA Report: Delivering the Digital Revolution

Facts and Figures

## Radio Frequency Policies for Selected Countries

| Country | RF Limit at 900 MHz (W/m²) | Requirement for RF licensing | Exemptions or simplified procedures for... | Location restrictions | Consultation during siting process |
|---|---|---|---|---|---|
| Australia | 4.5 | Compliance declaration | Small antennae, changes | None | Yes |
| Brazil | 4.5 | Approval | – | 50m [a] | Local |
| Canada | 2.7 | Approval | Small antennae, changes | None | Yes |
| Chile | 4.5/1 | Approval | Small antennae, changes | >50m [b] | Yes |
| Egypt | 4 | Approval | – | 20m [c] | No |
| France | 4.5 | Approval | Small antennae, changes | Voluntary, to minimise exposure [d] | Local |
| Germany | 4.5 | Approval | Small antennae, changes | None | Yes |
| India [e] | 0.45 | Compliance declaration | – | None nationally, local variation | No |
| Italy | 1/0.1 | Approval | Small antennae | Lower limits [f] | Yes |
| Japan | 6 | Approval | Small antennae | None | Local |

| Country | RF Limit at 900 MHz (W/m²) | Requirement for RF licensing | Exemptions or simplified procedures for... | Location restrictions | Consultation during siting process |
|---|---|---|---|---|---|
| Kenya | 4.5 | Compliance declaration | Changes | None | Yes |
| Malaysia | 4.5 | Approval | Small antennae | None | Yes |
| Netherlands | 4.5 | Compliance declaration | Small antennae, changes | None | Yes |
| New Zealand | 4.5 | Compliance declaration | Small antennae, changes | None | Local |
| Kingdom of Saudi Arabia | 4 | Compliance declaration | – | None | No |
| South Africa | 4.5 | Compliance declaration | – | None | Local |
| Spain | 4.5 | Approval | Small antennae, changes | None | Local |
| Turkey [g] | 0.18 | Approval | – | None | Local |
| United Kingdom | 4.5 | Compliance declaration | Small antennae, changes | None | Yes |
| United States | 6 | Approval | Small antennae, changes | None | Local |

a 50m around hospitals, schools and homes for old people
b ICNIRP with lower limit in urban areas and in 'sensitive areas'
c Not within 20m of schools and playgrounds
d Recommendation to minimise exposure in schools, day-cares or healthcare facilities located within 100m
e Adopted ICNIRP in 2008 and changed to 10 per cent of ICNIRP on 1 September 2012
f Lower limit in playgrounds, residential dwellings, schools and areas where people are >4 hours per day
g One installation; total exposure must not exceed four per cent of ICNIRP 1998

# Competition

## Background

Mobile phones are the most widely adopted consumer technology in history. A large part of this success can be attributed to how competition in the mobile industry has helped drive innovation.

The rise of the digital economy and explosive growth in smartphone adoption have brought innovation and disruption to traditional mobile communications services. These changes are also impacting existing policy frameworks and challenging competition policy (which includes government policy, competition law and economic regulation).

Despite the influence that new market dynamics are having on the mobile sector, the industry is still subject to the contradictions of a legacy regulatory system. This has resulted in services that are in competition with each other — such as voice services offered by mobile operators and those offered by internet players — being regulated differently.

These differences can be seen in how economic regulation (ex-ante) and competition law (ex-post) are applied to the sector. For example, a regulator's jurisdiction may be limited to the telecommunications sector, and not extend to internet players. As a result, regulators often fail to take wider market dynamics into account during the evaluation and decision-making process. Equally, a failure to understand the complex value chain can affect how competition law is applied.

Current competition policy is also being challenged by the competitive advantage conferred on some companies through their ability to collect and analyse large troves of data. This, combined with powerful network effects and the tendency for markets to tip in favour of dominant platforms, can harm consumers, hinder competition and stifle innovation. The ability of competition policy and enforcement to deal with issues arising in data markets is therefore key to the competitive development of the whole digital economy.

## Debate

*How should markets be defined in the digital age?*

---

*How can standard competition tools be applied in the digital age?*

---

*Are traditional significant market power (SMP) access remedies still appropriate?*

---

## Industry Position

**The mobile industry supports competition as the best way to deliver economic growth, investment and innovation for the benefit of consumers. Excessive regulation stifles innovation, raises costs, limits investment and harms consumer welfare through the inefficient allocation of resources, particularly spectrum.**

To ensure that competition and innovation thrive, it is essential that policymakers create a level playing field across the digital ecosystem. All competitors providing the same services should be subject to the same regulatory obligations, or absence of such obligations. This should be achieved through a combination of deregulation and the increasing use of horizontal legislation to replace industry-, technology- or service-specific rules.

Regulators and competition authorities must fully recognise the additional dynamic competition that exists in the digital age. Internet players adopt new and different business models to offer services to customers. Examples include advertising-supported services that make use of sophisticated internet analytics. Regulators and competition authorities need to understand these models, and map their competitive impact before imposing regulatory obligations or competition law commitments.

Otherwise, services that are in competition with each other may end up being regulated differently. For example, players that adopt traditional, better understood business models may find themselves subject to enhanced scrutiny.

Taking into account these new types of competitors when conducting market assessment reviews may show that there is a much greater level of competition in communication services markets than is currently recognised by regulatory and competition authorities. This type of analysis could demonstrate the potential for regulatory policy goals to be achieved through competition law, with the result that ex-ante regulation could be lessened, or may no longer be needed.

Indeed, it is a basic principle in economic regulation that regulation should not be imposed if competition law is sufficient to deal with the issues identified. As a result, a degree of deregulation of licensed providers is likely to be justified. Also, there is potential for competition law itself to be improved, to make it more effective. The GSMA published a report titled Resetting Competition Policy Frameworks for the Digital Ecosystem. This sets out 15 detailed recommendations to adapt competition policy to the challenges of the digital age, and is summarised on the following pages.

Resources:
GSMA Competition Policy website
GSMA Handbook: Competition Policy in the Digital Age
GSMA Competition Policy in the Digital Age: Case Studies from Asia and Sub-Saharan Africa
GSMA Report: The Data Value Chain

Deeper Dive

## Competition in Digital Markets

The global economy is undergoing a major transformation. The rapid take-up of technologies including mobile communications, digital platforms, Big Data, cloud computing and social media are changing the nature of products and services and the ways people interact. This transformation disrupts existing business models and industries, while offering substantial potential to enrich lives and raise living standards.

**Characteristics of the Digital Economy**

| | | |
|---|---|---|
| **Dynamic** waves of investment, innovation and technology | **Multi-sided** markets and platforms | **Network Effects** and economies of scale for digital services |
| **Quality** more important to consumers than price | **Big Data** as a key competitive factor | **Broader Markets** and blurring of traditional boundaries |

Competition in digital markets is different from competition in traditional markets. It has the following specific features:

- Waves of investment and innovation and rapid technological progress.
- Quality and product features that are often more important to customers than price.
- Winner-takes-all outcomes where new entrants offering innovative products or services may be able to leapfrog established firms.
- Economies of scale and strong network effects in the supply of digital services.
- Multi-sided markets and platforms, with distinct groups of users on the different sides benefitting from the presence of the other.
- Large-scale data gathering and analysis, with the potential for anticompetitive effects, especially where it contributes to the quality of service.

These differences challenge the existing policies and call for a reset of the competition framework and a more nuanced approach to competition policy for the digital ecosystem.

Deeper Dive

## Resetting Competition Policy Frameworks: Recommendations

The GSMA advocates that governments adopt the following recommendations to ensure their competition policy frameworks remain relevant for dealing with issues of abuse of market power and market failures in the digital economy.

**Market definition and market power**

1. Adjust existing tools to account for specific features of digital markets
2. Focus on actual substitution patterns
3. Use alternative tools to capture the main determinants of consumers' switching behaviour
4. Ensure market definition is sufficiently forward-looking, and revise and adapt policies to fully capture changes in the relevant market
5. Focus on alleged anticompetitive conduct and its likely effects rather than inferring market power from market structure
6. Assess the extent to which Big Data confers market power
7. Maintain a high threshold for intervention based on collective dominance

**The total welfare standard**

8. Adapt to a total welfare standard to support long-term productivity growth and higher living standards
9. Focus on dynamic effect when assessing mergers and competition in digital markets
10. Use better tools to assess efficiencies

**Ex-ante and ex-post regulation**

11. Review the thresholds for ex-ante regulation to ensure balance between regulation and investment risks
12. Focus ex-ante regulation on enduring market power
13. Ensure regulation is streamlined and consistent with competition law

**Institutional arrangements**

14. Adopt interim measures to accelerate ex-post enforcement and mitigate potential harm from anticompetitive conduct
15. Reassess institutional arrangements

# Efficient Mobile Market Structures

## Background

From the outset, mobile markets have been characterised by a vibrant, competitive market structure that drives investment and innovation.

Today, demand for robust, high-speed, high-quality mobile broadband continues to grow. This drives mobile operators to make large investments in network infrastructure and services at regular intervals to provide consumers with improved offerings at lower costs. For example, while operators are continuing to invest in their 4G networks, they are already starting to invest in the spectrum and technology required to roll out 5G networks.

The high level of competition in the markets for mobile services has also seen the tariffs charged to mobile users fall steadily and significantly over the past few years. At the same time, consumption of mobile services, particularly mobile data, has grown steadily, with the result that users today typically get more for their money.

In order to preserve competition, help drive innovation and support the wider societal benefits that mobile connectivity delivers, policymakers must ensure that the right economic conditions are in place to support investments. In particular, they must recognise the competitive nature of today's mobile markets, avoid regulating prices and steer clear of interventions aimed at engineering market structures. Instead, they should allow market mechanisms to determine the optimal mobile market structure.

Some regulators have used spectrum caps — limits on the amount of spectrum one entity can hold — to influence market structure, however, spectrum caps can generate unintended consequences including inefficient allocations of spectrum and/or reduced incentives to invest, ultimately resulting in poor outcomes for consumers, and as such they must be considered carefully.

At the same time, competition authorities tasked with assessing the impact of proposed mobile mergers must take full account of the dynamic efficiencies (and accompanying wider societal benefits) arising from mobile mergers.

## Debate

*Can mergers between mobile operators bring significant consumer benefits in mobile markets and wider society?*

---

## Industry Position

**When assessing mobile mergers, policymakers should consider the full range of static and dynamic benefits that can arise from mergers, including price effects, innovation, the use of spectrum and investments over both the short and longer term.**

### Investment and Quality of Service

- Competition authorities should consider placing greater emphasis on how mergers may change an operator's ability to invest. Growing demand for data services requiring ever increasing bandwidth means constant investment in new capacity and technology is needed.

### Positive spill-over effects in the wider economy

- Improvements in digital infrastructures support economic growth by positively affecting productivity across the whole economy.

### Greater benefits than network sharing

- Competition authorities have often argued that network sharing represents a preferred alternative to mergers. While the pro-competitive nature of network sharing agreements can only be assessed on a case-by-case basis, it is worth noting that network sharing agreements are not always feasible between the merging parties because of an asymmetry of assets (such as spectrum holding) or a different deployment strategy.

### Unit prices

- There is no robust evidence to suggest that four-player markets have produced lower prices than three-player markets in Europe and elsewhere over the past decade.
- Mergers can accelerate the transition between technology cycles in the mobile industry (technology cycles being responsible for significant reductions in unit prices), leading to improvements in quality and driving service innovation.
- As the market moves from voice to data, the global volume growth rate on mobile networks is accelerating. This calls for more concentrated market structures than in the past in order to meet the investment challenge and drive mobile data unit prices down so as to keep the demand for mobile data services growing.

### Effects of remedies on investments and use of spectrum

- In some cases, if operators are compelled to provide third parties with access to their networks, this could reduce rather than sharpen incentives to invest as a result of the merger, thus significantly reducing benefits to consumers. In addition, in the three cases (Ireland, Germany and Austria) where a network entry option was made available by the European Commission's Directorate-General for Competition, nobody took the option, even though this was arguably offered on favourable terms.
- Remedies that involve reallocating network assets or reserving spectrum for other operators could in some cases deter investment and lead to underutilised or misused resources.

Resources:
GSMA Report: Assessing the Case for In-country Mobile Consolidation
GSMA Report: Assessing the Case for In-country Mobile Consolidation in Emerging Markets
GSMA Report: Assessing the Impact of Mobile Consolidation on Innovation and Quality — An Evaluation of the Hutchison/Orange Merger in Austria
GSMA Report: Assessing the Impact of Market Structure on Innovation and Quality in Central America

Deeper Dive

## Dynamic Benefits In Mergers

Recently there has been heated debate about the effects of consolidation on the performance of mobile markets, following mergers in key European countries, including Austria, Germany, Ireland and the United Kingdom.

Some argue that consolidation has a detrimental effect on competition and prices. Others argue that if consolidation does not take place, mobile markets will not achieve the necessary scale and so fail to attract sufficient investment.

In the past three years multiple studies have analysed how mergers impact investment. For example, a 2017 GSMA report[1] analysed the impact of the Hutchison/Orange merger in Austria in 2012 on coverage and quality of service. We found that within two years Hutchison was able to accelerate population coverage of its 4G network by 20 to 30 percentage points as a result of the merger. Also, 4G download and upload speeds increased by 7 Mbps and 3 Mbps respectively within the same time period. The quality of mobile networks in Austria improved as a whole, with 4G download and upload speeds increasing by more than 13 Mbps and 4 Mbps in 2013 and 2014 respectively, and 3G download speeds increasing by 1.5 Mbps after 2014.

Since 2015, at least seven other studies[2] have examined the relationship between market structure, innovation and investment, as measured by operators' capital expenditure (capex). None found that increasing market concentration drove lower investment per operator or lower total country investment.

A first set of studies has found that investment always increases with market concentration, suggesting that the Hutchison/Orange merger would have had a positive effect on Austrian consumers via more investment.

CERRE (2015) found that, on average, a 10 per cent increase in the Herfindahl-Hirschman Index drives a boost of 24 per cent in merged operators' capex. In 2016, Jeanjean and Houngbonon found that markets with four players average 14 per cent lower investment per operator versus those with three players and that an increase in the number of operators tends to decrease investment. DG Competition (2017) finds that investment per operator increased as a result of the five-to-four merger in the United Kingdom in 2010, although no statistically significant effect is found when analysing investment per subscriber.

A second set of studies (Houngbonon & Jeanjean, 2016 and HSBC, 2015) suggests that greater market concentration increases capex per operator only when operators' profit margins are below 37 per cent to 44 per cent — with operators in most four-player markets being below this threshold, including Austrian operators before the merger. These studies suggest that the introduction of competition initially has a

### Effects of concentration on investment

| Research Paper | How does concentration affect investment per operator? | How does concentration affect total country investment? |
|---|---|---|
| WIK (2015) | No effect | No effect |
| CERRE (2015) | ↑ Investment increases | No effect |
| Houngbonon & Jeanjean (2016) | ↑ Investment increases | |
| Frontier (2015) | ↑ Investment increases in 4-player markets | |
| Houngbonon & Jeanjean (2015) | Inverted-U: investment maximised at 38% of margin | |
| HSBC (2015) | Inverted-U: investment maximised at 37% of margin | |

positive effect on investment, but that as mobile markets become less concentrated, it has a negative effect. Other studies have found that investment does not depend on market structure (WIK, 2015 and Frontier, 2015), suggesting that a mobile merger would have a neutral effect on outcomes such as network quality and coverage.[3]

One of the key findings is that post-merger, there is evidence that concentration leads to greater investment. While many believe that consolidation is likely to lead to a reduction of investment by operators, the evidence actually points to increased investment. This is because larger operators enjoy economies of scale that help when it comes to extending coverage and undertaking network upgrades. They also have greater financial strength — due to larger profit margins and improved access to complementary assets and commercial partnerships — and expect higher returns from their investments.

1 GSMA Report: Assessing the Impact of Mobile Consolidation on Innovation and Quality

2 CERRE (2015), Frontier (2015), Houngbonon & Jeanjean (2015), Houngbonon & Jeanjean (2016), HSBC (2015), WIK (2015), DG Competition (2017)

3 Though WIK (2015) found that market structures which provide higher profit margins and larger economies of scale (both enhanced by market consolidation) boost total capex per country

# Infrastructure Sharing

## Background

Common in many countries, infrastructure sharing arrangements allow mobile operators to jointly use masts, buildings and even antennae, avoiding unnecessary duplication of infrastructure. Infrastructure sharing has the potential to strengthen competition and reduce the carbon footprint of mobile networks, while reducing costs for operators.

Infrastructure sharing can provide additional capacity in congested areas where space for sites and towers is limited. Likewise, the practice can facilitate expanded coverage in previously underserved geographic areas.

As with spectrum trading arrangements, mobile infrastructure sharing has traditionally involved voluntary co-operation between licensed operators, based on their commercial needs.

## Debate

*Should regulators oversee, approve or manage infrastructure-sharing arrangements?*

*What role should governments play in the development and management of core infrastructure?*

## Industry Position

**Governments should have a regulatory framework that allows voluntary sharing of infrastructure among mobile operators.**

While it may at times be advantageous for mobile operators to share infrastructure, network deployment remains an important element of competitive advantage in mobile markets. Any sharing should therefore be the result of commercial negotiation, not mandated or subject to additional regulatory constraints or fees.

The regulatory framework of a country should facilitate all types of infrastructure sharing arrangements, which can involve the sharing of various components of mobile networks, including both so-called passive and active sharing.

In some cases, site sharing increases competition by giving operators access to key sites necessary to compete on quality of service and coverage.

Infrastructure sharing agreements should be governed under commercial law and, as such, subject to assessment under general competition law.

Access to government-owned trunk assets should be available on non-discriminatory commercial terms, at a reasonable market rate.

Resources:
GSMA Report: Mobile Infrastructure Sharing
GSMA Report: Unlocking Rural Coverage
ITU Mobile Infrastructure Sharing website
ZDnet: Could Tower Sharing Be the Solution to Rural Networks' Problems?

Deeper Dive

## Types of Infrastructure Sharing

Infrastructure sharing can be passive or active. Passive sharing includes site sharing, where operators use the same physical components but have different site masts, antennae, cabinets and backhaul. A common example is shared rooftop installations. Practical challenges include availability of space and property rights. A second type of passive sharing is mast sharing, where the antennae of different operators are placed on the same mast or antenna frame, but the radio transmission equipment remains separate.

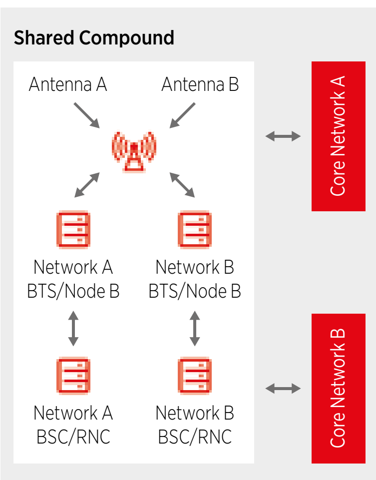
In active sharing, operators may share the radio access network (RAN) or the core network. The RAN-sharing case may create operational and architectural challenges. For additional core sharing, operators also share the core functionality, demanding more effort and alignment by the operators, particularly concerning compatibility between the operators' technology platforms.

Infrastructure sharing optimises the utilisation of assets, reduces costs and avoids duplication of infrastructure (in line with town and country planning objectives).

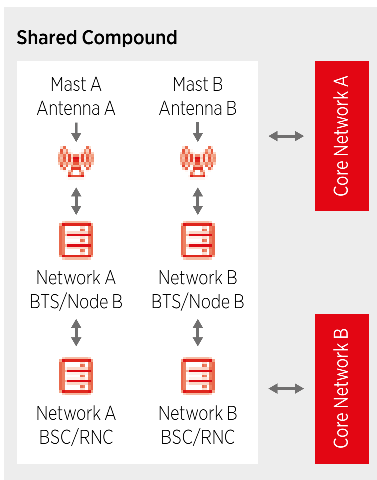
It may also:

- Reduce site acquisition time.
- Accelerate the roll out of coverage into underserved geographical areas.
- Strengthen competition.
- Reduce the number of antenna sites.
- Reduce the energy and carbon footprint of mobile networks.
- Reduce the environmental impact of mobile infrastructure on the landscape.
- Reduce costs for operators.

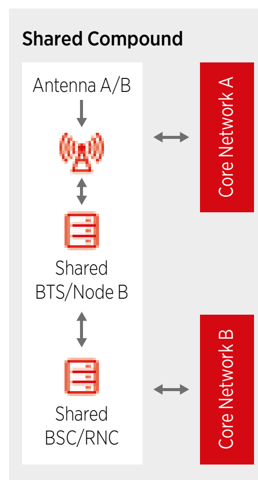
### Mast Sharing



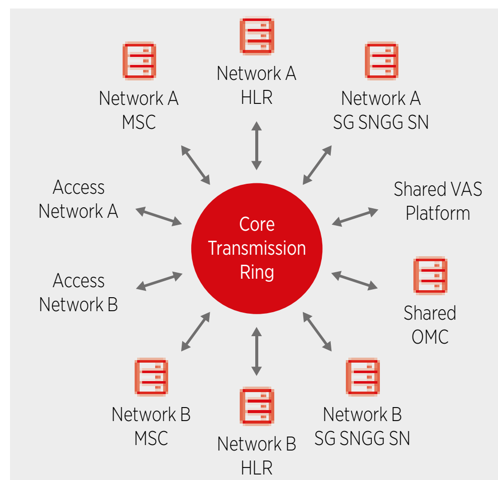

### Site Sharing




### Full RAN Sharing




### Shared Core Network Elements and Platforms




Source: GSMA

# Intellectual Property Rights — Copyright

## Background

Copyright is the basis for creative professionals such as artists, musicians, writers, filmmakers and composers to earn income, get recognition and receive protection for their works. The original intention of copyright was to encourage the development of new creative work. This is still the case today, but the emergence of digital technologies has radically changed the way creative content is produced, distributed and accessed by consumers.

Since the launch of its Digital Single Market (DSM) strategy in March 2015, the European Commission has published several proposals to improve cross-border access to content online, create wider opportunities to use copyrighted materials in education, research and cultural heritage and to create a better functioning copyright marketplace.

The proposal on temporary cross-border portability of online content services came into force on 1 April 2018. Now, suppliers of these services, when provided against remuneration, have to allow consumers to temporarily access content they have legally subscribed to in their member state of residence while staying in another EU member state. Providers are not requested to execute rights clearance or obtain additional copyright licences when so doing.

In the meantime, the European Commission's proposals on the modernisation of copyright in the DSM and on the extension of the Satellite and Cable Directive's broadcasting rules to other infrastructures, such as mobile networks and the open internet ('technology-neutral retransmission'), are still being fiercely debated. For example, now that consumers increasingly wish to access content online via their mobile and also across borders, the latter point has become problematic.

In addition, there is heated discussion related to the perceived 'value gap' between rights holders and online platforms as well as the issue of intermediary liabilities. One question that has arisen is whether there should be a neighbouring right for press publishers so that they receive remuneration when their news snippets are used. If this were put in place, news aggregators and possibly social networks and search engines would have to conclude licensing agreements with press publishers to be able to display news snippets. Similarly, the issue of whether online service providers should have to monitor and address (including via the use of content recognition technologies) the unlawful use of copyrighted content continues to be hotly debated.

These proposals have now been adopted by the European Parliament and will be at the centre of negotiations among EU co-legislators to finalise the copyright reform before the next European elections.

Furthermore, the European Commission has proposed new rules to compel internet platforms to remove terrorist content within one hour once it has been flagged by national competent authorities. These rules follow on from previous non-binding measures aimed at tackling illegal online content.

## Debate

*Should online service providers have to monitor and address 'illegal content' or the unlawful use of copyrighted content?*

*Who will be in the best position to make a reliable decision on what constitutes 'illegal content'?*

*How can access to content in the digital age be guaranteed and how can the clearance of rights be facilitated in a way that balances the interests of all stakeholders?*

## Industry Position

**The mobile industry recognises the importance of proper compensation for rights holders and supports the creation of fair, incentivising business models that respect the right balance. However, the GSMA cautions against putting the 'ISP liability regime' of the eCommerce Directive into question by having to take measures to prevent the availability of copyright infringing content.**

The exemptions from liability for intermediaries contained in the eCommerce Directive are core principles that guarantee users the freedom and confidentiality of communications and the freedom to access information, and offer legal certainty to internet service providers.

These principles are key, not only for the functioning of the information society and for the provision of innovative services in the DSM, but also for an effective fight against illegal content online. This fight requires, in most instances, contextualisation of different types of allegedly illegal content and must be weighed against the citizens' fundamental right to freedom of expression and access to information as well as privacy and protection of personal data.

Regarding access to content, the GSMA is in favour of extending the retransmission right in a technologically-neutral manner, including IP-based retransmission over the internet to different devices. However, the GSMA cautions against introducing a broadly-designed country-of-origin approach for broadcasters' rights clearance in respect of simulcasting, catch-up and similar services as this may negatively impact financing models, the contractual freedom of rights holders and service providers, and ultimately consumer choice.

Any new legislation should avoid double-paying, for redistributing content to its users (e.g., via licences).

Resources:
REGULATION (EU) 2017/1128 of 14 June 2017 on Cross-border Portability of Online Content Services in the Internal Market
European Commission Modernisation of EU Copyright Rules website
European Commission Recommendation on Measures to Effectively Tackle Illegal Content Online
European Commission Communication on Tackling Illegal Content Online — Towards an Enhanced Responsibility of Online Platforms

# Intellectual Property Rights — Patents

## Background

The mobile ecosystem has been a major driver of economic progress and welfare globally. Countries around the world continue to benefit from the improvements in productivity and efficiency brought about by the increased take-up of mobile products and services. As a result, GSMA Intelligence predicts mobile will generate five per cent of global GDP by 2022, equating to $4.6 trillion of economic value.

Without the immense efforts of the mobile operator community, many of the adopted technologies in 2G, 3G and 4G would not have been successfully developed, implemented or adopted on a mass scale.

At no point in history has telecommunications technology had a greater impact on peoples' lives than now. The public has become heavily reliant on mobile telecommunications technology and the mobile operators' abilities to deliver such services. Mobile telecommunications services provided by the operator community have become fundamental to everyday existence.

However, in the past few years, we have seen radical changes in the licensing of telecommunications technology (i.e., the prime use of patent portfolios in telecommunications). Initially patents were used to preserve a company's 'Freedom to Operate' (i.e., its ability to bring its products to market by seeking large portfolio cross-licences). Increasingly, patents have become tradable and income-generating assets (via the 'Secondary Patent Market'), capable of being asserted against start-ups, small and large companies, and, in some specific cases, to stifle competition.

## Debate

*Now that patents have become a tradable and income-generating asset, can they still be looked upon as a tool to support and promote innovation?*

---

*Are Patent Assertion Entities (PAEs) having a negative effect on competition?*

---

## Industry Position

**The Secondary Patent Market has greatly encouraged the rise in non-innovating, non-practising, patent monetisation and licensing or enforcement entities, known as PAEs. Usually, PAEs are purchasing patents (rather than developing and licensing technology) to be asserted against manufacturers and operators already using the technology.**

There are a number of reasons mobile operators' networks have become a premium target for so-called patent trolls in Europe, America and Asia. These include:

- The complexity of mobile operators' networks.
- The scale of investments needed to build them.
- The level of revenues they generate.
- The reliance of these networks on technology based on standards.

The multiple costs associated with PAEs' litigation and threats of injunction (as leverage in demands for disproportionately high licensing fees) have a detrimental effect on mobile network operators' businesses, as well as mobile telecommunications innovation and standardisation.

Increasing PAE litigations and adversarial/litigious licensing negotiations highlight the requirement for greater clarity in relation to the licensing of standard-essential technology. These efforts should focus on:

- The public's heavy reliance on mobile telecommunications technology and the mobile operators' abilities to deliver such services.
- That fact that disruption to these services, even in part, will have a severely negative effect on people's lives.
- The importance of maintaining the integrity of mobile telecommunication services and ensuring continuous investment and adoption of new technologies in the telecommunications market.
- The need to incorporate appropriate rules and regulations into the relevant frameworks governing the seeking and granting of injunctions in predatory patent assertion cases (in order to allow the judiciary to consider the above points).

Resources:
GSMA Report: The Rise of 'Predatory Patent Practices': A Major Escalation in Patent Assertion Entities Activity — A Telecommunications Operators' Perspective (2017)

# International Mobile Roaming

## Background

International mobile roaming (IMR) allows people to continue to use their mobile device to make and receive voice calls, send text messages and email, and use the internet while abroad.

Telecoms regulators and policymakers have raised concerns about the level of IMR prices and the lack of price transparency, which can cause consumer bill shock.

In December 2012, during the revision by the International Telecommunication Union (ITU) of the International Telecommunications Regulations (ITRs), several governments requested that the revised treaty include provisions on transparency and price regulation for mobile roaming. However, on balance, ITU member states concluded that roaming prices should be determined through competition rather than regulation, and text was included in the treaty to reflect this approach.

In the European Union, roaming regulation has been in place since 2007. From mid-June 2017, 'Roam-Like-At-Home' has been introduced in the EU. When offering roaming, mobile operators in a given EU country must include 'Roam-Like-At-Home' by default in contracts. Travellers can call, text and surf on their mobile devices when abroad in the EU for no extra charge on top of the price they pay at home. Operators can implement 'fair use' policies to prevent the abuse of regulated roaming services.

Bill shock and certain high roaming prices have also attracted the attention of international institutions such as the Organisation for Economic Co-operation and Development (OECD) and the World Trade Organisation (WTO). Additionally, regional and bilateral regulatory measures are either in place or being considered in many jurisdictions.

## Debate

*Some policymakers believe IMR prices are too high. Is regulatory intervention the right way to address this?*

---

*What measures can be taken to address concerns about price transparency, bill shock and price levels?*

---

*What other factors affecting roaming prices do policymakers need to consider?*

---

## Industry Position

**IMR is a valuable service delivered in a competitive marketplace. Price regulation is not appropriate, as the market is delivering many new solutions.**

The mobile industry advocates a three-phased strategy to address concerns about mobile roaming prices:

- **Transparency.** In June 2012, the GSMA launched the Mobile Data Roaming Transparency Scheme, a voluntary commitment by mobile operators to give consumers greater visibility of roaming charges and usage of mobile data services when abroad.
- **Removal of structural barriers.** Governments and regulators should eliminate structural barriers that increase costs and cause price differences between countries. These include double taxation, international gateway monopolies and fraud, all of which should be removed before any form of IMR price regulation is considered.
- **Price regulation.** Governments and regulators should only consider price regulation as a last resort, after transparency measures and innovative IMR pricing have failed to address consumer complaints, and after structural barriers have been removed. The costs and benefits of regulation must be carefully assessed, taking into account unique economic factors such as national variances in income, GDP, inflation, exchange rates, mobile penetration rates and the percentage of the population that travels internationally, as well as incidence of international travel to neighbouring countries, all of which have an impact on IMR prices.

The mobile industry is a highly competitive and maturing industry, and one of the most dynamic sectors globally. In the past decade, competition between mobile operators has yielded rapid innovation, lower prices and a wide choice of packages and services for consumers. Imposing roaming regulation on mobile operators not only reduces revenue and increases costs, but it deters investment.

Resources:
GSMA Roaming website
GSMA Information Paper: Overview of International Mobile Roaming
GSMA News: GSMA Launches Data Roaming Transparency Initiative

# Mobile Termination Rates

## Background

Mobile termination rates (MTRs) refer to the fees charged by operators to connect a phone call that originates from a different network.

The setting of regulated MTRs continues to be the focus of regulatory attention in both developed and developing countries, and many different approaches have been developed for the calculation of appropriate termination charges.

Regulators have generally concluded that the provision of call termination services on an individual mobile network is, in effect, a monopoly. Therefore, with each operator enjoying significant market power, regulators have developed various regulations, most notably the requirement to set cost-oriented prices for call termination.

## Debate

*How should the appropriate, regulated rate for call termination be calculated?*

---

*Is the drive towards ever-lower mobile termination rates, especially in Europe, a productive and appropriate activity for regulators?*

---

*Once termination rates have fallen below a certain threshold, is continued regulation productive?*

---

*What is the long-term role of regulated termination rates in an all-IP environment?*

---

*Intervening in a competitive market is far more complex and challenging than the traditional utility regulation of the kind normally applied to monopolies in gas, electricity and fixed-line telecommunications. With mobile, every action is more finely calibrated. The benefits of intervention are more ambiguous and the error costs larger.*

— Stewart White, former Group Public Policy Director, Vodafone

## Industry Position

**Regulated mobile termination rates should accurately reflect the costs of providing termination services.**

Beyond a certain point, evidence suggests that a focus on continued reductions in MTRs is not beneficial.

The setting of regulated MTRs is complex and requires a detailed cost analysis as well as a careful consideration of its impact on consumer prices and, more broadly, on competition.

MTRs are wholesale rates, regulated in many countries, where a schedule of annual rate changes has been established and factored into mobile network operators' business models. Unsignaled, unanticipated alterations to these rates have a negative impact on investor confidence.

The GSMA believes the setting of MTRs is best done at a national level, where local market differences can be properly reflected in the cost analysis, therefore extraterritorial intervention is not appropriate.

Resources:
Vodafone Report: The Impact of Recent Cuts in Mobile Termination Rates Across Europe
GSMA Report: The Setting of Mobile Termination Rates
GSMA Report: Comparison of Fixed and Mobile Cost Structure
Vodafone Report: Regulating Mobile Call Termination

# Net Neutrality

### Background

While there is no single definition of net neutrality, it is often used to refer to issues concerning the optimisation of traffic over networks. Net neutrality advocates assert that it is necessary to legislate that all traffic carried over a network be treated in the same way. Others contend that flexibility to offer different service levels for different applications enhances the user experience.

Where this flexibility exists, mobile network operators are able to offer a bespoke, managed service to providers of new connected products, such as autonomous cars, which could not exist without constant, high-integrity connectivity. Operators can also enter into commercial arrangements with content and application providers that want to attract users by offering free access — for example, by zero-rating their content — so mobile subscribers are not 'charged' for the data usage. These kinds of arrangements enable product and service innovation, deliver added value to consumers and generate new revenue for network operators, which face constant pressure to enhance, extend and upgrade their networks.

Mobile operators face unique operational and technical challenges in providing fast, reliable internet access to their customers, due to the shared use of network resources and the limited availability of spectrum.

Unlike fixed broadband networks, where a known number of subscribers share capacity in a given area, the capacity demand at any given cell site is much more variable, as the number and mix of subscribers constantly changes, often unpredictably. The available bandwidth can also fluctuate due to variations in radio frequency signal strength and quality, which can be affected by weather, traffic, speed and the presence of interfering devices such as wireless microphones.

Not all traffic makes equal demands of a network; for example, voice traffic is time-sensitive while video streaming typically requires large amounts of bandwidth. Networks need to be able to apply network management techniques to ensure each traffic type is accommodated and to support innovations with 5G and the Internet of Things. The principle of the open internet and allowing network operators to offer a variety of service options to consumers are not mutually exclusive. As the net neutrality debate has evolved, policymakers have come to accept that network management plays an important role in service quality.

*Just as content providers offer differentiated services such as standard and premium content for different prices, mobile network operators will offer different bandwidth products to meet different consumer needs. Customers are benefitting from these tailored solutions; only those who want to use premium services will have to pay the associated costs.*

— GSMA

### Debate

*Should networks be able to manage traffic and prioritise one traffic type or application over another?*

---

*For mobile networks, which have finite capacity, should fixed-line rules apply?*

---

*In some cases, net neutrality rules are being considered in anticipation of a problem that has yet to materialise. Is this an appropriate approach to regulation?*

---

### Industry Position

**To meet the varying needs of consumers, mobile network operators need the ability to actively manage network traffic.**

It is important to maintain an open internet. To ensure it remains open and functional, mobile operators need the flexibility to differentiate between different types of traffic.

Regulation that affects network operators' handling of mobile traffic is not required. Any regulation that limits their flexibility to manage the end-to-end quality of service and provide consumers with a satisfactory experience is inherently counterproductive.

In considering the issue, regulators should recognise the differences between fixed and mobile networks, including technology differences and the impact of radio frequency characteristics.

Consumers should have the ability to choose between competing service providers on the basis of being able to compare performance differences in a transparent way.

Mobile operators compete along many dimensions, such as pricing of service packages and devices, different calling and data plans, innovative applications and features, and network quality and coverage. The high degree of competition in the mobile market provides ample incentives to ensure customers enjoy the benefits of an open internet.

Resources:
GSMA Net Neutrality website
FCC Filing: GSMA Comments on the Open Internet Proceeding, 15 July 2014

Deeper Dive

### Traffic Management Is an Efficient and Necessary Tool

Traffic growth, the deployment of next-generation technologies and the emergence of new types of services are presenting mobile network operators with a huge challenge: how to manage different types of traffic over a shared network pipe, while providing subscribers with a satisfactory quality of service that takes into account different consumer needs and service attributes.

The finite capacity of mobile networks means they can experience congestion. Mobile operators use traffic management techniques to efficiently manage network resources, including spectrum, and to support multiple users and services on their networks. Congestion management is essential to prevent the network from failing during traffic peaks, and to ensure access to essential services.

Traffic management techniques are applied at different layers of the network, including admission control, packet scheduling and load management. In addition, operators need to cater to different consumer preferences, so customers can access the services they demand. Traffic management is therefore an efficient and necessary tool for operators to manage the flow of traffic over their network and provide fair outcomes for all consumers.

Mobile operators need the flexibility to experiment and establish new business models that align investment incentives with technological and market developments, creating additional value for their customers. As the operational and business models of networks evolve, a whole host of innovative services and business opportunities will emerge.

The current competitive market is delivering end-user choice, innovation and value for money for consumers and no further regulatory intervention related to the provision of IP-based services is necessary. The commercial, operational and technological environment in which these services are offered is continuing to develop, and any intervention is likely to impact the development of these services in a competitive context.

Traffic management techniques are necessary and appropriate in a variety of operational and commercial circumstances:

**Network integrity**

Protecting the network and customers from external threats, such as malware and denial-of-service attacks.

**Child protection**

Applying content filters that limit access to age-inappropriate content.

**Subscription-triggered services**

Taking the appropriate action when a customer exceeds the contractual data-usage allowance, or offering charging models that allow customers to choose the service or application they want.

**Emergency calls**

Routing emergency call services.

**Delivery requirements**

Prioritising real-time services, such as voice calls, as well as taking into account the time sensitivities of services such as remote alarm monitoring.

# Over-the-Top Voice and Messaging Communication Apps

## Background

The combination of mobile broadband access, smartphones and internet technology has led to the emergence of a new breed of consumer mobile voice and messaging communication services provided by internet-based companies, often referred to as over-the-top service providers (OTTs). These services are providing consumers with additional choices in how they communicate with each other.

OTT communications services are typically offered in competition with, and as direct substitutes to, the circuit-switched voice and SMS services provided by mobile operators, but they are typically not properly considered in the market analysis carried out by regulators.

Due to the global nature of the internet, and because they have not been considered as equivalent to traditional communication services, many OTT communications services sit outside the scope of sector-specific national or regional regulatory and fiscal obligations (e.g., e-privacy, legal interception, emergency calls, universal service contribution, national specific taxes, consumer rights and quality of service) that have been put in place to protect consumers and ensure that all providers make a fair and proportionate contribution to local economic growth through investment, employment and tax.

As OTT communications services become more and more popular, they increasingly render a number of regulations designed to address alleged network bottlenecks, such as termination and roaming, unjustified.

## Debate

*Should OTT services be subject to the same regulatory obligations that apply to calls and messages carried over the PSTN?*

---

*Does the fact that OTT players currently sit outside the scope of sector-specific regulations provide them with a competitive advantage over traditional telecoms providers?*

---

*Everybody knows today that with telecom service providers and OTT [players], there are unbalanced relations and we have to find a better balance.*

— Andrus Ansip, Vice-President for the Digital Single Market, European Commission, 2015

## Industry Position

**The mobile industry supports and promotes fair competition as the best way to stimulate innovation and investment for the benefit of consumers and to spur economic growth, and believes both objectives will be best served by the principle of 'same rules for the same service'. The growth in competition between different types of service provider calls for a move towards shared rules that are lighter touch than those applicable in less competitive environments.**

The principle of same rules for the same service maintains that where regulation is considered to be necessary, all equivalent consumer voice and messaging services should be subject to the same regulatory and fiscal obligations, regardless of the underlying technology, geographic origin or whether they are delivered by a mobile operator or OTT service provider. This will help to improve consumer confidence and trust in using internet-based services by ensuring a consistent approach to issues such as transparency, quality of service and data privacy. Consistent application of regulatory obligations will also support legitimate law enforcement and national security activities.

While the same rules should apply to the same services, these are not necessarily the rules that apply today to telecommunications services. There is a need for a forward-looking regulatory framework for communications services that is fit for purpose for a digital world. This framework must be driven by clear policy requirements around consumer protection, innovation, investment and competition.

By adopting a policy framework built around same rules for the same service, and properly recognising the competitive constraint imposed on mobile network operators by OTTs currently playing by different rules, national governments and regulators will be enabling an environment of fair and sustainable competition that promotes the best interests of consumers and fosters economic growth.

Resources:
Ovum: OTT Messaging Forecast: 2016–20
Juniper Research: OTT Messaging Users to Hit 4.2 Billion by 2021

# Passive Infrastructure Providers

### Background

Many mobile network operators share infrastructure on commercial terms to reduce costs, avoid unnecessary duplication and to expand coverage cost-effectively in rural areas.

The most commonly shared infrastructure is passive infrastructure, which may include: land, rights of way, ducts, trenches, towers, masts, dark fibre and power supplies, all of which support the active network components required for the transmission and reception of signals.

Infrastructure sharing is arranged through bilateral agreements between mobile network operators to share the specific towers, strategic sharing alliances, the formation of joint infrastructure companies between mobile operators or via independent companies providing towers and other passive infrastructure.

Increasingly, independent tower companies provide tower-sharing facilities to network operators. Several countries have established regulatory frameworks based on registration that encourage passive infrastructure sharing arrangements and provide regulatory clarity for network operators and independent passive infrastructure providers. While regulatory authorities in almost all countries are supportive of passive infrastructure sharing arrangements, a lack of regulatory clarity exists in some countries, particularly in relation to independent tower companies.

### Debate

*What benefits do independent tower companies offer to mobile operators?*

*Should passive infrastructure sharing ever be mandated by the regulatory authority?*

*What steps should regulators take to provide clarity to tower companies and mobile operators?*

### Industry Position

**Licensed network operators should be able to share passive infrastructure with other licensed network operators and outsource passive infrastructure supply to passive infrastructure providers without seeking regulatory approval.**

Sharing passive infrastructure on commercial terms enables operators to reduce capital and operating expenditure without affecting investment incentives or their ability to differentiate and innovate.

Infrastructure sharing provides a basis for industry to expand coverage cost-effectively and rapidly, while retaining competitive incentives. Regulation of passive infrastructure sharing should be permissive, but should not mandate such arrangements.

In markets with licensing frameworks that do not already provide for the operation of independent tower companies, regulatory authorities (or the responsible government department) should either permit independent passive infrastructure companies to operate without sector-specific authorisation or establish a registration scheme for such companies. The scheme should be a simple authorisation that provides for oversight of planning-related matters, while making a clear distinction with the licensing framework applicable to electronic communications network and service providers.

Registered providers should be permitted to construct and acquire passive infrastructure that is open to sharing with network operators, provide (e.g., sell or lease) passive infrastructure elements to licensed operators, and supply ancillary services and facilities essential to the provision of passive infrastructure.

Mobile network operators should be permitted to make use of infrastructure from passive infrastructure companies through commercial agreements without explicit regulatory approval. Infrastructure sharing agreements should be governed under commercial law and, as such, be subject to assessment under general competition law.

Public authorities should provide licensed operators and passive infrastructure providers with access to public property and rights of way on reasonable terms and conditions. Governments, seeking to support national infrastructure development, should ensure swift approval for building passive infrastructure, and environmental restrictions should reflect globally accepted standards.

Taxation and fees imposed on independent tower or passive infrastructure companies should not act as a barrier to the evolution of this industry, which makes possible more efficient, lower-cost forms of infrastructure supply.

Resources:
AT Kearney Report: The Rise of the Tower Business
Reuters News: Bharti Airtel to Sell 3,100 Telecom Towers

# Quality of Service

## Background

The quality of a mobile data service is characterised by a small number of important parameters, notably speed, packet loss, delay and jitter. It is affected by factors such as mobile signal strength, network load, and user device and application design.

Mobile network operators must manage changing traffic patterns and congestion, and these normal fluctuations result in customers experiencing a varying quality of service.

Connection throughput is seen by some regulatory authorities as an important attribute of service quality. However, it is also the most difficult to define and communicate to mobile service users. Mobile throughput can vary dramatically over time, and throughput is not the only product attribute that influences consumer choice.

## Debate

*Is it necessary for regulators to set specific targets for network quality of service in competitive markets?*

---

*Is it possible to guarantee minimum quality levels in mobile networks, which vary over time according to the volume of traffic being carried and the specific, local signal-propagation conditions?*

---

*Which regulatory approach will protect the interests of mobile service customers while not distorting the market?*

---

## Industry Position

**Competitive markets with minimal regulatory intervention are best able to deliver the quality of mobile service customers expect. Regulation that sets a minimum quality of service is disproportionate and unnecessary.**

The quality of service experienced by mobile consumers is affected by many factors, some of which are beyond the control of operators, such as the device type, application and propagation environment. Defining specific quality targets is neither proportionate nor practical.

Mobile networks are technically different from fixed networks; they make use of shared resources to a greater extent and are more traffic-sensitive.

Mobile operators need to deal with continually changing traffic patterns and congestion, within the limits imposed by finite network capacity, where one user's traffic can have a significant effect on overall network performance.

The commercial, operational and technological environment in which mobile services are offered is continuing to develop. Mobile operators must have the freedom to manage and prioritise traffic on their networks. Regulation which rigidly defines a particular service quality level is unnecessary and is likely to impact the development of these services.

Competitive markets with differentiated commercial offers and information that allows consumers to make an informed choice deliver the best outcomes. If regulatory authorities are concerned about quality of service, they should engage in dialogue with the industry to find solutions that strike the right balance on transparency of quality of service.

Resources:
GSMA Reference Document: Definition of Quality of Service Parameters and Their Computation
GSMA Latin America: Quality of Service

Deeper Dive

### A Network of Interconnections

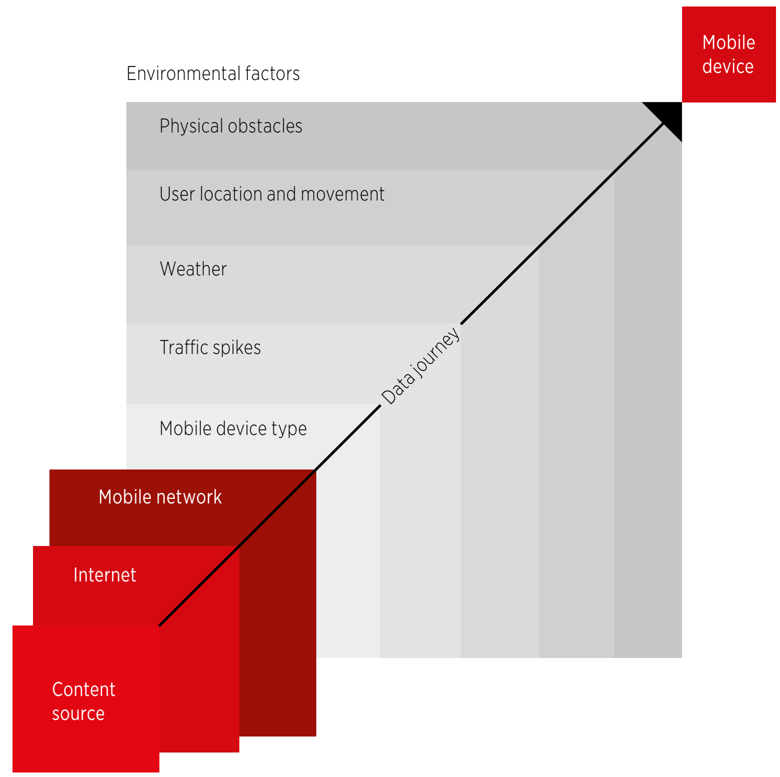
Offering a dependable quality of service is a priority for mobile network operators, as it allows them to differentiate the internet access service they provide from that of their competitors and meet customer expectations. However, mobile operators have little control over many of the parameters that can affect their subscribers' experience.

Factors beyond an operator's control include:

- The type of device and application being used.
- The changing usage patterns in a mobile network cell at different times of day.
- The movements and activities of mobile users, such as travel, events or accidents.
- Obstacles and distance between the terminal and antennae.
- The weather, especially rain.

In addition, the quality of internet access that users experience depends on the quality provided by each of the data paths followed. The internet service provider (ISP) only has control of the quality of service in its section of the network.

Factors affecting mobile quality of service




For these reasons, regulation concerning the quality of mobile internet service can be counterproductive. Regulation that does not consider the nature of mobile networks and the competitive workings of these services can be an obstacle to their development, widening the digital divide and promoting an inefficient use of the capital invested in networks.

# Single Wholesale Networks

## Background

Policymakers in some countries are considering establishing single wholesale networks (SWNs) or wholesale open-access networks (WOAN) instead of relying on competing mobile networks to deliver mobile broadband services in their country. Most of these proposals specify at least partial network ownership and financing by the government.

While there are variations in the SWN proposals discussed by different governments, SWNs can be generally defined as government-initiated network monopolies that compel mobile operators and others to rely on wholesale services provided by the SWN as they serve and compete for retail customers.

SWNs would represent a radical departure from the approach to mobile service provision that has been favoured by policymakers for the past 30 years — namely, to license a limited number of competing mobile network operators, which are usually under private ownership.

In 2000, there were almost as many countries served by a single mobile network as there were countries served by multiple competing networks. Today, however, only about 30 markets are served by a single mobile network.[1] Many of them are small islands with populations in the thousands, and, in total, they represent less than two per cent of the world's population. During the same period, network competition has produced unprecedented growth and innovation in mobile services, particularly in developing countries. The number of unique mobile subscribers has now surpassed five billion.[2] This success has fuelled innovation and helped increase speeds, improved network coverage and cut costs.

Supporters of SWNs argue they can address some concerns better than the traditional model of network competition in some markets. These concerns generally include inadequate or lack of coverage in rural areas, inefficient use of radio spectrum and fears that the private sector may lack incentives to maximise coverage or investment.

## Debate

*Are SWNs likely to increase the quality and reach of next-generation mobile broadband, compared with the existing approach of network competition?*

---

*What alternative policies should be considered before adopting a monopoly wholesale network model?*

---

## Industry Position

**SWNs and WOANs are likely to lead to worse outcomes for consumers than network competition.**

Some supporters claim they will deliver greater network coverage than network competition can. However, this claim often reflects the existence of public subsidies and other forms of favourable support for the SWN, which are not available to competing network operators, making it an unfair comparison. Commercial networks can deliver coverage even in areas where duplicate networks are uneconomic. This can be achieved in many ways, including through the implementation of voluntary network sharing among operators.

The benefits of network competition go beyond coverage. Innovation is a key driver of consumer value at the national level, and this occurs in networks as well as services and devices. While mobile technologies are typically developed at the international level, the speed at which they become available to consumers depends on national policies and market structures. In practice, government-mandated wholesale networks have been much slower to expand coverage, perform upgrades and to embrace new technologies.

Rather than use public funds to create a separate network to deliver coverage in areas into which commercial networks have not yet found it viable to cover, an alternative approach is to consider how public funds might be used to subsidise a commercial network provider to expand coverage to reach these areas.

1 GSMA & Frontier Economics Report: Assessing the Case for Single Wholesale Networks in Mobile Communications.

2 Source: GSMAi.

Resources:
GSMA & Frontier Economics Report: Assessing the Case for Single Wholesale Networks in Mobile Communications
GSMA Report: The Risks Associated with Wholesale Open Access Networks

Deeper Dive

## Risks Associated with Single Wholesale Networks

Governments often have ambitious goals when they mandate the creation of a single wholesale network (SWN) or a wholesale open-access network (WOAN) instead of relying upon the market, especially competing mobile networks, to deliver mobile broadband services in their country. However, research shows that of the five countries seriously considering this option, only Rwanda and Mexico have actually rolled out a network (as of mid-2018). The lessons from all five countries highlight the significant challenges associated with SWNs and WOANs.

For example, the public-private partnership project in Rwanda set ambitious goals but has faced a number of difficulties in meeting them. While an LTE network has been rolled out, connectivity is generally not being delivered in areas where operators are not already providing 3G coverage. The network is also competing directly with the existing mobile operators, as opposed to selling services to them on a wholesale basis. Pricing remains a concern, as levels are so low they are undercutting those of the existing mobile operators, leaving little room for reinvestment.

In the other four countries, efforts to roll out networks have either been severely delayed or abandoned altogether.

The roll out in Mexico was marred by delays and the scope of the project has been reduced. In May 2015, the government announced the investment target had been reduced from $10 billion to $7 billion. It also estimated that the number of cell towers built for the network will be closer to 12,000 instead of 20,000.

In 2016, the Altán consortium, as the sole remaining bidder, was granted access to 90 MHz of valuable spectrum in the 700 MHz band to build an LTE-based wholesale network. In mid-2018, the network had reached its first coverage target at 32 per cent of the population.

However, as with the project in Rwanda, the cost structure is a major concern. The government isn't receiving any revenue from the licence for this valuable spectrum and Altán is paying much reduced annual spectrum fees. This is distorting the market, as existing operators must still pay for their spectrum licence as well as full annual spectrum fees, while also finding funds to reinvest in their networks.

The Altán consortium is yet to prove its service is a valuable offering for Mexican consumers and businesses, as the network is also only available in areas where existing mobile operators already provide coverage. Consequently, take-up among the large operators, which would help increase the impact of the project, has been slow. This makes the final goal to reach 92.2 per cent of the population by 2024 look very optimistic.

In other countries, projects have been abandoned or made little progress. In Kenya and Russia, the push stalled due to complicated negotiations with key stakeholders. As of September 2018, a Ministerial Policy Directive in South Africa to assign high-demand spectrum to a WOAN and to other electronic communications network service licensees simultaneously was the subject of a public consultation process.

Improving rural coverage is something the mobile industry works on tirelessly. Instead of going down the wholesale monopoly route, the GSMA recommends governments conduct a comprehensive consultation with all stakeholders to address coverage gaps.

While it is often a fiercely competitive industry, mobile operators are not shying away from cooperation as a means of expanding coverage. In the end, the connectivity gap can only be overcome through close collaboration between the telecoms industry and governments. The basic building blocks that can help make this happen are:

- Cost-effective access to low-frequency spectrum.
- Support for flexible use in spectrum (e.g., refarming and technology neutral licenses).
- Support for all forms of voluntary infrastructure sharing.
- Better usage of government USF/subsidiaries to incentivise extended coverage.
- Elimination of sector-specific taxation on operators, vendors and consumers.
- Non-discriminatory access to public infrastructure.
- Support for streamlined planning and administrative processes.
- Relaxation of quality of service requirements.
- Context appropriate competition policy, especially concerning market structure.
- Support for multi-sided business models such as zero rating and sponsored data.

# Taxation

## Background

The mobile telecommunications sector has a positive impact on economic and social development, creating jobs, increasing productivity and improving the lives of citizens.

Sector-specific taxes are levied on mobile consumers and operators in many countries. These include special communication taxes, such as excise duties on mobile handsets and airtime usage, and revenue-share levies on mobile operators. These taxes contribute to a high tax burden on the mobile sector that exceeds the burden on other sectors.

Some countries have applied a surcharge on international inbound call termination (SIIT), which can have the effect of increasing international call prices and acting as a tax on other countries' citizens.

There is an increasingly broad consensus around the world that for tax systems to be effective they should follow internationally recognised best practice principles.

## Debate

*Do sector-specific taxes deliver short-term government income at the expense of longer-term additional revenues that could be accrued through increased economic growth?*

## Industry Position

**Governments should reduce or remove mobile-specific taxes because the resulting social impact and long-term positive impact on gross domestic product, and hence tax revenues, will outweigh any short-term reduction in contributions to governments' budgets.**

Taxes should align with internationally recognised principles of effective tax systems. In particular:

- Taxes should be broad-based — different taxes have different economic properties and, in general, broad-based consumption taxes are less distortionary than taxation on income or profits.
- Taxes should account for sector and product externalities.
- The tax and regulatory system should be simple, easily understandable and enforceable.
- Dynamic incentives for the operators should be unaffected — taxation should not disincentivise efficient investment or competition in the information and communication technology (ICT) sector.
- Taxes should be equitable and the burden of taxation should not fall disproportionately on the lower-income members of society.

Discriminatory, sector-specific taxes deter the take-up of mobile services and can slow the adoption of ICT. Lowering such taxes benefits consumers and businesses and boosts socio-economic development.

Governments often levy special taxes to finance spending in sectors where private investment is lacking, however this approach is inefficient. Fiscal policy that applies a special tax to the telecommunications sector causes distortions that deter private spending and, in the end, diminish welfare by preventing the realisation of the positive spill-overs that mobile provides throughout the economy.

Emerging economies need to align their approach to taxing mobile broadband with national ICT objectives. If broadband connectivity is a key social and economic objective, taxes must not create an obstacle to investment in broadband networks or adoption and usage of mobile broadband by consumers. Lowering the taxation burden on the sector increases mobile take-up and use, creating a multiplier effect in the wider economy.

Taxing international calls negatively impacts consumers, businesses and citizens abroad, damaging a country's competitiveness.

Resources:
GSMA Mobile Taxation Research and Resources
GSMA Report: Taxing Connectivity in Sub-Saharan Africa

Facts and Figures

## Taxes and Fees on Mobile Consumers and Operators

Mobile operators have repeatedly raised concerns that their customers are facing an undue burden from taxation, compared to other goods and services. The taxation and fees burden on the mobile sector consists of a wide range of charges. On the consumer side, this includes taxes on handset purchases and connection activation, as well as calls, messages and data access. High taxation has a negative impact on the affordability of mobile services and can also have wider negative effects on productivity and economic growth.

In addition to these consumer-facing charges, mobile operators also face a range of other charges including licensing fees, corporation tax, revenue charges and many more. Taxes and fees that specifically target the mobile sector affect an operator's incentive to invest in network roll-out. The extent to which these charges fall on operators or consumers depends on individual market conditions. Some taxes may be absorbed by operators in the form of lower profits, while others may be passed through to consumers as higher prices, or a combination of the two.

Research by Deloitte for the GSMA revealed that:

- Mobile operators paid $32 billion in 2015 across 27 nations surveyed. Sector-specific taxes accounted for around $8 billion of this. Sector-specific excise duties were present in 81 per cent of surveyed nations, as were spectrum fees.
- Just under a third (28 per cent) of operators' revenues were spent on taxes, excluding non-recurring payments such as spectrum auction fees.
- In eight countries, including Brazil, Chad and DRC, taxes account for 40 per cent or more of sector revenue.

Among the countries surveyed, it is only in South Africa and Italy that the sector's tax contribution as a proportion of the whole tax take closely match its proportion of the whole economy. In four nations, the sector pays more than double, in three others more than triple and in three others more than four times.

Taxes and fees on mobile services affect the affordability of access and usage. These taxes and fees may have a disproportionate impact on lower-income consumers, as they result in mobile services accounting for a larger share of the annual income of poorer households. For the Democratic Republic of Congo, the most extreme case, these fees represent 21 per cent of the gross national income of the bottom 20 per cent of income earners.

## Eight Steps Governments Can Take to Rebalance Taxation and Promote Digital Inclusion

1. Phased reductions of sector-specific taxes and fees can represent an effective way for governments to signal their support for boosting the connectivity agenda.
2. To enable more users to gain access to mobile services, governments should choose to lower the affordability barrier caused in part by so-called 'luxury' taxes on devices and connections.
3. Uncertainty over future taxation reduces investment because the risk of future tax rises is priced into investment decisions. Governments should seek to limit unpredictable tax and fee changes and streamline how tax and fees are levied.
4. The spectrum award approach needs to balance the relationship between ex-ante and ex-post fees in a transparent way, to ensure operators do not pay twice for access to the same resource.
5. Eliminating import duties for mobile network equipment and other local taxes levied directly on mobile sites has the potential to increase network investment.
6. Governments should avoid disproportionate taxation of services such as mobile money, as it puts a wide range of positive externalities at risk.
7. Removal of surtaxes on international incoming calls can ease barriers to regional and international trade by lowering the cost of international communication. It can also improve affordability, enabling more consumers to realise the benefits of mobile services.
8. Governments should apply fees on profits rather than revenues, so as not to discourage investment and innovation. These fees require the same payment from an operator regardless of whether it retains its profit or uses it to invest in new infrastructure and services.

# Universal Service Funds

## Background

Universal service — characterised by a telecommunications service that is available, accessible and affordable — is a policy goal of many governments.

Some countries have established universal service funds (USFs) on the premise that operators are unable to extend service to some areas without financial support.

USFs are typically funded by levies on telecommunication sector revenues. In these cases, operators continue to be required to contribute a share, despite the expansion of service to the vast majority of a countries' citizens and the increasingly large accumulations of undisbursed funds.

The reality is that most funds have performed poorly in achieving universal access. Studies by the GSMA[1] and the ITU[2] show that across the world, more than half of the sums collected for USFs were never utilised and over a third of the funds were not able to distribute any of the levies collected. When administered ineffectively, USFs can be counterproductive in that, by effectively taxing communications customers, they actually serve to raise the affordability barrier.

## Debate

*Are USFs an effective way to extend voice and data connectivity to underserved citizens?*

*What alternative strategies could be more effective?*

*How relevant are USFs in mature markets?*

## Industry Position

**Governments should phase out USFs and discontinue collecting USF levies. Existing USF monies should be returned to operators and used to extend mobile services to remote areas.**

Liberalised markets and private-sector investment have delivered telecommunication services to the majority of the world's population, a trend that the industry considers will continue.

Few USFs have successfully expanded access to telecommunication services, as is their objective, yet they continue to accumulate large sums of money.

There is little evidence that USFs are an effective way to achieve universal service goals and many have, in fact, been counterproductive, because they tax communications customers, including those in rural areas, and therefore raise the barrier to rural investment.

USFs that already exist should be targeted, time-bound and managed transparently. The funds should be allocated in a competitive and technically neutral way, in consultation with the industry.

Governments should consider incentives that facilitate market-based solutions. They can help by removing sector-specific taxes, stimulating demand and developing the supporting infrastructure. Alternative solutions (e.g., public-private partnerships) should be explored in preference to USFs for the extension of communications to rural and remote areas.

[1] GSMA Report: Survey of Universal Service Funds (2013)

[2] ITU Report: Universal Service Fund and Digital Inclusion for All (2013)

Resources:
GSMA Report: Survey of Universal Service Funds, Key Findings
GSMA Connected Society: Are Universal Service Funds an Effective Way To Achieve Universal Access?

# Spectrum Management and Licensing

Mobile networks must continue to evolve to close the connectivity gap, respond to skyrocketing data traffic growth and deliver on the immense potential of the nascent Internet of Things industry. All of these elements will also be key pillars of the 5G mobile future.

To support this evolution, mobile operators need access to sufficient, internationally harmonised spectrum. Effective spectrum licensing plays a key role in providing operators with access to this necessary resource.

Everything starts with solid planning. To encourage substantial investment in mobile services, it is important to have a transparent, long-term broadband plan that includes a strategy for making sufficient amounts of spectrum available to the mobile industry. This creates a certainty that allows the industry to innovate and thrive.

Spectrum pricing also has a significant impact on investment, and ultimately on mobile services. Governments that seek to maximise state revenues from spectrum pricing, for example, risk much greater costs to society if competition in communications markets is undermined with the result that network investment is stifled.

Instead, to ensure widespread, high-quality affordable services, it is essential that a sufficient amount of spectrum is released for mobile use — especially Digital Dividend spectrum — with fair access prices.

With the World Radiocommunication Conference 2019 (WRC-19) on the horizon, governments should build upon the foundations of previous conferences to identify sufficient mobile spectrum to support the future of the digital society.

The work centred around Agenda Item 1.13 looks at spectrum for mobile broadband in frequencies between 24.25 GHz and 86 GHz. The successful identification of a significant amount of these frequencies for international mobile telecommunication (IMT) is vital to realise 5G's full potential.

The GSMA is very active at national, regional and global levels in advocating for the timely identification and release of more spectrum for mobile broadband.

# Core Mobile Bands

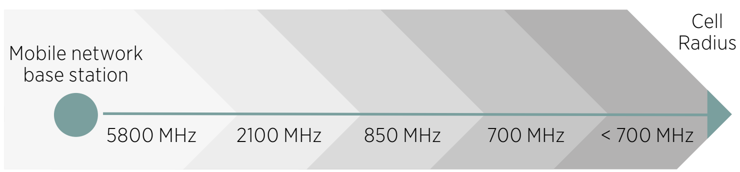
### Core frequency bands for mobile broadband

Not all radio frequencies are equal, and mobile network operators require access to a range of frequency bands to support affordable, high-quality mobile broadband services with excellent coverage. The core harmonised bands for mobile roughly fall within the frequency range of 400 MHz to 5 GHz, with the lower range providing large coverage areas and the higher range providing higher capacity.

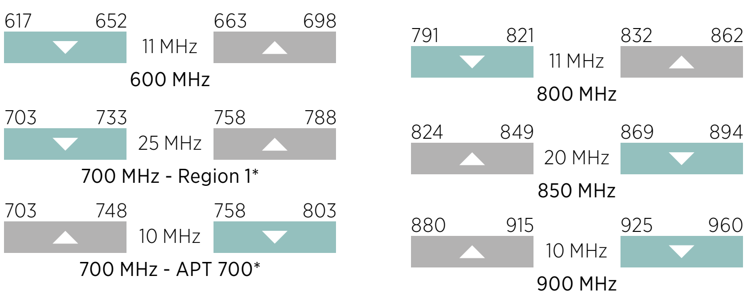
The frequency bands utilised in mobile networks today have been designated for mobile services internationally through ITU Radiocommunication Sector (ITU-R) and harmonised on either a regional or global basis. They are then standardised by 3GPP before commercial deployment. The most frequently deployed current bands are listed below. Although countries in different regions have adopted different combinations of those bands, regional and global harmonisation has created economies of scale, which in turn have made mobile services and handsets more affordable.

**Effects of frequency on range and coverage area**

In general, a network that uses higher-frequency spectrum requires more base stations to cover the same area as a network using lower frequencies.




Coverage Bands (<1 GHz)




*North America uses a more complex 700 MHz plan



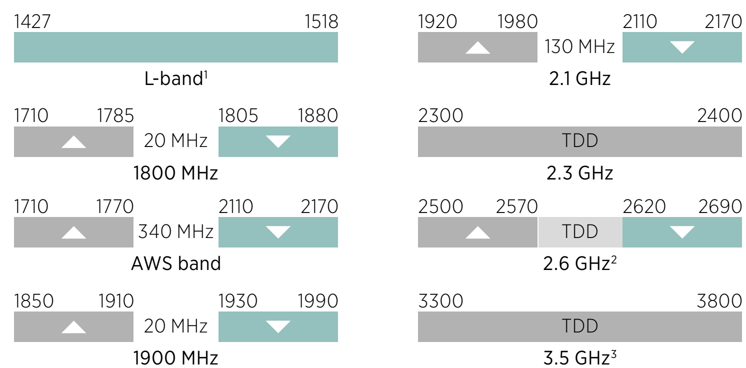
### Band Characteristics: Capacity vs. Coverage

In general, lower-frequency signals below 1 GHz reach further and are better at penetrating buildings. These frequencies are sometimes called coverage bands because an operator can serve a larger area with one base station. These bands are particularly important for providing affordable mobile broadband services in rural areas.

The capacity of a wireless connection for data or voice calls is dependent on the amount of spectrum it uses — the channel bandwidth — and wider channel bandwidths are more readily available at higher frequencies, for example at 1.8 GHz and above. These frequencies are often referred to as capacity bands. Deploying a network that uses these higher-frequency bands requires more base stations to cover the same area, thereby requiring more investment. However, these bands can support more mobile broadband traffic and higher speeds, making them effective in more densely populated areas.

It isn't an either/or proposal, however. A single mobile handset today can support a variety of bands, and mobile operators use a combination of different bands to provide good coverage and high data speeds. For future services, operators are looking at even higher bands, those above 6 GHz, to support data-intensive mobile applications.

Capacity Bands (> 1 GHz)




[1] Band plan is under development

[2] 50 MHz TDD in the centre gap

[3] Actual range differs by region/country

# 5G Spectrum

## Background

5G will support significantly faster mobile broadband speeds and heavier data usage than previous generations of mobile technology while also enabling the full potential of the Internet of Things (IoT). From autonomous cars and smart cities to the industrial internet and fibre-over-the-air, 5G will be at the heart of the future of communications. 5G is also essential for preserving the future of today's most popular mobile applications — such as on-demand video — by ensuring that growing uptake and usage can be sustained.

The technology will address four key usage scenarios:

- Enhanced mobile broadband, including multi-gigabit per second (Gbps) data rates.
- Ultra-reliable communications, including very low latency (sub-1 ms), very high availability and very high security.
- Massive machine-type communications, including the ability to support a huge number of low-cost IoT connections.
- Fixed-wireless access, including the ability to offer fibre-type speeds in both developed and developing markets.

The success of 5G services will be heavily reliant on national governments and regulators. Most notably, the speed, reach and quality of these services will depend on governments and regulators supporting timely access to the right amount and type of spectrum, under the right conditions. Spectrum awards for 5G have already begun and the variation in the amount of spectrum assigned, as well as the prices paid, means the potential of 5G services will vary between countries. This is because these factors impact the quality and capacity of 5G services and ultimately the competitiveness of national digital economies..

## Debate

*How much spectrum do regulators need to make available in key bands to support high-quality 5G services?*

---

*Should regulators aim to maximise state revenues or socio-economic benefits when assigning 5G spectrum?*

---

*What role could unlicensed and shared spectrum play within 5G?*

---



## Industry Position

**5G needs a significant amount of new harmonised mobile spectrum. Regulators should aim to make available 80-100 MHz of contiguous spectrum per operator in prime 5G mid-bands (e.g., 3.5 GHz) and around 1 GHz per operator in millimetre wave bands (i.e., above 24 GHz).**

5G needs sufficient spectrum in three key frequency ranges to deliver on prime 5G usage cases:

**Sub-1 GHz** will support widespread coverage across urban, suburban and rural areas and help support IoT services.

**1-6 GHz** offers a good mixture of coverage and capacity benefits and includes spectrum within the 3.3-3.8 GHz range, which is expected to form the basis of many initial 5G services.

**Above 6 GHz** is needed for the ultra-high broadband speeds envisioned for 5G. Currently, the 26 GHz and/or 28 GHz bands have the most international support in this range. Establishing international agreement on 5G bands above 24 GHz will be a key focus of the ITU World Radiocommunication Conference in 2019 (WRC-19).

WRC-19 will be vital to realise the ultra-high-speed vision for 5G, so government support for the mobile industry throughout the process is vital. The GSMA recommends the 26 GHz, 40 GHz and 66-71 GHz bands are supported for mobile, and that the 45.5-52.6 GHz range is studied in more detail.

Licensed spectrum should remain the core 5G spectrum management model. Unlicensed bands can play a complementary role.

Setting spectrum aside for vertical markets in priority 5G bands could jeopardise the success of public 5G services and may waste spectrum. Sharing approaches, such as leasing, are better options where vertical markets require access to spectrum.

Governments and regulators should avoid inflating 5G spectrum prices (e.g., through excessive reserve prices or annual fees) as they risk limiting network investment and driving up the cost of services.

Regulators must consult 5G stakeholders to ensure spectrum awards and licensing approaches consider technical and commercial deployment plans.

Governments and regulators need to adopt national spectrum policy measures to encourage long-term heavy investments in 5G networks (e.g., long-term licences, clear renewal processes, spectrum roadmaps, etc.).

Resources:
GSMA Public Policy Position: 5G Spectrum
GSMA Future Networks 5G website
GSMA Report: The 5G Era – Age of Boundless Connectivity and Intelligent Automation

# Digital Dividend

### Background

The Digital Dividend is the spectrum made available for alternative uses following the switchover from analogue to digital terrestrial television, as digital broadcasting uses spectrum far more efficiently than analogue broadcasting.

Digital Dividend spectrum is ideal for mobile broadband because it consists of lower-frequency bands that can cover wider areas with fewer base stations than current mobile broadband spectrum which relies on higher frequencies. This lowers deployment costs and allows operators to provide broader, more affordable coverage, especially in rural areas.

Digital Dividend spectrum also delivers benefits in urban areas, as it supports improved indoor coverage, because these frequencies can more easily penetrate buildings.

The initial upgrade to digital television created two potential new mobile bands. They are the 800 MHz band for use in Europe, the Middle East and Africa, and the 700 MHz band (698–806 MHz) — also known as APT 700 — for use in the Americas and the Asia Pacific region.

More recently, a second phase opens the door for two further mobile bands. The first one is 700 MHz (this time 694-790 MHz) for use in Europe, the Middle East and Africa. The second is 600 MHz in parts of the Americas and Asia Pacific, such as Bangladesh, Colombia, Mexico, New Zealand and the United States.

### Debate

*What goals should governments try to achieve when relicensing Digital Dividend bands?*

---

*How important is spectrum harmonisation when planning for the Digital Dividend?*

---

### Industry Position

**The Digital Dividend should be allocated for mobile use in alignment with regionally harmonised band plans as soon as possible.**

The switchover to digital television supports the delivery of a wide variety of high-definition broadcast content, while also improving the provision of mobile broadband services. Licensing as much Digital Dividend spectrum as possible for mobile use is key if governments are to give their citizens access to affordable, high-quality, mobile broadband services.

Governments should not seek to generate excessive fees from licensing these bands, as this can lead to spectrum remaining unsold and risks impacting network investment and deployment, while also potentially leading to higher mobile phone bills. Ultimately, excessive spectrum fees have the potential to limit the socio-economic benefits that affordable mobile broadband access can deliver.

Regional harmonisation of the bands will maximise economies of scale for equipment manufacturers (helping to drive down the cost of handsets for consumers) and mitigate interference along national borders. For these reasons:

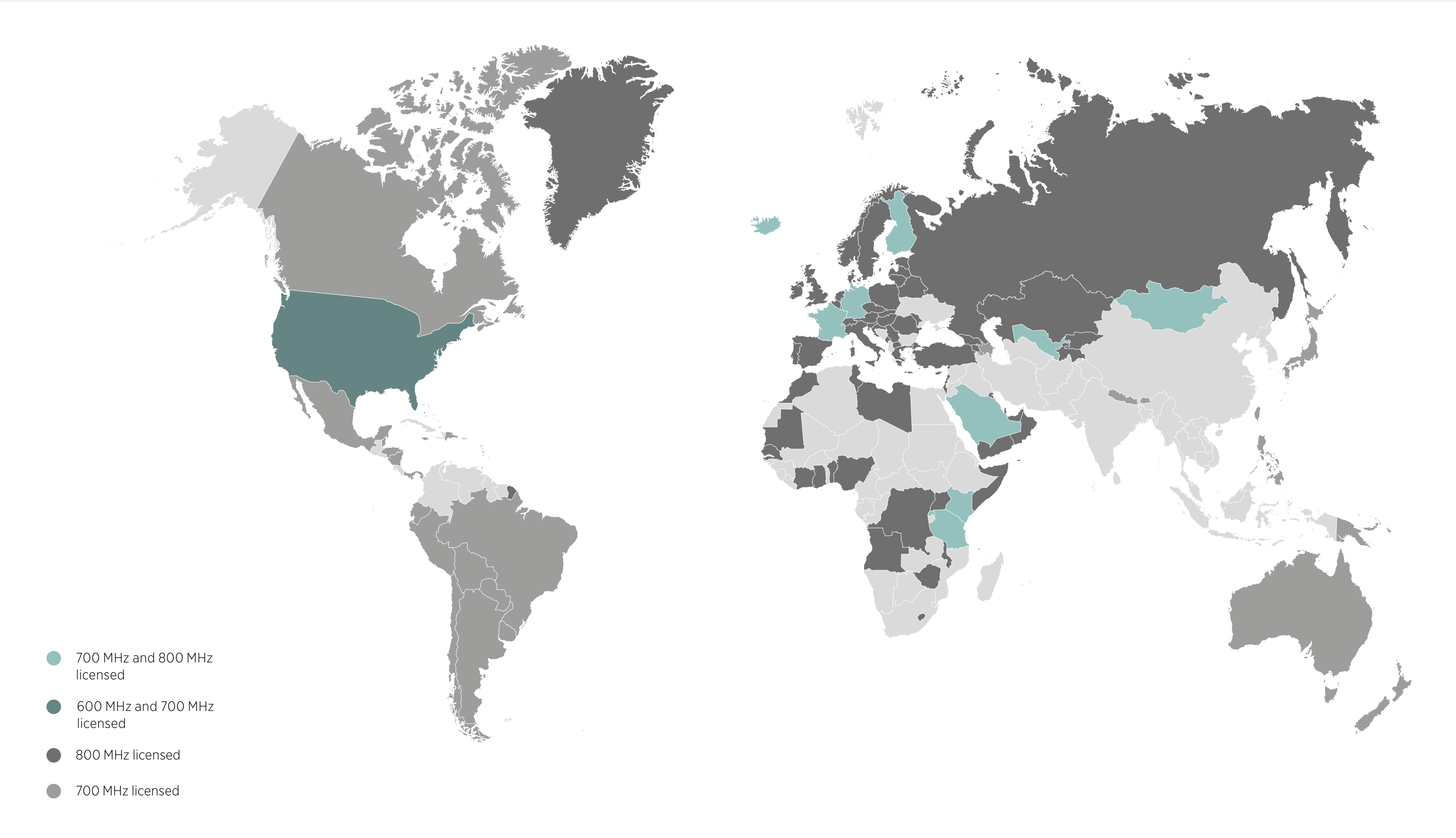
- Asia Pacific and Latin America should adopt the APT 700 MHz band plan.
- Europe, the Middle East and Africa should adopt the ITU Region 1 700 MHz band, which is compatible with APT 700 MHz equipment.
- Countries from ITU Region 2 and 3 (US, Mexico, New Zealand, etc.) are converging on the same 600 MHz FDD band plan, and this is laying an important foundation towards global harmonisation of the band.

Resources:
GSMA Public Policy Position: Securing the Digital Dividend for Mobile Broadband
GSMA Public Policy Position: Recommended Band Plan for Digital Dividend 2 in ITU Region 1
GSMA Public Policy Position: Asia Pacific Digital Dividend/UHF Band Plans
GSMA & ASIET Report: Economic Benefits of the Digital Dividend for Latin America
GSMA & BCC Report: The Economic Benefits of Early Harmonisation of the Digital Dividend Spectrum and the Cost of Fragmentation in Asia-Pacific

Facts and Figures

**Releasing Digital Dividend Spectrum for Mobile**

This map shows individual countries' progress in licensing Digital Dividend spectrum for mobile telecommunications.




Source: GSMA Intelligence, August 2018

# Limiting Interference

### Background

Radio transmissions always have the potential to interfere with radio systems operating in adjacent frequency bands, due to transmitter imperfections or imperfect receiver filtering.

New technologies are better at mitigating interference, although they can be more costly because of equipment complexity and energy consumption.

The solution is to define radio transmitter and receiver parameters to ensure compatibility between radio systems operating in the same or adjacent frequency bands. This approach cannot, however, be applied to technologies that lack standards.

The traditional way to manage interference has been to establish guard bands that are left vacant. However, these guard bands reduce the overall efficiency of spectrum use. Other interference-mitigation techniques should be employed as much as possible to minimise the loss of usable spectrum.

### Debate

*Are guard bands the only way to prevent interference between mobile bands and systems using adjacent bands?*

---

*Should potential interference be solved ex-ante by the national regulatory authority before allocating new spectrum to mobile operators, or should this be left to the operators?*

---

### Industry Position

**Interference can be managed with proper planning and mitigation techniques.**

For mobile telecommunications, regional harmonisation of allocated mobile bands is the best way to avoid interference along national borders.

Issues of cross-border interference are usually addressed through bilateral or multilateral agreements among neighbouring countries.

To minimise guard-band size and the cost of interference mitigation, radio system standards defining the RF performance of transmitters and receivers are necessary.

Broadcasters are rightly concerned that mobile services introduced in the UHF band do not interfere with television reception, and mobile operators are equally concerned that this does not happen. A television receiver standard would improve the situation.

*The more countries that support a band, the greater the possibility for global harmonisation, offering substantial economies of scale, reducing interference along country borders and delivering cost benefits for consumers.*

— GSMA

Resources:
GSMA Reference Document: Managing Radio Interference
GSMA Briefing Paper: WRC Agenda Item 1.17 — Broadcast Interference
GSMA Reference Document: Potential for Interference to Electronics

Case Study

## Real-World Experience of 800 MHz LTE Coexistence

Because Digital Dividend spectrum is, by definition, adjacent to frequency bands that continue to be used for television broadcasting, regulators and industry have worked hard to ensure that mobile services using the 800 MHz Digital Dividend band do not interfere with television broadcasting. Nevertheless, concerns continue to be aired in most markets until the actual roll out of the mobile services. Now that mobile network operators in several countries have begun to deploy LTE networks using Digital Dividend spectrum, these concerns can largely be put to rest.

In Germany, as of October 2012, more than 4,600 800 MHz base station sites had been deployed, in urban, suburban and rural areas. Reported incidents of interference were very low. Six cases of interference with digital terrestrial television were reported, and this includes the most critical case, involving the lower block of LTE spectrum and TV channel 60, which O2 rolled out in Nuremburg in July 2012. In addition, 22 cases involved wireless microphones (which had already been asked to migrate to other frequencies by the regulator), and six involved other radio services and applications.

In Sweden, hundreds of 800 MHz base station sites have been deployed, with the first-line response for reported interference managed jointly by the mobile operators. During the first quarter of 2012, approximately 40 cases of interference with the television bands were reported, of which 30 were quickly resolved by supplying the viewers with a television receiver filter.

Globally, up to now, there have been fewer cases of interference with digital terrestrial television by mobile services in the 800 MHz band than forecast. However, the incidence rate may vary depending on the proportion of the population that uses the digital television platform and the digital television network topology. Radio frequency (RF) amplifiers are a more significant factor than anticipated, but RF filters can solve the majority of interference cases.

So far, there has been no interference to cable networks.

Source: Vodafone



Case Study

## at800 in the United Kingdom

In 2012, mobile operator licensees in the UK set up a joint venture called at800 to act as the mechanism for resolving television interference issues when LTE services were launched in the 800 MHz band.

The four mobile operators are shareholders, and each had to contribute £30 million per 5 MHz lot acquired. at800 was then responsible for collecting information about each operator's LTE800 roll out plans and arranging a leafleting campaign in the affected areas, giving details of how householders could report interference issues. at800 manages the call centre, posts filters to consumers and sends engineers to fix any remaining problems. Any funds remaining after the completion of the programme will be divided among the shareholders. In practice, it has become apparent that the scale of interference was greatly overestimated.

In August 2017, at800 achieved a 100 per cent pass rate against its primary KPI, as it had every month in the previous year. For example, all 393 confirmed 4G interference cases in August 2017 were resolved within the 10-working-day target. For disruption that is not related to LTE at 800 MHz, at800 directs viewers to organisations that may be able to help.

# Spectrum Auctions

## Background

Spectrum management for mobile telecommunications is increasingly complex as governments release new spectrum in existing mobile bands, manage the renewal of licences coming to the end of their initial term, and release spectrum in new bands for mobile broadband services.

Effective and efficient management of these processes is central to the continued investment in, and development of, mobile services.

Auctions are an efficient way to allocate spectrum when there is competition for scarce spectrum resources and demand is expected to exceed supply. However, they need to be carefully planned if they are to lead to successful outcomes. In-demand Digital Dividend spectrum — which is the key to extending affordable mobile broadband services — has gone unsold in several developing markets because governments have set excessively high reserve prices.[1]

There are a number of different possible auction designs, each with its strengths and limitations. While multi-round auctions are often preferred, the best choice is dependent on the market circumstances and the objectives of the government and regulators.

When assigning spectrum via an auction, governments typically have a number of goals to achieve, which may include:

- The maximum long-term value to the economy and society from the use of the spectrum.
- Efficient technical implementation of services.
- Sufficient investment to roll out networks and new services.
- Revenue generation for the government.
- Adequate market competition.
- A fair and transparent allocation process.

## Debate

*How is the value of spectrum best determined?*

---

*Should governments design auctions to maximise revenue in the short term, or to ensure an economically efficient means of allocating a scarce resource?*

---

*Countries that get their licensing approach right can better realise the potential of mobile broadband, bringing substantial benefits to consumers and businesses in terms of innovative, high-quality services and lower costs of provision.*

— Competition Economists Group, 2016

## Industry Position

**Efficient allocation of spectrum is necessary to realise the full economic and societal value of mobile.**

There is no 'one size fits all' design for spectrum auctions. Each auction needs to be designed to meet the market circumstances and to achieve the specific objectives set by government.

As with most auction design elements, the appropriateness of simultaneous auctions (multiple bands being auctioned together) versus sequential auctions (bands being auctioned one after the other) is dependent on specific market conditions. The effectiveness of either approach will be dependent on a clear spectrum road map with well-defined rights and conditions understood in advance.

Regulators should work with stakeholders to ensure the auction design is fair, transparent and appropriate for the specific market circumstances. Auctions are not the only option available to governments to manage spectrum allocation and should only be used in appropriate circumstances.

Auctions should be designed to maximise the long-term economic and social benefits that can be gained from use of the spectrum. They should not be designed to maximise short-term revenue for governments. The following key principles can help guide licensing authorities:

- Auctions can deliver strong social benefits as long as they are properly designed.
- High spectrum prices jeopardise the effective delivery of wireless services.
- Spectrum licences should be technology and service neutral.
- Licence conditions should be used with caution.
- Licence duration should be at least 20 years to incentivise network investment.
- Competition can be supported by licensing as much spectrum as possible and limiting charges and other barriers to services.
- Voluntary spectrum trading should be encouraged to promote efficient spectrum use.

[1] In 2016 alone, part or all of the Digital Dividend mobile spectrum went unsold in Ghana, Senegal and India.

Resources:
GSMA & CEG Report: Best Practice in Mobile Spectrum Licensing
GSMA & NERA Report: Effective Spectrum Pricing: Supporting Better Quality and More Affordable Mobile Services
GSMA Report: Spectrum Pricing in Developing Countries — Evidence to Support Better and More Affordable Mobile Services
GSMA Public Policy Position: Spectrum Auctions
GSMA Managing Spectrum website

Case Study

## Rising Spectrum Prices Harming Consumers and the Digital Economy

Globally, spectrum prices reached all-time highs with the 3G auctions at the start of the millennium, before falling gradually until 2007. From 2008-2016, when 4G auctions became common, the average final price paid for spectrum sold at auction increased 3.5 fold.[1] A key factor behind this significant rise was a number of outlier auctions where final prices were extremely high.

High spectrum prices are associated with more expensive, lower-quality mobile broadband services and irrecoverable losses in consumer welfare worth billions of dollars worldwide.[2] For example, research shows that when prices are too high, operators are likely to invest less in their networks — which impacts the quality and reach of services. High spectrum prices are particularly harmful in developing countries where they have become a major roadblock to increasing much-needed mobile penetration. Pricing in developing countries is, on average, more than three times higher than in developed countries, when income is taken into account.[3]

The cause of these extremely high prices are typically policy factors that appear to prioritise maximising short-term state revenues above long-term support for the digital economy through improved mobile services. Policy factors include setting excessive reserve prices, making insufficient spectrum available for auction, while also providing a lack of clarity on future releases or the process of renewing expiring licences. Such factors can create uncertainty, artificial scarcity of spectrum and encourage excessive bidding above operators' true valuations of the licences on offer.

Spectrum is a valuable asset and governments have the option to use it to raise revenues to fund vital state activities. However, the primary goal in all awards should be to encourage the most efficient use of spectrum through investment in widespread, high-quality networks. Many countries around the world successfully strike the right balance between raising revenues and delivering efficient spectrum awards. To do this, the GSMA recommends that governments and regulators:

1. Set modest reserve prices and annual fees, and rely on the market to set prices.
2. License spectrum as soon as it is needed, so as to avoid artificial spectrum scarcity.
3. Avoid measures which increase risks for operators, forcing them to overbid for spectrum.
4. Publish long-term spectrum award plans that prioritise welfare benefits over state revenues.

### India: Enough Spectrum Made Available but Hooked on High Reserve Prices

In a 2015 auction, the main Indian carriers had competed intensely to retain their existing spectrum holdings. However, when fresh spectrum was made available in a 2016 auction across the 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2300 MHz and 2500 MHz bands, they were not forced to compete as fiercely. Nevertheless, the TRAI set the reserve price for 700 MHz, in particular, at an extremely high level, having based it on 1800 MHz prices achieved in the hotly contested 2015 auction (the 700 MHz price being four times what was paid for 1800 MHz). As a result, the final revenues from the auction were less than anticipated — only $9.9 billion of total revenues as opposed to $85 billion of total reserve prices. There were no bids for the 700 MHz band and bids for 850 MHz, 2100 MHz and 2500 MHz spectrum were also very limited, with many blocks in several circles unsold. The entire 2300 MHz spectrum was sold and 80 per cent of 1800 MHz spectrum that was put up for auction was also sold.

### Thailand: Expensive Rationed Spectrum Hampers Investment

In 2015, Thailand auctioned 1800 MHz spectrum in November, followed by 900 MHz spectrum in December. The winning bids in the December auction were almost six times the reserve price for the 900 MHz spectrum and more than double the final proceedings for the 1800 MHz spectrum auction. In total, the auction of just 100 MHz of spectrum raised THB232.73 billion (US$6.52 billion), making the winning bids among the highest in the world on a per-MHz per-capita basis. The Thailand auctions demonstrate what can happen in markets where spectrum is artificially rationed and there is no clear roadmap for its release. Although the auctions raised huge funds for the Thai government, they have dramatically reduced the Thai operators' ability to invest in their networks and services. This is likely to hold back the development of Thailand's digital economy and the country runs the risk of falling behind other countries in South East Asia.

In the words of Brett Tarnutzer, Head of Spectrum, GSMA, "Acquiring spectrum is only the first step before making the necessary investment in network deployment to deliver mobile services to consumers. Unreasonably high reserve prices lead to spectrum remaining unsold, delays in the delivery of mobile services and, ultimately, an increase in consumer tariffs."

1 GSMA & NERA Economic Consulting Report: Effective Spectrum Pricing — Supporting Better Quality and More Affordable Mobile Services, 2017

2 Ibid NERA, 2017

3 GSMA Report: Spectrum Pricing in Developing Countries — Evidence to Support Better and More Affordable Mobile Services, 2018

# Spectrum for Drones (UAVs)

## Background

Unmanned Aerial Vehicles (UAVs), or drones as they are commonly referred to, have the potential to deliver profound socio-economic benefits. These range from transforming how businesses deliver their products to supporting life-saving services such as drug delivery in remote areas. However, this is all contingent on effective UAV authentication, monitoring and connectivity.

In Europe alone there are expected to be over 400,000 commercial and government UAVs by 2050.[1] Current aeronautical communication systems are not designed to manage such a huge new fleet of vehicles, nor can they enable them to operate effectively in built-up urban areas and support high-bandwidth traffic such as streaming video.

Mobile networks already provide wide area broadband connectivity and sim cards are a trusted authentication mechanism. Trials have shown that terrestrial mobile networks are able to safely support UAV connectivity at altitudes of at least 400 feet.[2] Mobile networks can also provide the connectivity to support an air traffic management system for UAVs, as well as enabling no-fly zones and issuing commands such as flight path updates.

But these significant benefits can only be realised if regulators remove barriers in the way of using of mobile networks to support UAVs — most notably those associated with the use of licensed mobile spectrum.

## Debate

*Should regulators permit licensed mobile spectrum to be used for UAV connectivity?*

---

## Industry Position

**Licensed mobile spectrum enables widespread, high-quality connectivity for UAVs with sufficient capacity to support competitive services and rising usage levels.**

Mobile services in licensed bands are well established worldwide in mature networks, so could be used to support UAV connectivity today if permitted by regulators. Mobile operators typically have exclusive access to coverage spectrum (i.e., below 1 GHz) to reliably cover very wide areas and capacity spectrum (i.e., above 1 GHz bands) which supports very fast data speeds. Taken together this means operators can support very safe, reliable, wide-area broadband connectivity for UAVs.

Another benefit of licensed mobile spectrum is that it can support affordable UAV connectivity worldwide. Mobile spectrum bands are often harmonised regionally or globally, so economies of scale already exist to support affordable radio equipment for UAVs.

It is therefore essential that there are no unnecessary barriers to using licensed mobile spectrum for UAV connectivity. Restrictions could damage the significant benefits cellular connectivity delivers. This could happen, for example, if regulators decide that mobile spectrum licences may not be used to provide connectivity to devices that are 'off the ground'. Similarly, if regulators choose to classify mobile services for UAVs as an 'aeronautical mobile service' then the bands mobile operators can use may be restricted. This would adversely affect the coverage and capacity of the resulting LTE services, as well as competition in markets to provide such services.

It is not clear that any such restrictions on the use of mobile spectrum would be justified given there is no evidence that mobile-connected UAVs present interference concerns to other wireless services.

Regulators should also adopt a service and technology neutral framework to fully support UAVs. It is essential that governments provide a regulatory framework for licensed spectrum that facilitates the development and growth of UAV connectivity, and does not impose service or technological restrictions that hold back innovation. Operators should not be prevented from deploying any mobile technology in their spectrum to support UAVs. Spectrum licences which are technology specific may limit the ability to provide high-speed data connectivity for UAVs (e.g., 3G or 4G), or new IoT-specific cellular technologies that could provide simple narrow-band authentication and identification (e.g., NB-IoT or LTE-M).

1 SESAR, European UAVs Outlook Study, 2016.
2 Several trials have taken place including those held by Nokia and Qualcomm.

Resources:
GSMA Drones website
GSMA Public Policy Position: Mobile Spectrum for Unmanned Aerial Vehicles
Qualcomm Technologies: LTE Drone Trial
SESAR Report: European Drones Outlook Study

# Spectrum for IoT

## Background

The Internet of Things (IoT) is a hugely important and rapidly growing market with the potential to transform the digital economy. Mobile services play an important role in the wide-area IoT market and are evolving to meet a growing array of different requirements. For example, the key markets for mobile IoT solutions include the utility, medical, automotive and retail sectors. This is in addition to current consumer electronics devices, including e-book readers, GPS navigation aids and digital cameras.

According to data from GSMA Intelligence, the total number of IoT connections is predicted to grow from just over nine billion (9.1 billion) in 2018 to 25 billion by 2025, with the total IoT revenue opportunity worth $1.1 trillion by 2025.

The bulk of the machine-to-machine (M2M) market (92 per cent) uses short-range, unlicensed connections (e.g., Wi-Fi and ZigBee), while the wide-area market is heavily reliant on mobile connectivity. Licenced cellular IoT connections (cellular M2M and licenced LWPA) are expected to grow from 1.1 billion in 2018 to 3.5 billion by 2025.

The requirements of wide-area IoT services vary much more widely than those for traditional mobile services. As a result, mobile technology standards are continuously evolving to support these use cases, which is driving innovation and ensuring that mobile IoT is increasingly well placed to compete effectively with other IoT solutions.

The latest mobile standard — 3GPP Release 13 — supports all the key requirements for mobile IoT technologies, including: long battery life, low device cost, low deployment cost, widespread coverage and support for a massive number of devices.

The mobile industry already plays a significant role in the wide-area M2M market — most notably via GSM systems for low-bandwidth applications, such as vending machines, and through 3G and 4G-LTE for high-bandwidth applications such as streaming video.

## Debate

*How can governments and regulators use spectrum policy to incentivise the rapid roll out of IoT services?*

---

*What are the benefits of using licensed spectrum for IoT?*

---

## Industry Position

**Licensed spectrum is vital in order to deliver the most reliable IoT services. This is because of its unique ability to support quality of service guarantees over wide areas, as networks using licensed spectrum are not at risk of interference and operators can control usage levels on their networks.**

As a result, licensed mobile IoT may be the only choice for services that require concrete assurance levels, such as security and medical applications.

Licensed spectrum has the capacity and coverage capabilities to support IoT growth. Crucially, the IoT technologies included in the latest mobile standard, Release 13, significantly build on the coverage capabilities of existing spectrum.

The viability of mobile IoT is contingent on governments adopting a positive regulatory framework, especially as it pertains to mobile spectrum. This type of framework must not impose service or technological restrictions that hold back innovation. Instead it should be designed to nurture evolution in the capabilities of mobile networks and allow the market to decide which solutions will thrive.

International spectrum harmonisation is vital for the development of a global, affordable mobile IoT market. This is because it enables the development of mass-market, low-cost mobile IoT devices, through the creation of an addressable market that is large enough to support manufacturing economies of scale.

Harmonised mobile spectrum is needed to support all wide-area IoT use cases, including coverage bands for Low-Power Wide-Area (LPWA) use cases and capacity bands for high-bandwidth applications like video streaming.

Regulators should work with the mobile industry to support IoT in 5G spectrum planning, as 5G is expected to play an important role in the evolution of mobile IoT.

Resources:
GSMA Public Policy Position: Internet of Things
GSMA Guide: The Internet of Things
GSMA Video: The Internet of Things — A World of Opportunity

# Spectrum Harmonisation

## Background

Spectrum harmonisation refers to the uniform allocation of radio frequency bands, under common technical and regulatory regimes, across entire regions. A country's adherence to internationally identified spectrum bands offers many advantages:

- Lower costs for consumers, as device manufacturers can mass-produce devices that function in multiple countries on a single band.
- Availability of a wider portfolio of devices, driven by a larger, international market.
- Roaming, or the ability to use a mobile device abroad.
- Fewer issues of cross-border interference.

At the World Radiocommunication Conference (WRC) in 2015 in Geneva, agreement was reached on the creation of three global spectrum bands for mobile — 700 MHz, 1427-1518 MHz and 3.4-3.6 GHz. The outcome provides the industry with an important mix of internationally harmonised coverage and capacity spectrum to meet the growing demand for mobile services. Spectrum harmonisation through the WRC process is also key to enabling lower-cost mobile devices through economies of scale.

## Debate

*How harmonised does a band need to be to realise the benefits of harmonisation?*

---

*Can a national market be so large that the benefits of spectrum harmonisation are inconsequential?*

---

*In the future, will cognitive technologies enable devices to tune dynamically to any band removing the need for countries to harmonise?*

---

## Industry Position

**Governments that align national use of the spectrum with internationally harmonised band plans will achieve the greatest benefits for consumers and avoid interference along their borders.**

At a minimum, harmonisation of mobile bands at the regional level is crucial. Even small variations on standard band plans can result in device manufacturers having to build market-specific devices, with costly consequences for consumers.

All markets should harmonise regionally where possible, as this benefits the entire global mobile ecosystem. There is no advantage in going it alone.

Cognitive radio technologies will not reduce the need for harmonised mobile spectrum anytime soon. Adhering to internationally recognised band plans is the only way to achieve large economies of scale.

*Twenty-eight different approaches to manage radio frequencies in the EU do not make economic sense in the Digital Single Market… We propose a joint approach to use the 700 MHz band for mobile services. This band is the sweet spot for both wide coverage and high speeds. It will give top-quality internet access to all Europeans, even in rural areas, and pave the way for 5G, the next generation of communication network.*

— Andrus Ansip, Vice-President for the Digital Single Market, European Commission, 2016

Resources:
GSMA & Boston Consulting Group Report: The Economic Benefits of Early Harmonisation of the Digital Dividend Spectrum and the Cost of Fragmentation in Asia-Pacific
GSMA & Plum Consulting Report: The Benefits of Releasing Spectrum for Mobile Broadband in Sub-Saharan Africa
GSMA Report: Economic Benefits of the Digital Dividend for Latin America

Deeper Dive

## World Radiocommunication Conference 2019 (WRC-19)

Spectrum harmonisation has created economies of scale for existing generations of mobile networks, which in turn have made mobile services and handsets more affordable. To become a success, widely harmonised mobile spectrum is again needed to ensure 5G meets its future expectations and delivers the full range of affordable services.

5G networks require spectrum within three key frequency ranges: sub-1 GHz, 1-6 GHz and above 6 GHz. The availability of widely harmonised spectrum for 5G in the latter frequency range will depend to a large extent on the decisions made at WRC-19. This spectrum is needed for 5G to be able to offer multi-gigabit per second (Gbps) data rates and to support very low latency (sub-1 ms).

The work at WRC-19 includes Agenda Item 1.13 (AI 1.13), which looks at spectrum for mobile broadband between 24.25 and 86 GHz. In total, eight frequencies are being considered:

### Frequencies being considered under Agenda Item 1.13

- 24.25-27.5 GHz
- 31.8-33.4 GHz
- 37-43.5 GHz
- 45.5-50.2 GHz
- 50.4-52.6 GHz
- 66-71 GHz
- 71-76 GHz
- 81-86 GHz

The GSMA advocates for identification of the 26 GHz, 40 GHz and 66 GHz bands. The 26 GHz band (24.25-27.5 GHz) is already gaining traction and has been chosen in Europe as a ‘pioneer band’. Africa, the Middle East, Asia, member countries of RCC and parts of the Americas are also planning to use this band for 5G. Identifying the band for IMT at WRC-19 sets the stage for harmonisation and helps build the scale necessary for low-cost devices and services. There are also technical and economic benefits. For example, as the 26 GHz band is adjacent to the 28 GHz band, it allows for economies of scale and early equipment availability. The 28 GHz band will be used as the first millimetre-wave 5G band in the US, Korea, Japan and Canada, with implementation done outside of the WRC-19 process and under an existing mobile allocation.

The GSMA also supports the identification of 37-43.5 GHz (known as the 40 GHz band) for IMT. Identifying the whole band for IMT at WRC-19 allows for flexibility. For example, it lets different countries and regions choose which part of the band to implement.

Another band that holds strong interest for the mobile industry is 66-71 GHz. The decision by the Federal Communications Commission in the US to use this band for 5G adds momentum to the existing support for this band in Europe, Africa and member countries of RCC. The GSMA supports the identification of the 66-71 GHz band for International Mobile Telecommunications (IMT) and believes it should be available for use by 5G systems with flexibility to allow for different licensing regimes, thus enabling its use by both IMT and non-IMT technologies.

It is important to remember that the WRC process is a long-term endeavour. Spectrum identified at WRC-19 will be in use for decades to come, so it is important to get involved and ensure the details are correct now, irrespective of when the first commercial 5G services will be launched.

WRC-19 runs from 28 October to 22 November 2019. Here are the GSMA’s recommendations on how to succeed at the conference:

- Advocate positions as much as possible at national and regional levels before the conference.
- Familiarise yourself with the process and structure of the conference to make it easier to follow the agenda items.
- Know who you can ask for help on important issues.
- Keep track of who is on your side and, even more importantly, who is not, on each issue; getting to know the opposition and what can be offered is key.
- Have fall-back positions ready if the optimum outcome can’t be reached.
- Don’t assume that decisions are just rubber stamped by the plenary during the last couple of days.
- Manage energy levels — the WRC is a marathon, not a sprint: prioritisation is key to a successful outcome.

Learn more about the WRC process at: www.gsma.com/spectrum/wrc-intro

# Spectrum Licensing

## Background

Spectrum licensing is central to the delivery of high-quality mobile broadband services and long-term, heavy investment in networks.

The amount of spectrum made available and the terms on which it is licensed fundamentally drive the cost, range and quality of mobile services.

Mobile is a capital-intensive industry requiring significant investment in infrastructure. Governments' spectrum licensing policies — when supported by a stable, predictable and transparent regulatory regime — can dramatically raise the attractiveness of markets to investors.

Spectrum management for mobile telecommunications is complex, as governments release new spectrum in existing mobile bands; manage the renewal of licences coming to the end of their initial term; and release spectrum in new bands for mobile broadband services.

## Debate

*What is the most effective way to license spectrum?*

---

*What conditions should be tied to spectrum-access rights?*

---

*Are licensing rules the best way to ensure a healthy, well-functioning mobile sector, or should the development of the industry be shaped predominantly by market forces?*

---

## Industry Position

**Spectrum rights should be assigned to the services and operators that can generate the greatest benefit to society from the use of that spectrum.**

Regulatory authorities should foster a transparent and stable licensing framework that prioritises exclusive access rights, promotes a high quality of service and encourages investment.

Licensing authorities should publish a road map of the planned release of additional spectrum bands to maximise the benefits of spectrum use. The road map should take a five- to ten-year view and include a comprehensive and reasonably detailed inventory of current use.

Restrictive licence terms and conditions limit operators' abilities to use their spectrum resources fully, and risk delaying investment in new services. In particular, service and technology restrictions in existing licences should be removed. New licences should be at least 15-20 years in length to encourage significant investment in networks, including in rural areas.

To the maximum practical extent, spectrum should be identified, allocated and licensed in alignment with internationally harmonised mobile spectrum bands to enable international economies of scale, reduce cross-border interference and facilitate international services.

For new spectrum allocations, market-based approaches to licensing, such as auctions, are the most efficient way to assign spectrum to the bidders that value the spectrum the most.

The primary goal in all awards should be to encourage the most efficient use of spectrum through investment in widespread, high-quality networks. Efforts to use awards to raise excessive revenues, such as through high auction reserve prices or annual fees, have been linked to negative consumer outcomes through reduced network investment and increased prices. Instead, auction reserves should be set conservatively to let the market determine the price and licence fees should be limited to recovering the administrative costs of spectrum management.

Resources:
GSMA & CEG Report: Best Practice in Mobile Spectrum Licensing
GSMA & NERA Report: Effective Spectrum Pricing — Supporting Better Quality and More Affordable Mobile Services
GSMA Public Policy Position: Licence Renewal

# Spectrum Licence Renewal

### Background

Many of the original 2G spectrum licences are coming up for renewal in the next few years. National regulatory authorities must determine how mobile operators' spectrum rights will be affected as licences approach the end of their initial term.

The prospect of licence expiry creates significant uncertainty for mobile operators. A transparent, predictable and coherent approach to renewal is therefore important, enabling operators to make rational, long-term investment decisions.

There is no standard approach to relicensing spectrum. Each market needs to be considered independently, with industry stakeholders involved at all stages of the decision process. Failure to effectively manage the process can delay investment in new services, potentially affecting mobile services for millions of consumers.

### Debate

*Which approach to spectrum licence renewal will have the most beneficial outcome for consumers and society?*

---

*Should spectrum licence holders presume they will have the option to renew when the licence reaches the end of its term, unless otherwise specified in the licence?*

---

*Should governments feel free to reshuffle spectrum allocations, change bandwidths or alter licence conditions on renewal?*

---

### Industry Position

**It is essential that governments and regulators implement a clear and timely process for the renewal of spectrum licences.**

Maintaining mobile service for consumers is critical. To ensure this, the approach for licence renewal should be agreed at least three to four years before licence expiry.

Governments and regulators should work on the presumption of licence renewal for the existing licence holder. Exceptions should only apply if there has been a serious breach of licence conditions in advance of renewal.

Should a government choose to reappraise the market structure at the time of renewal, the priorities should be to maintain service for consumers and ensure network investments are not stranded. Governments should not discriminate in favour of, or against, new market entrants, but establish a level playing field.

New licences should be granted for 15 to 20 years, at least, to give investors adequate time to realise a reasonable return on their investment.

Renewed mobile licences should be technology and service neutral.

Resources:
GSMA Public Policy Position: Licence Renewal
GSMA & CEG Report: Licensing to Support the Mobile Broadband Revolution

# Spectrum Sharing

### Background

Continually rising data traffic means mobile services must rely on access to growing amounts of spectrum to meet demand. However, completely clearing new frequency bands for future mobile use has become increasingly difficult. When clearing a band is not possible, spectrum sharing may offer a way to help by enabling mobile access to additional bands in areas, and at times, when other services are not using them.

Sharing is only possible if regulations do not prohibit it, commercial measures incentivise it, and it is technically practical (i.e., different users can operate effectively without interference). Regulators can enable sharing by giving incumbent users the right to share their spectrum voluntarily through sharing agreements or by awarding rights to use spectrum in areas and/or at times when the incumbent is not using it. Sharing will impose opportunity costs on incumbents, so they will generally need to be remunerated for sharing their spectrum, especially if they have paid for access.

Policymakers increasingly see spectrum sharing as a means of opening up additional spectrum for 4G and 5G mobile services. Their decisions regarding bands and frameworks for sharing are likely to have a significant impact on the quality and coverage of these services, as well as the level of investment mobile operators and other users are willing to make in them.

### Debate

*What role can spectrum sharing play alongside traditional spectrum management approaches, such as exclusively licensed spectrum and unlicensed spectrum?*

---

*What spectrum sharing frameworks could be used to enable mobile services and how would they impact investment in these services?*

---

### Industry Position

**Spectrum sharing is an opportunity to open up access to new spectrum for mobile services but needs careful planning to succeed. It is essential that the approach chosen protects the needs of incumbents, supports the needs of new users, and avoids limiting the future evolution of the band including possible repurposing.**

Exclusive licensing has been central to the success of mobile services and must continue. Spectrum sharing is a complementary, not an alternative, approach.

Sharing will only be useful for operators if the proposed band is harmonised for mobile use and is available and usable in sufficient quantities in areas and at times where needed.

Mobile operators favour a simple sharing framework that is investment-friendly and supports reliable, high-quality mobile services. Complex sharing frameworks, such as those with three tiers, are likely to be less desirable to mobile operators. They may limit the amount of spectrum for prioritised licensed access — which may make a band unsuitable for 5G — and introduce conditions (e.g. relatively low power limits, small licence areas, short licences) that restrict deployment options (e.g. for macrocells or fixed wireless access) and discourage significant long-term wide-area network investment.

Mobile operators should be permitted to voluntarily share spectrum to support faster services, improve coverage and drive innovation. They should also be permitted to voluntarily establish commercial agreements to lease spectrum to other types of operators (e.g. verticals or rural wireless internet service providers). However, it should be noted that sharing may not always be possible in areas where it is currently unused. This can be due to future planned use of the band or because the required coordination or synchronisation measures may undermine good-quality services.

Sharing can play a role in the 5G era but poor implementation risks harming its potential. Mobile operators will need a core foundation of exclusively licensed 5G spectrum, including in millimetre wave bands, to support wide-area services, heavy network investment and good quality of service. Sharing can play a complementary role if the band and sharing framework is carefully designed. If sharing means an insufficient amount of licensed spectrum is available to mobile operators where and when they need it then sharing may limit, or eliminate, the potential for 5G in the band.

Spectrum sharing will not succeed unless incumbent users are encouraged to share their spectrum in areas where it is underused and there is clear, and commercially viable, demand from other users.

Sharing should balance the current and future requirements of incumbents and sharers. The success of spectrum management has been contingent on providing reliable, guaranteed access to spectrum users to allow long-term investment and enable technology evolution. It is vital sharing does not undermine this success.

Resources:
GSMA Public Policy Position: Spectrum Sharing
GSMA & Deloitte Report: The Impact of Licensed Shared Use of Spectrum
AT&T Public Policy blog: The Power of Licensed Spectrum

Deeper Dive

## Spectrum Sharing Models

Licensed use of spectrum, on an exclusive basis, is a time-tested approach for ensuring that spectrum users — including mobile operators — can deliver a high quality of service to consumers without interference. However, as demand for spectrum increases there is growing interest in exploring spectrum sharing.

There are a variety of frameworks that can be used to implement sharing. These frameworks control who can share the band and define respective usage rights and limitations. The key variables usually include:

**The number of access tiers:**

A one-tier model typically grants everyone the same usage rights. Two-tier models include the incumbent and one class of shared user. Some models add a third tier with further reduced access rights (e.g., low-power uses).

**Access guarantees:**

The framework outlines the access guarantees that the tiers of users can expect. These can include traditional licensing to provide strong guarantees and high quality of service.

**Access terms, technical conditions and fees (if any):**

These define the geographic area over which users may operate and, where necessary, for how long and at what cost (e.g., when a tier is licensed). They also include technical conditions (e.g., power levels) which affect coverage.

**TV white space:**

Television spectrum in the UHF band that, due to predictable geographical or temporal gaps in TV broadcasting, offers the potential for licence-exempt devices to use the spectrum for broadband services — but usage is typically controlled through a database.

**CBRS-type approaches:**

The planned 'Citizens Broadband Radio Service' approach in the United States in the 3.5 GHz band aims to support three tiers using dynamic sharing. The top tier are the incumbents (e.g., radars, satellite companies and wireless ISPs) who have the most protection. The secondary tier are Prioritised Access Licence (PAL) holders, who will pay to buy rights to use a portion of the available spectrum where it is not in use by the top tier. The third tier is for General Authorised Access (GAA) and is available to anyone but will have the least protection. Portions of the spectrum are reserved for GAA and PAL tiers in areas where the incumbent is not using the spectrum. PAL and GAA users can access each other's reserved portion of spectrum where it is not registered as being used in the Spectrum Access System (SAS) database.

**Licensed Shared Access:**

Incumbent licence holders can sub-license spectrum to other users in a controlled way. The traditional model was developed in Europe for the 2.3 GHz band. It has two tiers including the incumbent and secondary users (e.g., mobile operators) who are permitted to use the spectrum in areas when it is available. More advanced models are being developed.

**Concurrent Shared Access (e.g., club licensing):**

Unlike the approaches above, this only allows one class of user but allows them to share spectrum with each other in a coordinated way. This could allow sharing between mobile operators to improve data speeds and spectrum efficiency.

**Licence-exempt spectrum (aka unlicensed spectrum):**

A one-tier approach where the band can be used by multiple systems and services if they meet predefined 'politeness protocols' and technical standards. Wi-Fi is a technology that uses licence-exempt spectrum.

# Spectrum Trading

## Background

Spectrum trading is a mechanism by which mobile network operators can transfer spectrum-usage rights on a voluntary commercial basis.

Trading spectrum-usage rights is a relatively recent development. In Europe, most countries that allow the practice have done so since 2002 or later, and each country has established different rules governing the practice.

Trading rules can facilitate the partial transfer of a usage right, which could permit a licensee to use a specified frequency band at a particular location or for a certain duration. This may result in more intensive use of the limited spectrum.

## Debate

*Should spectrum-trading arrangements between operators be allowed?*

*What role should regulators play in overseeing such arrangements?*

*What regulatory procedures are required to ensure transparency and notification of voluntary spectrum trading?*

## Industry Position

**Countries should have a regulatory framework that allows operators to engage in voluntary spectrum trading.**

Spectrum trading creates increased flexibility in business planning and ensures that spectrum does not lie fallow, but instead is used to deliver valuable services to citizens.

Spectrum-trading restrictions should only be applied when competitive or other compelling concerns are present.

Spectrum-trading agreements are governed by commercial law and subject to the rules applicable to such agreements. They may also be subject to assessment under competition law.

It makes sense for governments to be notified of spectrum-trading agreements and to grant approval. Notification requirements preserve transparency, making it clear which entities hold spectrum-usage rights and ensuring that trading arrangements are not anti-competitive.

Governments should implement appropriate and effective procedures for handling notification requests of spectrum-trading agreements.

Resources:
GSMA Public Policy Position: Spectrum Trading
GSMA Response: RSPG Public Consultation on Secondary Trading of Rights to Use Spectrum
CEPT & CEE Report: Description of Practices Relative to Trading of Spectrum Rights of Use

# Technology Neutrality and Change of Use

## Background

Technology neutrality is a policy approach that allows the use of any non-interfering technology in any frequency band.

In practice, this means that governments allocate and license spectrum for particular services (e.g., broadcasting, mobile, satellite), but do not specify the underlying technology used (e.g., 3G, LTE or WiMAX).

Many of the original mobile licences were issued for a specific technology, such as GSM or CDMA, which restricts the ability of the licence holder to 'refarm' the band using an alternative, more efficient technology.

Refarming refers to the repurposing of assigned frequency bands, such as those used for 2G mobile services (using GSM technology) for newer technologies, including third-generation (UMTS technology) and fourth-generation (LTE technology) mobile services.

Spectrum allocations for international mobile telecommunications (IMT) are technology neutral. IMT technologies — including GPRS, EDGE, UMTS, HSPA, LTE and WiMAX — are standardised for technical coexistence.

## Debate

*Should governments set the technical parameters for a band's use or should the market decide?*

*Should licence conditions restrict operators' ability to deploy more efficient technologies and adapt to market changes?*

*How is spectrum coexistence best managed to prevent interference between services and operators using different technologies?*

*In Mexico, we are technologically neutral, so operators can innovate and offer better services to consumers.*

— Mario Fromow, Commissioner at Instituto Federal de Telecomunicaciones, Mexico, August 2018

## Industry Position

**We support a licensing approach that allows any compatible, non-interfering technology to be used in mobile frequency bands.**

Adopting harmonised, regional band plans for mobile ensures that interference between services can be managed. Governments should allow operators to deploy any mobile technology that can technically coexist within the international band plan.

Technology neutrality encourages innovation and promotes competition, allowing markets to determine which technologies succeed, to the benefit of consumers and society.

Governments should amend technology specific licences to allow new technologies to be deployed, enabling operators to serve more subscribers and provide each subscriber with better, more innovative services per unit of bandwidth.

Enabling spectrum licence holders to change the underlying technology of their service, known as refarming, generates positive economic and social outcomes and should be allowed.

Resources:
GSMA Public Policy Position: Change of Use of Spectrum
GSMA & CEG Report: Licensing to Support the Broadband Revolution

Deeper Dive

## The 1800 MHz Band: A Global Refarming Success Story for LTE

The lack of truly global LTE frequency bands made it difficult to establish a wide range of low-cost devices for the first phase of 4G services. It also prevented widespread international roaming.

Because mobile devices can only support a limited number of frequency bands, a lack of harmonised bands means devices can only operate and be sold in a limited number of markets. This problem was highlighted when several early 4G-enabled Apple devices could not operate on some 4G networks around the world, as they did not support the right frequency bands.

A critical part of the solution has been the 1800 MHz band, which has traditionally been used for 2G GSM services. The band has historically been one of the key enablers of low-cost devices and international roaming, as it is one of the only bands to be harmonised worldwide.

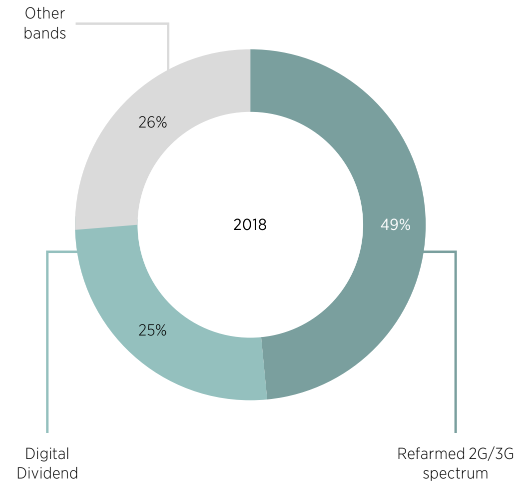
In countries where regulators support technology neutral spectrum licences, operators have been able to refarm the 1800 MHz band for LTE services. The 1800 MHz band is now the most widely deployed LTE band globally, as well as the most widely supported in mobile devices. According to the Global Mobile Suppliers Association (GSA), the 1800 MHz band has the largest device ecosystem of any LTE band, with over 6,171 compatible user devices available as of December 2017.

## Technology and Service Neutrality Incentivises the Adoption of New Technologies

Restricting the use of spectrum to particular technologies and services exacerbates the problem of scarcity of spectrum and prevents customers from gaining access to new services. Removing restrictions that limit the use of spectrum to particular services or technologies (beyond those needed to manage interference) enables a country to maximise the benefits from its spectrum resources on an ongoing basis. Operators' ability to introduce new, more spectrally efficient, mobile technologies (including LTE, LTE Advanced and in future 5G) will be critical to meeting exponential growth in demand for mobile data services. A number of countries only allow for licences to be made technology neutral after the payment of fees. High charges for amending licences to make them technology and service neutral risks delaying the benefits of new technology reaching end users.

### Mapping 4G-LTE Deployments by Frequency Bands

As of July 2018, 675 operators worldwide have live LTE networks, covering 208 countries. More LTE deployments are now using new bands assigned to mobile service, such as AWS or the 2.3-2.6 GHz frequencies.




| Breakdown of bands | MHz |
|---|---|
| Digital Dividend | 700, 800 |
| Refarmed 2G/3G | 850, 900, 1500, 1800, 1900, 2100, 1700/2100 |
| Other bands | 450, 2300, 2500, 2600, 3500, 3600, 3700, 5000, 5800 |

Source: GSMA Intelligence

# TV White Space

## Background

Today, several approaches are being explored to help improve broadband coverage in rural areas, including gaps that might exist between licensed spectrum users. The expression ‘white space’ is often used to describe these gaps. They are parts of a spectrum band that are not used at a given time in a geographical location.

TV white space (TVWS) describes spectrum in the television broadcasting bands (470–790 MHz in Europe and 470–698 MHz in the Americas, for example). Because of necessary geographical separation between television stations on the same and adjacent channels, there are varying amounts of unused spectrum.

The actual amount depends on the number of TV stations in a specific area and nearby areas. It is worth noting that commercially desirable geographic locations, such as major urban and suburban areas with high population and business densities, typically have little, if any, TV white space at all.

## Debate

*What approach should regulators take to TVWS?*

---

*What challenges do TVWS networks face?*

---

*What role can the technology play in helping connect everyone and everything?*

---

*The over-eager pursuit of unlicensed sharing models cannot turn a blind eye to the model proven to deliver investment, innovation, and jobs — exclusive licensing. Industry and government alike must continue with the hard work of clearing and licensing underutilised government spectrum where feasible.*

— Joan Marsh, Executive Vice President of Regulatory and State External Affairs, AT&T

## Industry Position

**TVWS networks make opportunistic use of white spaces to provide generally small-scale services on a secondary and unlicensed basis. These services aren’t allowed to interfere with TV signals, the primary users of the spectrum. Since the spectrum is shared, devices can only operate if white space is available and other TVWS devices aren’t using it already. As such, there is no guarantee users will be able to stay connected or connect at all.**

For TVWS to work, careful avoidance of interference is needed with primary licensees such as existing TV broadcasters and other TVWS devices and services in adjacent bands. Even in the most developed markets this technology hasn’t yet been proven.

The roll out of TVWS services should not be allowed to disrupt the licensing of the Digital Dividend bands for mobile broadband services (i.e., 800 MHz, 700 MHz and increasingly the 600 MHz band, too).

The Digital Dividend is central to extending commercially proven mobile broadband services across whole countries, including rural areas.

The advantages of licensed mobile services over the secondary unlicensed approach of TVWS include: a more mature and developed ecosystem, better reliability, higher quality of service and increased coverage (due to higher power limits for licensed devices).

New regulatory and technical solutions are needed to connect everyone. TVWS networks can be used to provide backhaul for Wi-Fi hotspots in rural areas where there is no cellular connectivity.

Still, they face challenges related to the availability of equipment, cost and quality of service. Public authorities must carefully consider this when making long-term decisions about spectrum allocations. The same is true when considering how best to meet future broadband goals.

Resources:
GSMA Public Policy Position on TV White Space
GSMA Public Policy Position on Spectrum Sharing
GSMA Europe Response to Radio Spectrum Policy Group 2010 Work Programme
AT&T Public Policy Blog: The Power of Licensed Spectrum

# Consumer Protection

With the growing economic and social importance of mobile services, particularly the mobile internet, there is a corresponding need to ensure the more than five billion people currently connected via these services can continue to enjoy them safely and securely. The challenge is providing this protection while also ensuring users have control over their privacy and personal data.

It is essential for the mobile industry, therefore, to deliver safe and secure technologies, services and apps that inspire trust and confidence. At the same time, there is a need to educate consumers about potential risks and raise awareness of the steps they can take to avoid those risks.

The mobile industry takes consumer protection seriously. The GSMA and its members play a leading role in developing and implementing appropriate safety and security solutions, technical standards and protocols. They also work with governments, multilateral organisations and non-governmental organisations to address concerns related to consumer protection by:

- Defining, sharing and promoting global best practice.
- Building and participating in cross-sector coalitions.
- Educating consumers and businesses in the safe use of mobile technologies and applications.
- Commissioning research that offers real-world insight and evidence.

The following pages provide a small indication of the work undertaken by the mobile industry to ensure consumers continue to be appropriately protected and informed as they enjoy the full range of benefits that mobile technology makes possible.

# Addressing Cybersecurity Challenges

The internet and mobile connectivity have become ever-more pervasive and embedded in daily life, so there is a corresponding need to ensure people can continue to use these increasingly essential services safely and securely. The mobile industry has worked to educate consumers while incorporating new features and enhancing existing security capabilities such as encryption, integrity checking and user identification validation into mobile services, minimising the potential for fraud, identity theft and other possible threats.

Governments and policymakers have put in place measures to prevent cyberattacks, which are not only harmful and criminal, but undermine trust in digital services. National and regional strategies have been adopted in many countries to strengthen resilience, build capacity and fight cybercrime.

'Cybersecurity' is not often clearly defined[1] and can cover a number of areas. Generally, it refers to the protection, by any means, of network-related systems and devices and the software and data they contain. As such, cybersecurity typically comprises the protection of technical infrastructure, procedures and workflows, physical assets, national security as well as the confidentiality, integrity and availability (CIA triad) of information.

The mobile industry has a long history of providing secure products and services to its customers in the following ways:[2]

- **Protecting network infrastructure and devices.** Operators are constantly improving standards, deploying better versions of technology, identifying risks and reducing vulnerabilities. They test networks for weaknesses and build their capacity to detect and deter malicious attacks on current-generation and future networks. The GSMA and its members support the principles of 'security-by-design' to be applied across the value chain.

- **Protecting public safety.** Mobile networks are considered to constitute critical national infrastructure in many jurisdictions and they play a key role in protecting the public, for example by enabling people to call emergency services. Operators have a legal obligation to assist law enforcement agencies, which they do while being supportive of human rights concerns.

- **Protecting consumers from fraud.** Fraudulent attacks take many forms, such as identity theft, financial fraud, phishing, SMiShing or vishing, where victims are tricked to reveal sensitive personal information and service access credentials. Operators implement solutions to prevent the use of networks to commit fraud and the use of devices to harm consumers.

- **Protecting consumer privacy.** Information security implies that information, including personal data, is not accessible or disclosed to unauthorised individuals, entities or processes, and that it is maintained, complete and available, throughout its life. The GSMA has done extensive work on data protection and data privacy.

Given that risks are dynamic and not confined to national borders, sustained, international multi-stakeholder cooperation is key in all areas of security to manage risks. Furthermore, robust security measures must be adopted by the entire digital value chain. Looking ahead, mobile operators and the GSMA will remain engaged in a number of activities, including:

- Continuing to invest in the security of their own networks, devices and services and building the capacity to detect and deter malicious attacks, improving preparedness and incidence response.

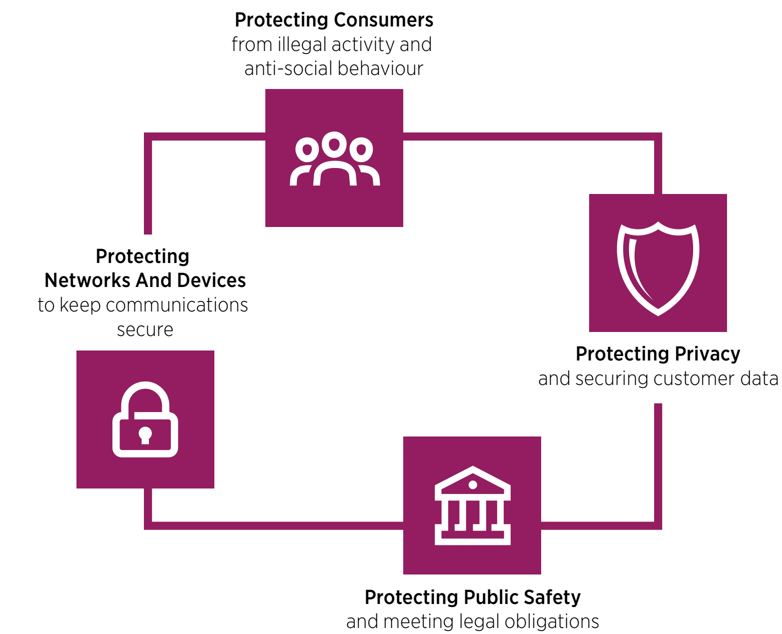
- Contributing to the development of globally recognised, industry-led, voluntary consensus security standards, assurance programmes and conformity assessment schemes.

- Participating in capacity building and in public-private partnerships to share best practices with other stakeholders.

1 A useful overview of definitions can be found in ENISA's report: Definition of Cybersecurity – Gaps and overlaps in standardisation.

2 GSMA Report: Safety, Privacy and Security Across the Mobile Ecosystem for All (2013).

**Personal privacy, security and data protection**



# Children and Mobile Technology

## Background

Young children and teenagers are enthusiastic users of mobile technology. Young people's knowledge of mobile applications and platforms often surpasses that of parents, guardians and teachers, and children now use social networking services more than their parents.

For growing numbers of young people, mobile technology is an increasingly important tool for communicating, accessing information, enjoying entertainment, learning, playing and being creative. As mobile technology becomes increasingly embedded into everyday life, mobile phone operators can play an important role in protecting and promoting children's rights.

Mobiles can be key enablers to access:

- Skills for employment.
- Enhanced formal and informal education and learning.
- Information and services to aid in health, well-being and support.
- Improved social and civic engagement.
- Opportunities to play and to be creative.

Mobile devices increasingly play a role in formal education and informal learning. In developing and rural areas, as well as places where certain people — girls in particular — are excluded from formal education, mobile connectivity offers new opportunities to learn.

Like any tool, mobile devices can be used in ways that cause harm, so children require guidance in order to benefit from mobile technologies safely and securely.

The mobile industry has taken active steps in the area of safe and responsible use of mobile services by children. The GSMA has played a leading role in self-regulatory initiatives dealing with issues such as parental controls, education and awareness.

## Debate

*What potential harm are children exposed to in the online environment?*

*How can all stakeholders navigate tensions between differing child rights in the digital world?*

*Our partnership with the GSMA is one of our most productive and engaging. Children everywhere are ever more digital and mobile; GSMA's leading-edge policy and practice on keeping children safe and productive in their ever-changing digital environments are vital in enhancing the knowledge and capacity of our member child helplines to prevent harm and respond to children and young people.*

— Sheila Donovan, Executive Director, Child Helpline International

## Industry Position

**Mobile devices and services enhance the lives of young people. This perspective needs to be embraced, encouraged and better understood by all stakeholders to ensure young people get the maximum benefits from mobile technology.**

Addressing safe and responsible use of mobile by children and young people is best approached through multi-stakeholder efforts.

Working closely with Unicef, the GSMA and its mobile operator members — as well as a range of other organisations including the International Centre for Missing and Exploited Children (ICMEC) and INHOPE — hold national and regional multi-stakeholder workshops on the issue. These workshops bring together policymakers, NGOs, law enforcement and industry, to facilitate the development of collaborative approaches to safe and responsible use of the internet.

Through its mYouth programme, the GSMA also works closely with Child Helpline International to foster collaboration between mobile operators and child helplines in promoting children's rights — in particular their right to be heard — and to work together on areas of mutual concern, such as safer internet.

The GSMA takes part in international initiatives related to safeguarding children online, including contributing to the ITU's Child Online Protection programme, and actively engages with governments and regulators looking to address this issue. Through its Capacity Building programme, for example, the GSMA helps policymakers better understand children's use of technology, and discusses strategies for encouraging young people to become positive, engaged, responsible and resilient users of digital technology.

Young people are critical to the evolution of the mobile sector as they represent the first generation to have grown up in a connected, always-on world. They are future consumers and innovators who will deliver the next wave of innovation in mobile.

Resources:
UNICEF Guidelines for Industry on Child Online Protection website
UNICEF Tools for Companies in the ICT Sector website
ICT Coalition website
GSMA mYouth website
GSMA and Child Helpline International: Internet Safety Resources
Global Kids Online: Research Results

Deeper Dive

### Collaboration in Action

Growing numbers of young people are leading digital lives, and when they encounter problems online many will reach out to child helplines for support and guidance.

And while many child helplines have already built up experience in this area, globally there is still a number of them who are in the early stages of development and would benefit from guidance on these issues. GSMA and Child Helpline International wanted to extend their support to child helplines that fall into the latter category by harnessing the experience of experts in this field from a range of stakeholder groups.

In May 2016, GSMA and Child Helpline International co-hosted an intensive one-day workshop. This session brought together expertise from the child helpline community, the Child Helpline International youth panel, mobile operators and other industry players, NGOs, child online safety experts — including a specialist child and adolescent psychiatrist — and law enforcement.

The workshop was used to kick-start the process for creating a series of high-level guides for child helpline counsellors and volunteers on nine of the more common or challenging digital issues that lead young people to seek advice from helplines. The nine guides were launched in November 2016 and cover: cyberbullying, discrimination and hate speech, grooming, illegal content, inappropriate content, privacy, sexual extortion, sexual harassment and unsolicited contact.

The guides were created with child helplines and their counsellors and volunteers in mind — in particular those for whom internet safety issues were relatively new or where counsellor guidance and training was still under development. Each guide was created using input from experts from a range of fields who then also reviewed and approved the content. The guides are purposely high level in order to accommodate differing local contexts, with each guide providing a definition and some examples of the issue, options for discussion with the child or a parent/carer, practical and technical advice, as well as any ‘red flags’ that counsellors should look out for.

Deeper Dive

### The 30th anniversary of the UN Convention on the Rights of the Child

The year 1989 was significant, as it marked both the agreement of the UN Convention on the Rights of the Child (UNCRC) and the birth of the World Wide Web.

The UNCRC sets out a number of child-specific needs and rights that children, everywhere, are entitled to in order to survive and thrive, to learn and grow, and to reach their full potential. It outlines children’s rights to education, information, privacy and the highest attainable standard of health. It also outlines their rights to leisure and play, to be heard, as well as to protection from violence, sexual exploitation and abuse.

The provisions in the UNCRC were set out and agreed without knowledge of the technology revolution that would follow shortly after, and yet — as the UNCRC reaches its 30th anniversary — they remain as important and relevant in today’s connected world as they were for children at the time of its creation.

The GSMA supports its members as they seek to enable the safe and positive realisation of the many opportunities afforded through connectivity, whilst taking steps to mitigate potential risks.

As UNICEF’s State of the World’s Children 2017 report notes, the internet “...reflects and amplifies the best and worst of human nature. It is a tool that will always be used for good and for ill. Our job is to mitigate the harms and expand the opportunities digital technology makes possible.”

# Cross-Border Flows of Data

## Background

The global digital economy depends on cross-border flows of data to deliver crucial social and economic benefits to individuals, businesses and governments.

When data is allowed to flow freely across national borders, it enables organisations to operate, innovate and to access solutions and support anywhere in the world. Enabling cross-border flows of data can help organisations adopt data-driven digital transformation strategies that ultimately benefit individuals and society. Policies that inhibit the free flow of data through unjustified restrictions or local data storage requirements can have an adverse impact on consumers, businesses and the economy in general.[1]

Cross-border flows of personal data are currently regulated by a number of international, regional and national instruments and laws intended to protect individuals' privacy, the local economy or national security.

While many of these instruments and laws adopt common privacy principles, they do not create an interoperable regulatory framework that reflects the realities, challenges and potential of a globally connected world. Emerging frameworks such as the Asia-Pacific Economic Co-operation (APEC) Cross-Border Privacy Rules and the EU's Binding Corporate Rules allow organisations to transfer personal data generally under certain conditions. These frameworks contain accountability mechanisms and are based on internationally accepted data protection principles.

However, their successful adoption is undermined by the implementation by governments of 'data localisation' (also known as 'data sovereignty') rules that impose local storage requirements or use of local technology.[2] Such localisation requirements can be found in a variety of sector- and subject-specific rules created for financial service providers, the public sector or to maintain professional confidentiality. They are sometimes imposed by countries in the belief that supervisory authorities can more easily scrutinise data that is stored locally.[3]

1 International Chamber of Commerce Report: Trade in the Digital Economy, 2016; ECIPE Report: The Cost of Data Localisation, 2014.

2 Emory Law Journal: Anupam Chander and Uyen Le, Data Nationalism, 2015; Hague Institute for Global Justice: Jonah Force Hill, The Growth of Data Localization Post-Snowden, 2014.

3 European Commission Report: Building a European Data Economy Communication, 2017.

## Debate

*How can industry, legislators, regulators and civil society engage effectively to develop policy that supports cross-border flows of data?*

---

*How can data protection safeguards adequately address the legitimate concerns of governments that seek to impose localisation requirements?*

---

## Industry Position

**Cross-border flows of data play a key role in innovation, competition and economic and social development. Governments can facilitate these data flows in a way that is consistent with consumer privacy and local laws by supporting industry best practices and frameworks for the movement of data and by working to make these frameworks interoperable.**

Governments can also ensure that these frameworks have strong accountability mechanisms, and that the authorities can play a role in overseeing/monitoring their implementation. Governments should only impose measures that restrict cross-border data flows if they are absolutely necessary to achieve a legitimate public policy objective. The application of these measures should be proportionate and not arbitrary or discriminatory against foreign suppliers or services.

Mobile Network Operators (MNOs) welcome frameworks such as the APEC Cross-Border Privacy Rules or the EU's Binding Corporate Rules, which allow accountable organisations to transfer data globally, provided they meet certain criteria. Such mechanisms are based on commonly recognised data privacy principles and require organisations to adopt a comprehensive approach towards data privacy.

This encourages more effective protection for individuals than formalistic administrative requirements, while helping to realise potential social and economic benefits. Such frameworks should be made interoperable across countries and regions to the greatest extent possible. This would stimulate convergence between different approaches to privacy, while promoting appropriate standards of data protection, allowing accountable companies to build scalable and consistent data privacy programmes.

Requirements for companies to use local data storage or technology create unnecessary duplication and cost for companies and there is little evidence that such policies produce tangible benefits for local economies or improved privacy protections for individuals.

To the extent that governments need to scrutinise data for official purposes, MNOs would encourage them to achieve this through existing lawful means and appropriate intergovernmental mechanisms that do not restrict the flow of data.

The GSMA and its members believe that cross-border data flows can be managed in ways that safeguard the personal data and privacy of individuals and remain committed to working with stakeholders to ensure that restrictions are only implemented if they are necessary to achieve a legitimate public policy objective.

Resources:
United Nations Conference on Trade and Development (UNCTAD) Report: Data Protection Regulations and International Data Flows, 2016
White Paper: Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems, 2016
International Chamber of Commerce Report: Trade in the Digital Economy, 2016

Deeper Dive

## National Data Privacy Regimes Should be Based on Shared, Core Principles and Provide Flexibility in Implementation

The challenge when regulating for data privacy, including cross-border flows of data, is to put in place measures that consistently provide consumers with confidence in existing and new services, without limiting service adoption or imposing significant additional costs on service providers.

To achieve this, it is crucial for privacy regulation to be based on shared core principles which, according to United Nations Conference on Trade and Development (UNCTAD) sit "at the heart of most national [privacy] laws and international regimes" as well as industry initiatives. This would allow companies to treat data consistently across their operations, innovate more rapidly, achieve larger scale and reduce costs. Consumers will also benefit from wider choice, improved quality and lower prices of services.

The 2009 Madrid Resolution on International Standards for the Protection of Personal Data and Privacy, for example, encourages consistent international protection of personal data and embraces privacy approaches from all five continents. As well as being designed "to ease the international flow of personal data, essential in a globalized world", the resolution advocates six privacy principles to be adopted by policymakers:

| Lawful and fair | Purpose | Proportionate |
|---|---|---|
| Personal data must be lawfully and fairly processed | Processing should be limited to specified purposes | Processing should be proportionate and not excessive |
| **Quality** | **Openness** | **Accountable** |
| Data held should be accurate | The processor should be open regarding their activities | The processor should be accountable for their activities |

Similar principles are reflected repeatedly in laws and policy initiatives around the world such as the Council of Europe Convention 108, the OECD Guidelines, the EU General Data Protection Regulation, the US Federal Trade Commission's Fair Information Practice Principles and the APEC Privacy Framework. The mobile industry has also adopted the GSMA Mobile Privacy Principles to give consumers confidence that their personal data is being properly protected, irrespective of service, device or country.

## Localisation Rules Risk Undermining the Protection of Personal Data

There are several reasons countries give to justify the imposition of data localisation rules. These include concerns about foreign surveillance and national security and a desire to stimulate a national digital economy through in-country data analysis.

The range of localisation restrictions can include subjecting the data flows to certain restrictions to benefit citizens' privacy and requiring organisations to keep data in-country, but allowing the data to flow thereafter. It may also include forcing the data to be kept in-country altogether or imposing requirements that have the indirect effect of keeping the data in-country, such as mandating the use of local infrastructure.

However, restrictions do not necessarily lead to better protection of personal data. For example, a fragmented approach results in inconsistent protection (e.g., differences across jurisdictions and sectors in what can be stored and for how long) and causes confusion that ultimately has a negative impact on the secure management of personal data.

The risks identified by governments can be mitigated by various solutions and principles without restricting data flows. For example, over the last five years internet platform companies and cloud computing providers have established regional hubs. These allow governments that are concerned about the surveillance activities of foreign countries to avoid data being held in particular jurisdictions. In addition, encryption techniques allow data to be protected from access and stored securely abroad. Requiring localisation on the grounds of a perceived economic benefit are equally flawed. Restricting data processing activities to a national, rather than global, scale is likely to lead to significantly higher costs of operation per customer served while also stopping citizens from accessing innovative digital services that emerge on the global stage.

In order to address legitimate concerns about privacy, governments have adopted a patchwork of international, regional and national rules. In addition to APEC's Privacy Framework and the EU's General Data Protection Regulation (GDPR), regional frameworks have emerged in ASEAN, Latin America and Africa. These frameworks have the commendable aim of aligning economies within regions around a common understanding of data privacy. However, in order to reflect the realities of a globally connected world, they need to be interoperable across regions to the greatest extent possible. This would allow companies to build scalable and accountable data protection and privacy platforms.

Flows of data across borders are important for societal and economic reasons. Without them both economic growth and the potential benefits to society of digital transformation can be hampered. It is therefore incumbent on governments, regulators, industry and civil society groups to reject localisation measures and instead find ways to enable the flow of data while protecting individuals.

# Electromagnetic Fields and Health

## Background

Research into the safety of radio signals, which has been conducted for more than 50 years, has led to the establishment of human exposure standards that provide protection against all established health risks.

The World Health Organization (WHO) and the International Telecommunication Union (ITU) recommend that governments adopt the radio-frequency exposure limits developed by the International Commission on Non-Ionizing Radiation Protection (ICNIRP). These were reviewed and updated in 2018.

The WHO set up the International EMF Project in 1996 to assess the health and environmental effects of exposure to electromagnetic fields (EMF) from all sources.

The strong consensus of expert groups and public health agencies, such as the WHO, is that no health risks have been established from exposure to the low-level radio signals used for mobile communications.

However, research has suggested a possible increased risk of brain tumours among long-term users of mobile phones. As a result, in May 2011, the International Agency for Research on Cancer classified radio signals as a possible human carcinogen.

Health authorities have advised that given scientific uncertainty and the lack of support from cancer trend data, this classification should be understood as meaning that more research is needed. They have also reminded mobile phone users that they can take practical measures to reduce exposure, such as using a hands-free kit or text messaging.

New applications, such as 5G, wireless IoT and wearable devices, will be designed to comply with existing exposure limits. The international exposure guidelines are not technology specific and are periodically reviewed.

## Debate

*Does using a mobile phone regularly, or living near a base station, have any health implications?*

---

*Are there benefits in adopting EMF limits for mobile networks or devices?*

---

*Are new methods needed to assess compliance of advanced antennae planned for 5G deployment?*

---

*Should there be particular restrictions to protect children, pregnant women or other potentially vulnerable groups?*

---

## Industry Position

**National authorities should implement EMF-related policies based on established science, in line with international recommendations and technical standards.**

Large differences between national limits and international guidelines can cause confusion and increase public anxiety. Consistency is vital, and governments should:

- Base EMF-related policy on reliable information sources, including the WHO, trusted international health authorities and expert scientists.
- Set a national policy covering the siting of masts, balancing effective network roll out with consideration of public concerns.
- Accept mobile operators' declarations of compliance with international or national radio frequency levels using technical standards from organisations such as the International Electrotechnical Commission (IEC) and ITU.
- Actively communicate with the public, based on the positions of the WHO, to address concerns.

Parents should have access to accurate information so they can decide when and if their children should use mobile phones. The current WHO position is that international safety guidelines protect everyone in the population with a large safety factor, and that there is no scientific basis to restrict children's use of phones or the locations of base stations. We encourage governments to provide information and voluntary practical guidance to consumers and parents, based on the position of the WHO.

The mobile industry works with national and local governments to help address public concern about mobile communications. Adoption of evidence-based national policies concerning exposure limits and antenna siting, public consultations and information can reassure citizens.

Ongoing, high-quality research is necessary to support health-risk assessments, develop safety standards and provide information to inform policy development. Studies should follow good laboratory practice for EMF research and be governed by contracts that encourage open publication of findings in peer-reviewed scientific literature.

Resources:
WHO International EMF Project website
International Agency for Research on Cancer Monograph on Radiofrequency Fields website
GSMA Report: Mobile Communications and Health
GSMA Report: Arbitrary Radio Frequency Exposure Limits — Impact on 4G Network Deployment
GSMA Report: LTE Technology and Health
GSMA Report: Smart Meters: Compliance with Radio Frequency Exposure Standards
GSMA Report: 5G, the Internet of Things (IoT) and Wearable Devices
GSMA Mobile and Health — Independent Expert Review website
Mobile & Wireless Forum SAR Tick Programme website
ITU EMF Guide website

Deeper Dive

## Health Authorities on the Science

*A large number of studies have been performed over the last two decades to assess whether mobile phones pose a potential health risk. To date, no adverse health effects have been established as being caused by mobile phone use.*
— WHO Fact Sheet 193, October 2014

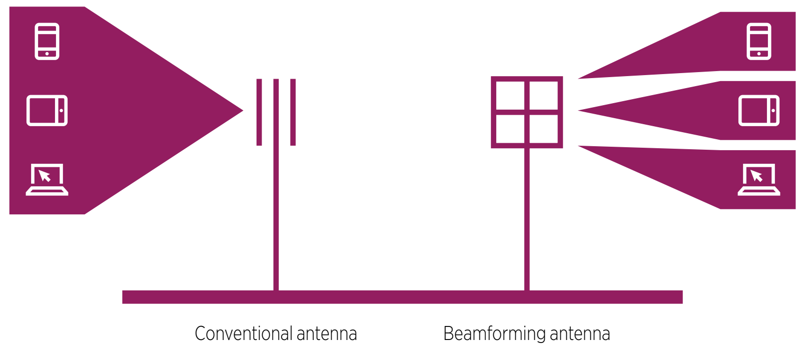
*The results of epidemiological studies in the period reviewed confirm that no higher risk of brain tumors is observed in cell phone users. This conclusion coincides with those of other systematic reviews and risk assessments in the same period by agencies and competent international committees in the evaluation of the effects of electromagnetic fields on health.*
— Scientific Advisory Committee on Radiofrequency and Health — CCARS (Spain), 2017

*Whether mobile phone use causes brain tumours or not was mainly addressed using time trends studies in the last two years. The results were not entirely consistent but mainly point towards a lack of association. Whereas these time series studies do not suffer from recall and selection bias, which is of concern for case-control studies, they are vulnerable to secular time trends. Changes in coding praxis or improved diagnostic tools and thus better detection rate may produce an apparent increase or a decrease in the incidence of brain tumours or specific subtypes. The few indications of changing incidence are thus rather attributed to such methodological limitations than actual changes in risk.*
— Swedish Radiation Safety Authority, 2018

Deeper Dive

## Advanced Antenna Technologies

Many of the antennae used for 5G will look similar to those in use today. Advanced antenna technologies, such as beam-forming, require the use of arrays of antennae to optimise the delivery of the wanted radio signal to connected mobile devices.




As shown above, a conventional base station antenna transmits a radio signal to a wide area regardless of how many users are connected. Advanced beam forming antennae transmit radio signals only to connected users, reducing unwanted exposure.

Beamforming involves combining the signal from multiple antennae to improve performance. However, operation at higher frequencies means that while some could be larger, the size of many of the antennae is expected to be similar to that of existing installations.

Deeper Dive

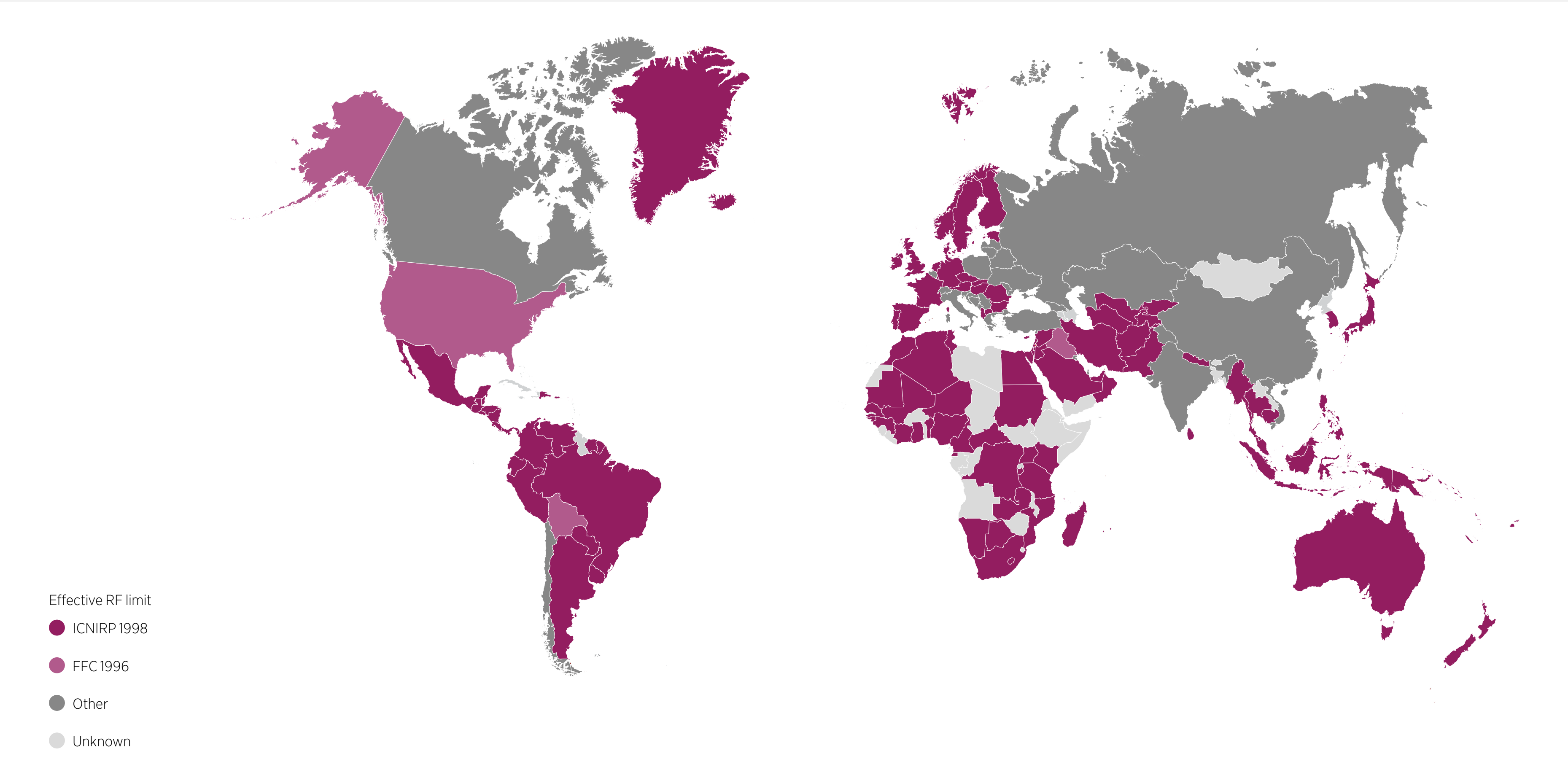
## A Global Look at Mobile Network Exposure Limits

The World Health Organization (WHO) endorses the guidelines of the International Commission for Non-Ionizing Radiation Protection (ICNIRP) and encourages countries to adopt them. While many countries have adopted this recommendation, some have chosen to adopt other limits or additional measures regarding the siting of base stations.

This map shows the approach to radio frequency (RF) exposure limits countries have adopted for mobile communication antenna sites. Much of the world follows the ICNIRP 1998 guidelines or those of the US Federal Communications Commission.

In some cases (e.g., China and Russia) historical limits have not been updated to reflect more recent scientific knowledge. In other cases, RF limits applicable to mobile networks may be the result of arbitrary reductions, as a political response to public concern.

Excluding countries or territories with unknown limits, 126 apply ICNIRP, 11 follow the FCC limits from 1996, and 36 have other limits. Although the map uses only one colour for the 'other' category, there are many differences between these countries in the limit values and their application.



# eWaste

## Background

Electronic waste — also known as e-waste or waste electrical and electronic equipment (WEEE) — is a type of waste generated when devices related to the Information and Communications Technology (ICT) industry reach the end of their life. Parts and materials that make up e-waste usually contain precious or high-value metals that can be recycled at the end of a device's useful life. However, they can also contain hazardous materials that must be treated responsibly and in compliance with environmental legislation. Some used electronic equipment may be suitable for re-use, perhaps after repair and refurbishment.

As part of the ICT sector, mobile operators generate e-waste during periods of technological renewal and also through the normal supply of products (such as routers, mobile phones and tablets) to customers.

Mobile operators around the world have developed WEEE management programmes both as compliance measures to conform to current legislation, and also in their desire to meet their own sustainability and corporate social responsibility goals.

However, in some regions, such as Latin America, there are limited legal frameworks specifically covering e-waste management. Unfortunately, this also means there is a lack of clarity around the concept of extended producer responsibility (EPR).

Usually, EPR rules firmly establish the roles and responsibilities of producers, importers and distributors for equipment in the e-waste chain. The absence of clear rules means operators in Latin America are finding it difficult to manage the e-waste generated through their operations. In some cases, they have even had to take on 100 per cent of the operational and financial responsibility for the management of their customers' e-waste, whereas in most other regions the responsibility is shared among a range of parties including equipment manufacturers, importers and distributors.

In addition, operators have faced other challenges such as a dearth of qualified e-waste managers in some countries, the high costs of e-waste transport and storage, and restrictions (from the Basel Convention) on the export of equipment to countries where it could be treated appropriately.

## Debate

*How should the responsibility for processing e-waste be shared out among a range of industry parties, including operators, equipment manufacturers, importers and distributors?*

---

*How is it possible to distinguish between e-waste and used electronic equipment destined for re-use?*

---

## Industry Position

**The effective management of WEEE at a country and company level must be based on specific regulatory frameworks that recognise the environmental risks that e-waste presents and also the potential for efficient resource recovery. This is to ensure there is no ambiguity among the various parties who are responsible for e-waste management as to how they must act in order to conform to the agreed guidelines.**

Mobile operators have long recognised the importance of WEEE management.

This is why, in regions such as Latin America, they have actively sought to draw attention to loopholes in the legal system and communicate the challenges they have faced during the development of their WEEE management programmes. Moreover, they continue to look for ways to collaborate with the environmental authorities in order to define effective legal frameworks that promote environmentally responsible WEEE management.

With this in mind, they have come up with a number of proposals for regions where there is currently a lack of robust legal frameworks in place:

- Environmental and telecommunications authorities should work together to design, promote and implement policies, standards, laws, regulations and programmes for responsible WEEE management.

- Guidelines that recognise the principle of EPR should be created by relevant environmental authorities and developed into legal frameworks for e-waste management.

- WEEE management programmes should include measures to promote recycling in order to extend the lifespan of devices and material recovery. These need to explain the importance of these processes for the re-use of materials, so they can in turn increase the economic value of devices collected for re-use or recycling.

- Governments, manufacturers, importers, distributors and WEEE management companies should work together to create e-waste awareness campaigns aimed at the general public. These campaigns will help create a culture of WEEE recycling, foster buy-in across all sectors of society and drive improved results when all the parties involved begin implementing WEEE management campaigns.

Resources:
GSMA & United Nations University Report: eWaste in Latin America — Statistical Analysis and Policy Recommendations
GSMA, IDB & South Pole Report: Technology for Climate Action in Latin America
Step Initiative website
United Nations University, International Telecommunication Union & International Solid Waste Association Report: The Global E-waste Monitor 2017 Quantities, Flows, and Resources

# Illegal Content

## Background

Today, mobile networks not only offer traditional voice and messaging services, but also provide access to virtually all forms of digital content via the internet. In this respect, mobile operators offer the same service as any other internet service provider (ISP). This means mobile networks are inevitably used, by some, to access illegal content, ranging from pirated material that infringes intellectual property rights (IPR) to racist content or child sexual abuse material (child pornography).

Laws regarding illegal content vary considerably. Some content, such as child sexual abuse material, is considered illegal around the world, while other content, such as dialogue that calls for political reform, is illegal in some countries while being protected by 'freedom of speech' rights in others.

Communications service providers, including mobile network operators and ISPs, are not usually liable for illegal content on their networks and services, provided they are not aware of its presence and follow certain rules (e.g., 'notice and takedown' processes to remove or disable access to the illegal content as soon as they are notified of its existence by the appropriate legal authority).

Mobile operators are typically alerted to illegal content by national hotline organisations or law-enforcement agencies. When content is reported, operators follow procedures according to the relevant data protection, privacy and disclosure legislation. In the case of child sexual abuse content, mobile operators use terms and conditions, notice and takedown processes and reporting mechanisms to keep their services free of this material.

## Debate

*Should all types of illegal content — from IPR infringements to child sexual abuse content — be subject to the same reporting and removal processes?*

---

*What responsibilities should fall to governments, law enforcement or industry in the policing and removal of illegal content?*

---

*Should access to illegal content on the internet be blocked by ISPs and mobile operators?*

---



## Industry Position

**The mobile industry is committed to working with law enforcement agencies and appropriate authorities, and to having robust processes in place that enable the swift removal or disabling of confirmed instances of illegal content hosted on their services.**

ISPs, including mobile operators, are not qualified to decide what is and is not illegal content, the scope of which is wide and varies between countries. As such, they should not be expected to monitor and judge third-party material, whether it is hosted on, or accessed through, their own network.

National governments decide what constitutes illegal content in their country; they should be open and transparent about which content is illegal before handing enforcement responsibility to hotlines, law-enforcement agencies and industry.

The mobile industry condemns the misuse of its services for sharing child sexual abuse content. The GSMA's Mobile Alliance Against Child Sexual Abuse Content provides leadership in this area and works proactively to combat the misuse of mobile networks and services by criminals seeking to access or share child sexual abuse content.

Regarding copyright infringement and piracy, the mobile industry recognises the importance of proper compensation for rights holders and prevention of unauthorised distribution.

Resources:
GSMA Reference Document: Mobile Alliance Against Child Sexual Abuse Content
Interpol Crimes Against Children website
International Centre for Missing & Exploited Children: Model Legislation & Global Review
INHOPE website
GSMA and UNICEF: Notice and Takedown — Company Policies and Practices to Remove Online Child Sexual Abuse Material
GSMA Guide: Hotlines — Responding to Reports of Illegal Online Content
GSMA and Child Helpline International: Internet Safety Guides (see, in particular, Grooming, Illegal Content, Sexual Extortion of Children)
WePROTECT Global Alliance Model National Response

Deeper Dive

## Mobile Alliance Against Child Sexual Abuse Content

The Mobile Alliance Against Child Sexual Abuse Content was founded by an international group of mobile operators within the GSMA to work collectively on obstructing the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content.

**Alliance members have made the commitment to:**

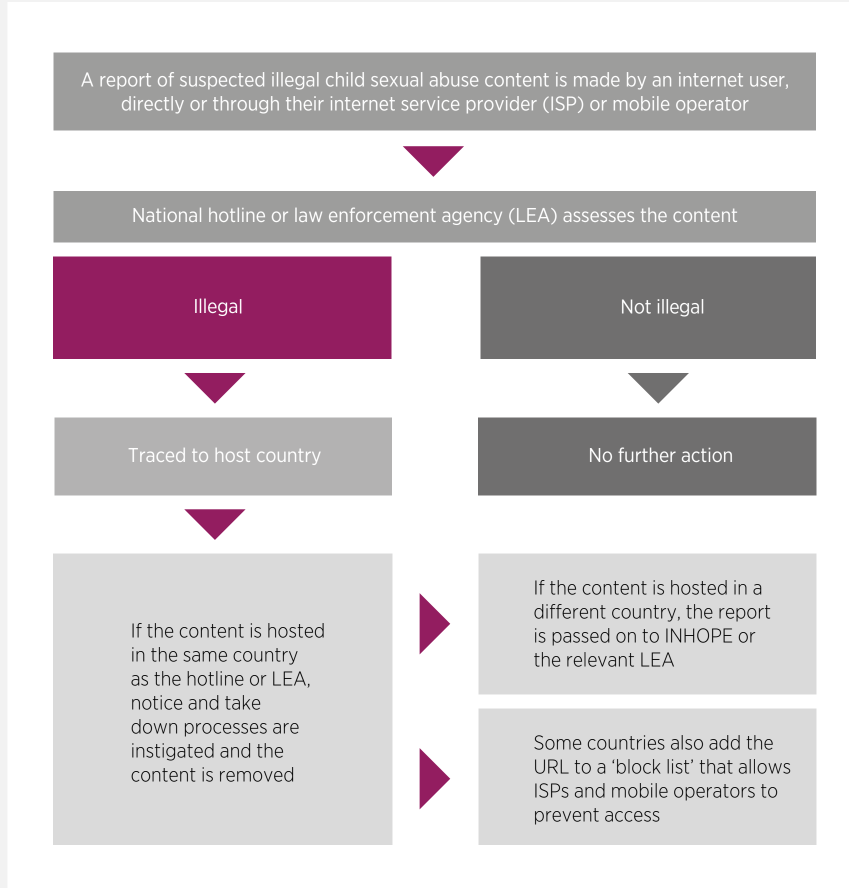
- Implement technical mechanisms to restrict access to websites or URLs identified by an appropriate, internationally recognised agency as hosting child sexual abuse content.
- Implement 'notice and take-down' processes to enable the removal of any child sexual abuse content posted on their own services.
- Support and promote hotlines or other mechanisms for customers to report child sexual abuse content discovered on the internet or on mobile content services.

Through a combination of technical measures, cooperation and information sharing, the Mobile Alliance is working to stem, and ultimately reverse, the growth of online child sexual abuse content around the world.

The Mobile Alliance also contributes to wider efforts to eradicate online child sexual abuse content by publishing guidance and toolkits for the benefit of the whole mobile industry. For example, it has produced a guide to establishing and managing a hotline in collaboration with INHOPE, the umbrella organisation for hotlines, and a guide to implementing notice and take-down processes with UNICEF.

In the 10 years that have passed since the founding of the Mobile Alliance, changes to the digital ecosystem — including the increase in online interactivity and user-generated content — have altered the nature of online child sexual exploitation and abuse. For example, hotlines are increasingly seeing self-generated content (also known as 'sexting') being shared online. Child helplines are receiving calls from children related to 'sexual extortion'. This is where a young person is blackmailed by an offender using self-produced sexual images or videos of the young person to make further sexual or financial demands. GSMA and the Mobile Alliance members continue to work with their external partners to monitor emerging issues and seek additional ways to contribute to the wider efforts to address them. For example, they are collaboratively developing guidance for child helpline counsellors on internet safety issues (including illegal content and sexual extortion) and members are running internet safety consumer education and awareness campaigns on an ongoing basis.

## Mobile Alliance Procedures To Stop Child Sexual Abuse Content



# Internet Governance

## Background

Internet governance involves a wide array of activities related to the policy and procedures of the management of the internet. It encompasses legal and regulatory issues such as privacy, cybercrime, intellectual property rights and spam. It is also, for example, concerned with technical issues related to network management and standards and economic issues such as taxation and internet interconnection arrangements.

Because mobile industry growth is tied to the evolution of internet-enabled services and devices, decisions about the use, management and regulation of the internet will affect mobile service providers and other industry players and their customers.

Internet governance requires input from diverse stakeholders, relating to their interests and expertise in technical engineering, resource management, standards and policy issues, among others. Interested and relevant stakeholders will vary from issue to issue.

## Debate

*Who 'owns' the internet?*

*Should certain countries or organisations be allowed to have greater decision-making powers than others?*

*How should a multi-stakeholder model be applied to internet governance?*

## Industry Position

**The multi-stakeholder model for internet governance and decision making should be preserved and allowed to evolve.**

Internet governance should not be managed through a single institution or mechanism, but be able to address a wide range of issues and challenges relevant to different stakeholders more flexibly than traditional government and intergovernmental mechanisms.

The internet should be secure, stable, trustworthy and interoperable, and no single institution or organisation can or should manage it.

Collaborative, diverse and inclusive models of internet governance decision-making are requisite to participation by the appropriate stakeholders.

The decentralised development of the internet should continue, without being controlled by any particular business model or regulatory approach.

Some questions warrant a different approach at the local, national, regional or global level. An effective and efficient multi-stakeholder model ensures that the stakeholders, within their respective roles, can participate in the consensus-building process for any specific issue.

Technical aspects related to the management and development of internet networks and architecture should be addressed through standards bodies, the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB) and other forums.

Economic and transactional issues such as internet interconnection charges are best left to commercial negotiation, consistent with commercial law and regulatory regimes.

*Only a concerted joint global effort by governments, businesses, the technical community and civil society will produce a governance architecture that is as generic, scalable and transnational as the internet itself. No single actor or group of actors can solve this alone.*

— Vint Cerf, Chief Internet Evangelist at Google and Co-inventor of the Internet Protocol suite, February 2018

Resources:
The Internet Governance Forum website
World Summit on the Information Society WSIS+10 website
The Internet Society Internet Governance website
UNESCO Internet Governance website

# Mandated Government Access

## Background

Mobile network operators are often subject to a range of laws and/or licence conditions that require them to support law enforcement and security activities in countries where they operate. These requirements vary from country to country and have an impact on the privacy of mobile customers.

Where they exist, such laws and licence conditions typically require operators to retain data about their customers' mobile service use and disclose it, including customers' personal data, to law enforcement and national security agencies on lawful demand. They may also require operators to have the ability to intercept customer communications following lawful demand.

Such laws provide a framework for the operation of law enforcement and security service surveillance and guide mobile operators in their mandatory liaison with these services.

However, in some countries, there is a lack of clarity in the legal framework to regulate the disclosure of data or lawful interception of customer communications.

This creates challenges for industry in protecting the privacy of its customers' information and their communications.

Legislation often lags behind technological developments. For example, it may be the case that obligations apply only to established telecommunications operators but not to more recent market entrants, such as those providing internet-based services, including Voice over IP (VoIP), video or instant messaging.

In response to public debate concerning the extent of government access to mobile subscriber data, a number of major telecommunications providers (such as AT&T, Deutsche Telekom, Orange, Rogers, SaskTel, Sprint, T-Mobile, TekSavvy, TeliaSonera, Telstra, Telus, Verizon, Vodafone and Wind Mobile) as well as internet companies (such as Apple, Amazon, Dropbox, Facebook, Google, LinkedIn, Microsoft, Pinterest, Snapchat, Tumblr, Twitter and Yahoo!) publish 'transparency reports', which provide statistics relating to government requests for disclosure of such data.

## Debate

*What is the correct legal framework to achieve a balance between a government's obligation to ensure its law-enforcement and security agencies can protect citizens, and the rights of those citizens to privacy?*

---

*Should all providers of communication services be subject to the same interception, retention and disclosure laws on a technology neutral basis?*

---

*Would further transparency about the number and nature of the requests that governments make assist the debate, improve government accountability and bolster consumer confidence?*

---

## Industry Position

**Governments should ensure they have a proportionate legal framework that clearly specifies the surveillance powers available to national law enforcement and security agencies.**

Any interference with the right to privacy of telecommunications customers must be in accordance with the law.

The retention and disclosure of data and the interception of communications for law enforcement or security purposes should take place only under a clear legal framework and using the proper process and authorisation specified by that framework.

There should be a legal process available to telecommunications providers to challenge requests which they believe to be outside the scope of the relevant laws.

The framework should be transparent, proportionate, justified and compatible with human rights principles, including obligations under applicable international human rights conventions, such as the International Convention on Civil and Political Rights.

Given the expanding range of communications services, the legal framework should be technology neutral.

Governments should provide appropriate limitations of liability or indemnify telecommunications providers against legal claims brought in respect of compliance with requests and obligations for the retention, disclosure and interception of communications and data.

The costs of complying with all laws covering the interception of communications and the retention and disclosure of data should be borne by governments. Such costs and the basis for their calculation should be agreed in advance.

The GSMA and its members are supportive of initiatives that seek to increase government transparency and the publication by government of statistics related to requests for access to customer data.

Resources:
United Nations General Assembly Report: Guiding Principles on Business and Human Rights — Implementing the United Nations "Protect, Respect and Remedy" Framework
Sixth Form Law — Malone v. The United Kingdom website
High Court Judgement: Data Retention and Investigatory Powers Act 2014 ("DRIPA")
UK Investigatory Powers Review Report: A Question of Trust
Office of the Privacy Commissioner of Canada website

Deeper Dive

## Trending Towards Transparency

There is an important global public debate about the scope, necessity and legitimacy of the legal powers that government authorities use to access the communications of private individuals. ICT firms are increasingly reporting the demands of governments for communications data where it is legal to do so. These reports have revealed the degree to which government intelligence and law enforcement agencies rely on such information.

Many of the largest communications and internet content providers (including AT&T, Deutsche Telekom, Telenor, Verizon, Vodafone, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter and Yahoo!) publish periodic transparency reports.

Typically, these reports include how many of these requests resulted in the disclosure of customer information. They reveal the frequency of such requests and also some detail about the kind of information accessed. This can include customer account information, the interception of communications and metadata, which can reveal an individual's location, interests or relationships. Mobile operators often have no option but to comply with such requests, but they are increasingly pressing for greater transparency about the nature and scale of government access.

Questions have also arisen as to the role that telecommunications network and service providers play in relation to such access. For example, misunderstandings can arise about the level to which mobile network operators have the technical capacity to intercept communications. Intercepting standard phone calls or SMS messages to and from specific users is technically possible and lawful interception requirements and capabilities have been described in the global mobile standards for decades.

However, communications between users using an internet-based platform, known as an over-the-top (OTT) service, is generally beyond the reach of mobile network operators. OTT messaging applications are usually encrypted, with messages not stored by the mobile network operators nor decryption keys made available to them. So operators can neither access or provide messages' content, even on receipt of lawful requests. Both internet companies and mobile network operators may find themselves in a difficult position — bound to meet their obligations to provide lawful access, while assuring their customers that they protect private user information.

To further support their commitment to transparency, some operators have joined forces with internet companies and other stakeholders in initiatives such as the Global Network Initiative (GNI). The GNI brings together telecommunications operators, major internet companies, leading academics, civil society organisations, and investors to advance privacy and freedom of expression in the information and communications technology (ICT) sector. In March 2017, seven operators — Millicom, Nokia, Orange, Telefónica, Telenor Group, Telia Company and Vodafone — joined an expanded GNI after having previously promoted transparency through the Telecommunications Industry Dialogue. These companies committed to the GNI Principles on Freedom of Expression and Privacy, which provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of these human rights globally.

Civil society organisations have contributed to the advancement of these issues by trying to provide trustworthy measures of transparency. Ranking Digital Rights (RDR) publishes an annual report on telecoms and internet companies disclosed commitments, policies and practices that affect users' privacy and freedom of expression. The RDR calls for governments to allow encryption and publish their own transparency reports, to make it clear what information they demanded from companies  and why.

The debate can be heated on both sides — those who argue that law enforcement agencies require broad access in order to fight crime versus those who challenge the government's level of inquiry into private lives and strive to maintain citizens' rights to privacy in the digital age. GSMA members maintain that transparency reporting brings valid information to the public and policymakers, raising key questions about the balance between government access and privacy.

**Government Access – Encouraging Transparency**

# Mandated Service Restriction Orders

## Background

From time to time, mobile network operators (MNOs) receive orders from government authorities to restrict services on their networks. These service restriction orders (SROs) require operators to shut down or restrict access to their mobile network, a network service or an over-the-top (OTT) service. Orders include blocking particular apps or content, restricting data bandwidth and degrading the quality of SMS or voice services. In some cases, operators would risk criminal sanctions or the loss of their licence if they were to disclose that they had been issued with an SRO.

SROs can have a number of serious consequences. For example, national security can be undermined if the powers are misused and public safety can be endangered if emergency services and citizens are not able to communicate with one another. Freedom of expression, freedom of assembly, freedom to conduct business and other human rights can also be impacted.

Furthermore, individuals and businesses who are not the target of the SRO may no longer be able to pay friends, suppliers or salaries. This can have a knock-on effect on credit and investment plans, ultimately damaging the country's reputation for managing the economy and foreign investment, and discouraging donor countries from providing funds or other resources.

MNOs also suffer. Not only do they sustain financial losses due to the suspension of services, as well as damage to their reputation, but their local staff can also face pressure from authorities and possibly even retaliation from the public.

## Debate

*What factors and alternatives should governments consider before planning an SRO?*

---

*What tools and methods can be used to avoid the need for an SRO or to avoid negative impacts if an SRO is the only option?*

---

## Industry Position

**The GSMA discourages the use of SROs. Governments should only resort to SROs in exceptional and pre-defined circumstances, and only if absolutely necessary and proportionate to achieve a specified and legitimate aim that is consistent with internationally recognised human rights and relevant laws.**

In order to aid transparency, governments should only issue SROs to operators in writing, citing the legal basis and with a clear audit trail to the person authorising the order. They should inform citizens that the service restriction has been ordered by the government and has been approved by a judicial or other authority in accordance with administrative procedures laid down in law. They should allow operators to investigate the impacts on their networks and customers and to communicate freely with their customers about the order. If it would undermine national security to do so at the time when the service is restricted, citizens should be informed as soon as possible after the event.

Governments should seek to avoid or mitigate the potentially harmful effects of SROs by minimising the number of demands, the geographic scope, the number of potentially affected individuals and businesses, the functional scope and the duration of the restriction.

For example, rather than block an entire network or social media platform, it may be possible for the SRO to target particular content or users. In any event, the SRO should always specify an end date. Independent oversight mechanisms should be established to ensure these principles are observed.

Operators can play an important role by raising awareness among government officials of the potential impact of SROs. They can also be prepared to work swiftly and efficiently to determine the legitimacy of the SRO once it has been received. This will help establish whether it has been approved by a judicial authority, whether it is valid and binding and whether there is opportunity for appeal, working with the government to limit the scope and impact of the order. Procedures can include guidance on how local personnel are to deal with SROs and the use of standardised forms to quickly assess and escalate SROs to senior company representatives.

All decisions should first and foremost be made with the safety and security of the operators' customers, networks and staff in mind, and with the aim of being able to restore services as quickly as possible.

Resources:
Australian Government Draft Guidelines on Website Blocking
Global Network Initiative and the Telecommunications Industry Dialogue Joint Statement: Service Restrictions
Telia Company Form for Assessment and Escalation of SROs

# Mandatory Registration of Prepaid SIMs

## Background

In a number of countries, customers of prepaid or pay-as-you-go services can anonymously activate their subscriber identity module (SIM) card by simply purchasing credit, as formal user registration is not required. Around 150 governments around the world[1] have mandated prepaid SIM registration citing a perceived, but unproven, link between the introduction of such policies and the reduction of criminal and anti-social behaviour. Mandated prepaid SIM registration is most prevalent in Africa, where 90 per cent of UN-recognised states have such laws.

Some governments — including the Czech Republic, the United Kingdom and the United States — have decided against mandating registration of prepaid SIM users, concluding that the potential loopholes and implementation challenges outweigh the merits.

SIM registration can, however, allow many consumers to access value-added mobile and digital services that would not otherwise be available to them as unregistered users, including identity-linked services such as mobile money, e-health and e-government services.

For a SIM registration policy to lead to positive outcomes for consumers, it must be implemented in a pragmatic way that takes into account local market circumstances, such as the ability of mobile operators to verify customers' identity documents. If the registration requirements are disproportionate to consumers' ability to meet them in a specific market, mandating this policy may lead to implementation challenges and unforeseen consequences. For example, it could unintentionally exclude vulnerable and socially disadvantaged consumers or refugees who lack the required identity documents. It might also lead to the emergence of a black market for fraudulently registered or stolen SIM cards, based on the desire by some mobile users, including criminals, to remain anonymous.

## Debate

*To what extent do the benefits of mandatory prepaid SIM registration outweigh the costs and risks?*

---

*What factors should governments consider before mandating such a policy?*

---

## Industry Position

**While registration of prepaid SIM card users can deliver valuable benefits to citizens, governments should not mandate it.**

To date, there has been no empirical evidence that mandatory SIM registration directly leads to a reduction in crime. Where a decision to mandate the registration of prepaid SIM users has been made, we recommend that governments take into account global best practices and allow registration mechanisms that are flexible, proportionate and relevant to the specific market, including the level of official ID penetration in that market and the timing of any national identity roll-out plans.

If these conditions are met, the SIM registration exercise is more likely to be effective and lead to more accurate customer databases. Furthermore, a robust customer verification and authentication system can enable mobile operators to facilitate the creation of digital identity solutions, empowering customers to access a variety of mobile and non-mobile services.

We urge governments who are considering the introduction or revision of mandatory SIM-registration to take the following steps prior to finalising their plans:

- Consult, collaborate and communicate with mobile operators before, during and after the implementation exercise.
- Balance national security demands against the protection of citizens' rights, particularly where governments mandate SIM registration for security reasons.
- Set realistic timescales for designing, testing and implementing registration processes.
- Provide certainty and clarity on registration requirements before any implementation.
- Allow and/or encourage the storage of electronic records and design registration processes that are administratively 'light'.
- Allow and/or encourage the SIM-registered customer to access other value-added mobile and digital services.
- Support mobile operators in the implementation of SIM-registration programmes by contributing to joint communication activities and to their operational costs.

[1] GSMA Report: Access to Mobile and Proof of Identity.

Resources:
GSMA website: Mandatory Registration of Pre-paid SIMs
GSMA Report: Access to Mobile and Proof of Identity
GSMA Policy Note: Enabling Access to Mobile Services for the Forcibly Displaced
GSMA Report: Mandatory Registration of Prepaid SIM cards — Addressing Challenges Through Best Practice
GSMA Report: Regulatory and Policy Trends Impacting Digital Identity and the Role of Mobile

# Mobile Devices: Counterfeit

## Background

A counterfeit mobile device explicitly infringes the trademark or design of an original or authentic 'branded' product, even where there are slight variations to the established brand name.

Due to their illicit nature, these mobile devices are typically shipped and sold on black markets globally, by organised criminal networks. As a result, there is limited awareness among consumers and governments about the true scale and impact of counterfeit mobile devices.

It is estimated that almost one in five mobile devices may be counterfeit.[1] This has negative effects for consumers who risk lower quality, safety, security, environmental health and privacy assurances. It also impacts governments who forego tax and duties and must contend with increased crime. Industry players are also affected, as it can harm their trademarks and brands.

Some countries are considering the implementation of national white lists to combat counterfeit, smuggled and non-homologated devices. The purpose of white lists is to indicate which devices are permitted access to the networks. Operators implement device blocking capabilities on their local networks and connect with the national white list to ensure permitted devices are allowed network access.

However, counterfeit mobile devices are not easy to identify and block, given that many have IMEIs that appear legitimate. It is now commonplace for counterfeiters to hijack IMEI number ranges allocated to legitimate device manufacturers for use in their products and this makes it more difficult to differentiate between authentic and counterfeit products.

## Debate

*How can governments and other stakeholders best address the issue of counterfeit mobile devices?*

---

*How can anti-counterfeit measures be framed to also consider consumers who have unwittingly purchased counterfeit devices?*

---

## Industry Position

**The mobile industry supports the need for legal and product integrity in the device market and is increasingly concerned about the negative impact of counterfeit devices on consumer welfare and society in general.**

Although mobile operators and legitimate vendors cannot stop the production and distribution of counterfeit devices, multi-stakeholder collaboration can help combat the issue at the source. In particular, national law enforcement and customs agencies should take measures to stop the production and exportation of counterfeit devices in their jurisdictions. It is essential that information on crime patterns and specific criminal activity relating to counterfeit devices is provided by national agencies to appropriate international bodies, such as Interpol and the World Customs Organization, to facilitate action in other jurisdictions by the relevant agencies.

GSMA has made its IMEI database available to the World Customs Organization to establish a global security gateway where customs officers can verify the authenticity of mobile device identities online. National customs agencies are advised to systematically make use of this facility as part of a rigorous set of measures to monitor the importation of mobile devices. The database is made available to national customs agencies directly.

The GSMA encourages operators to deploy systems like Equipment Identity Registers (EIR) and to connect to the GSMA's IMEI Database. Using the GSMA's global Type Allocation Code (TAC) list of all legitimate device identity number ranges, operators can block devices with invalid IMEIs.

National authorities should study which factors, such as import duties and taxation levels, contribute to the local demand for counterfeit devices. The potential of reduced tax levels to narrow the gap between the cost of counterfeit/smuggled and legitimate devices should be carefully considered with a view to making the black market a less lucrative place in which to trade.

Some countries are considering the implementation of national white lists to combat counterfeit, smuggled and non-homologated devices. White lists can be successful if they are linked with the GSMA TAC list for verification of the legitimate TAC/IMEI holders. If national import verification systems and national device homologation systems exist these should also be linked to the national white list. Some implementations propose that customers register their details and devices centrally. GSMA is opposed to central customer registrations since they are unnecessary — the subscriber identities associated with each device can be established by the network operators without the need for consumer action.

Where national authorities are considering introducing a white list system and the pursuant blocking of devices, they should consider offering an amnesty to existing consumers who have non-compliant devices, as the loss to consumers and the social, economic and security impact on the country of the immediate blocking of huge quantities of devices is significant. In addition, it is recommended that the funding model for such systems should not place a burden on the end users (i.e., consumers and network operators) since they are not the cause of the underlying issue. White list systems should also not be applied to roamers who might be denied service without cause.

[1] According to figures from OECD, 2017

Resources:
IMEI Services provided by the GSMA
GSMA Device Check Platform
OECD Report: Trade in Counterfeit ICT Goods
The WCO Tool in the Fight Against Counterfeiting website

# Mobile Devices: Theft

## Background

Policymakers in many countries are concerned about the incidence of mobile device theft, particularly when organised crime becomes involved in the bulk export of stolen devices to other markets.

For many years, the GSMA has led industry initiatives to block stolen mobile devices, based on a shared database of the unique identifiers of devices reported lost or stolen. Using the International Mobile Equipment Identifier (IMEI) of mobile devices, the GSMA maintains a central list — known as the GSMA Black List — of all devices reported lost or stolen by mobile network operators' customers. The GSMA IMEI Database that hosts the GSMA blacklisting service is available to other network operators around the world to ensure those devices transported to other countries are also denied network access.

The efficient blocking of stolen devices on individual network Equipment Identity Registers (EIRs) depends on the secure implementation of the IMEI in all mobile devices. Leading device manufacturers have agreed to support a range of measures to strengthen IMEI security, and progress is monitored by the GSMA.

## Debate

*What can industry do to prevent mobile phone theft?*

---

*What are the policy implications of this rising trend?*

---

## Industry Position

**The mobile industry has led numerous initiatives and made great strides in the global fight against mobile device theft.**

Although the problem of device theft is not of the industry's creation, the industry is part of the solution. When lost or stolen mobile devices are rendered useless, they have significantly reduced value, removing the incentive for thieves to target them.

The GSMA encourages its member operators to deploy EIRs on their networks to deny connectivity to any stolen device. Operators should connect to the GSMA IMEI Database and share their own network's black list to ensure devices stolen from their customers can be blocked on any other networks that also connect to the database. These black list solutions have been in place on some networks for many years.

To better enable a range of stakeholders to combat device crime, GSMA provides services that allow eligible parties such as law enforcement, device traders and insurers to check the status of devices against the GSMA Black List.

IMEI blocking, when complimented with additional measures undertaken by, and in consultation with, a variety of stakeholders, can be the cornerstone of a highly effective anti-theft campaign.

Consumers that have had their devices stolen are particularly vulnerable to their personal data being used to commit a range of additional crimes. Industry, law enforcement agencies and regulators are recommended to provide anti-theft consumer education material on their websites reflecting the advice and measures appropriate to their market.

The concept of a 'kill switch' — a mechanism allowing mobile device users to remotely disable their stolen device — has received much attention. The GSMA supports device-based anti-theft features and has defined feature requirements that could lead to a global solution. These high-level requirements have set a benchmark for anti-theft functionality, while allowing the industry to innovate.

The deployment of persistent endpoint security solutions on mobile devices can also help render devices useless and unattractive to criminals by preventing those devices from working on non-mobile networks, such as Wi-Fi, where EIR blocking would otherwise be ineffective.

National authorities have a significant role to play in combatting this criminal activity. It is critical that they engage constructively with the industry to ensure the distribution of mobile devices through unauthorised channels is monitored and that action is taken against those involved in the theft or illegal distribution of stolen devices.

A coherent cross-border information sharing approach involving all relevant stakeholders increases the effectiveness of national measures. GSMA advocates the sharing of stolen device data internationally for blocking and status checking purposes and the GSMA IMEI Database facilitates this function. Only if regulation allows stolen device information to be shared across all countries will the deterrent have most impact.

Some national authorities have proposed national white lists or black lists with ongoing centralised customer registration requirements to combat device theft. These systems are unnecessary, as blacklisting systems are sufficient and less complex or expensive to implement and maintain.

In markets where a national white list or black list exists, lost and stolen device information can be exchanged between mobile network operators through the GSMA IMEI Database. Alternatively, if a national device blacklisting system is already in place, and is compliant with the GSMA's requirements, it may be connected to the GSMA Black List.

Resources:
IMEI Services provided by the GSMA
GSMA IMEI Database Portal
GSMA Security Technical Design Principles
GSMA IMEI Security Weakness Reporting and Correction Process
GSMA Reference Document: Anti-Theft Device Feature Requirements
GSMA Mobile Phone Theft — Consumer Advice
GSMA & OAS Briefing Paper Aug 2011: Theft of Mobile Terminal Equipment

# Mobile Network and Device Security

## Background

Security attacks threaten all forms of ICT, including mobile technologies. Consumer devices are targeted for a variety of reasons, from changing the IMEI number of a mobile phone to re-enable it after theft, through to data extraction or the use of malware to perform functions that have the potential to cause harm to users.

Mobile networks use encryption technologies to make it difficult for criminals to eavesdrop on calls or to intercept data traffic. Legal barriers to the deployment of cryptographic technologies have been reduced in recent years and this has allowed mobile technologies to incorporate stronger and better algorithms and protocols, which remain of significant interest to hackers and security researchers.

Recent years have seen a significant increase in interest in protocols such as SS7 and Diameter, which support interconnection between network operators to support mobile services. The GSMA has led a range of industry initiatives to ensure network operators are aware of the risks and the mitigation options open to them to protect their networks and their customers.

The GSMA's work and recommendations have been acknowledged by regulators around the world as being sufficient to eliminate the need for regulation.

The GSMA plays a key role in coordinating the industry response to security incidents and it has developed and launched a Coordinated Vulnerability Disclosure (CVD) programme. This allows the GSMA to work with a range of stakeholders, including its operator members, security researchers and industry suppliers, to ensure an appropriate response to threats that could affect services, networks or devices.

The GSMA's Warning Advice and Reporting Point (WARP) helps coordinate the mobile ecosystem worldwide, and provides crucial support around security challenges. Drawing on the collective knowledge of mobile operators, vendors and security professionals, WARP collects and disseminates information and advice on security incidents within the mobile community — in a trusted and anonymised way. Stakeholders from the mobile ecosystem are encouraged to join WARP to collectively address the critical security issues faced by the industry, its partners and its customers.

GSMA's Fraud and Security Group acts as a centre of expertise to drive the industry's management of fraud and security matters. The group seeks to maintain or increase the protection of mobile operator technology and infrastructure, and customer identity, security and privacy, so that the industry's reputation stays strong and mobile operators remain trusted partners in the ecosystem.

## Debate

*How secure are mobile voice and data technologies and what is being done to mitigate the risks?*

---

*Do emerging technologies and services create new opportunities for criminals?*

---

*What will the 5G security landscape look like?*

---

## Industry Position

**The protection and privacy of customer communications is at the forefront of operators' concerns.**

The mobile industry makes every reasonable effort to protect the privacy and integrity of customer and network communications. The barriers to compromising mobile security are high and research into possible vulnerabilities has generally been technically quite complex.

While no security technology is guaranteed to be unbreakable, practical attacks on mobile services are rare, as they tend to require considerable resources, including specialised equipment, computer processing power and a high level of technical expertise beyond the capability of most people.

Reports of eavesdropping are not uncommon, but such attacks have not taken place on a wide scale, and UMTS and LTE networks are considerably better protected against eavesdropping risks than GSM networks. Moreover, 5G technology boasts a host of new security capabilities that further enhance protection levels.

The GSMA supports global security standards for emerging services and acknowledges the role that SIM-based secure elements have played in protecting users and mobile services because the SIM card has proven itself to be resilient to attack. The Embedded Universal Integrated Circuit Card (UICC) approach that has been defined by GSMA, and is being rolled out by industry, inherits the best security properties from the SIM and is designed to build on the protection levels achieved in the past.

The GSMA constantly monitors the activities of hacker groups, as well as researchers, innovators and a range of industry stakeholders, to improve the security of communications networks. Our ability to learn and adapt can be seen in the security improvements implemented from one generation of mobile technology to the next.

Resources:
GSMA Security Accreditation Scheme website
GSMA Security Advice for Mobile Phone Users website
GSMA Coordinated Vulnerability Disclosure website
GSMA Warning Advice and Reporting Point website

# Number-Resource Misuse and Fraud

## Background

Many countries have serious concerns about number-resource misuse, a practice whereby calls never reach the destination indicated by the international country code. Instead they are terminated prematurely, through carrier and/or content provider collusion, to revenue-generating content services without the knowledge of the ITU-T assigned number-range holder.

This abuse puts such calls outside any national regulatory controls on premium-rate and revenue-share call arrangements, and is a key contributing factor to International Revenue Share Fraud (IRSF) perpetrated against telephone networks and their customers. Perpetrators of IRSF are motivated to generate incoming traffic to their own services with no intention of paying the originating network for the calls. They then receive payment quickly, long before other parties within the settlement process.

Misuse also affects legitimate telephony traffic, as high-risk number ranges can be blocked as a side-effect.

## Debate

*How can regulators, number-range holders and other industry players collaborate to address this type of misuse and the resulting fraud?*

## Industry Position

**Number-resource misuse has a significant economic impact for many countries, so multi-stakeholder collaboration is key.**

The telecommunications fraud carried out as a consequence of number-resource misuse is one of the topics being addressed by the GSMA Fraud and Security Group, a global conduit for best practice with respect to fraud and security management for mobile network operators. The Fraud and Security Group's main focus is to drive industry management of mobile fraud and security matters to protect operators and consumers, and safeguard the mobile industry's trusted reputation.

The Fraud and Security Group supports European Union guidelines under which national regulators can instruct communications providers to withhold payment to downstream traffic partners in cases of suspected fraud and misuse.

The group believes that national regulators can help communications providers reduce the risk of number-resource misuse by enforcing stricter management of national numbering resources. Specifically, regulators can:

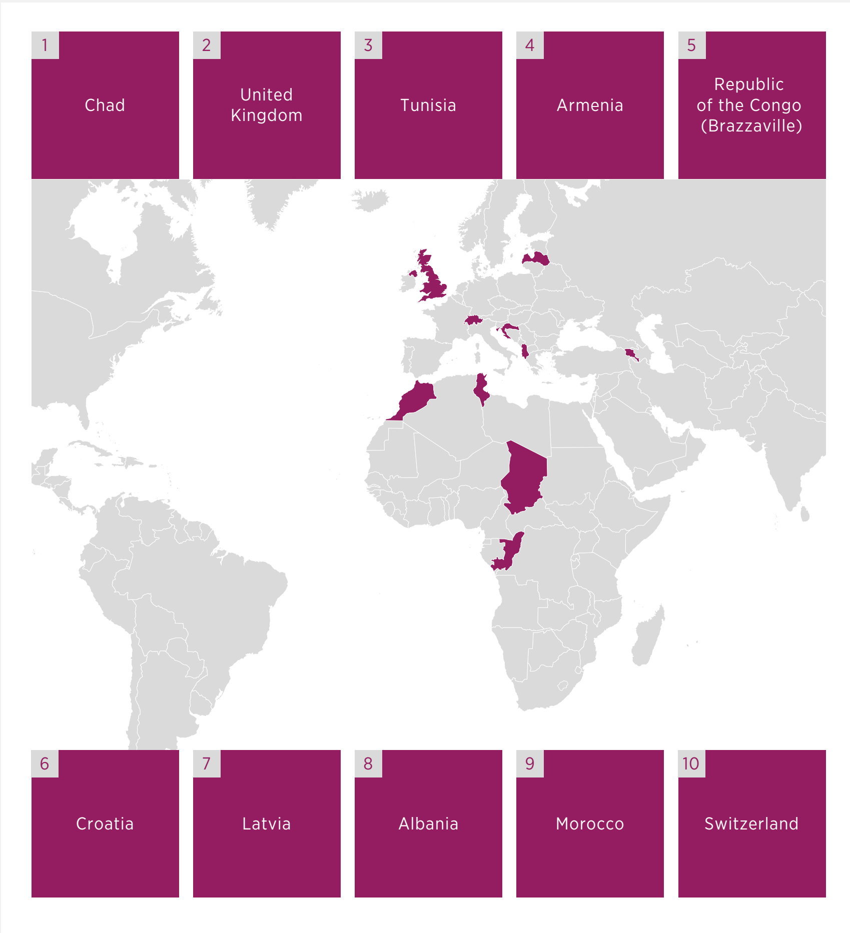
- Ensure national numbering plans are easily available, accurate and comprehensive.
- Implement stricter controls over the assignment of national number ranges to applicants and ensure the ranges are used for the purpose for which they have been assigned.
- Implement stricter controls over leasing of number ranges by number-range assignees to third parties.

The Fraud and Security Group shares abused number ranges among its members and with other fraud-management industry bodies. It also works with leading international transit carriers to reduce the risk of fraud that arises as a result of number-resource misuse, and with law enforcement agencies to support criminal investigations in this area.

Resources:
ITU-T Misuse of an E.164 International Numbering Resource website

Facts and Figures

## Top 10 Countries Whose Numbering Resources Are Being Abused




Source: GSMA July 2018



Best Practice

## Recommended Operator Controls to Reduce Exposure to Fraud from Number-Resource Misuse

Implement controls at the point of subscriber acquisition and controls to prevent account takeover.

Remove the conference or multi-call facility from a mobile connection unless specifically requested, as fraudsters can use this feature to establish up to six simultaneous calls.

Remove the ability to call forward to international destinations, particularly to countries whose numbering plans are commonly misused.

Utilise the GSMA high-risk ranges list, so that unusual call patterns to known fraudulent destinations can raise alarms or be blocked.

Ensure roaming usage reports received from other networks are monitored 24x7, preferably through an automated system.

Ensure that up-to-date tariffs, particularly for premium numbers, are applied within roaming agreements.

Implement the Barring of International Calls Except to Home Country (BOIEXH) function for new or high-risk subscriptions.

# Privacy

## Background

Research shows that mobile customers are concerned about their privacy and want simple and clear choices for controlling how their private information is used. They also want to know they can trust companies with their data. A lack of trust can act as a barrier to growth in economies that are increasingly data driven.

One of the major challenges faced by the growth of the mobile internet is that the security and privacy of people's personal information is regulated by a patchwork of geographically-bound privacy regulations, while the mobile internet service is, by definition, international. Furthermore, in many jurisdictions the regulations governing how customer data is collected, processed and stored vary considerably between market participants. For example, the rules governing how personal data is treated by mobile operators may be different to those governing how it can be used by internet players.

This misalignment between national privacy laws and global standard practices that have developed within the internet ecosystem makes it difficult for operators to provide customers with a consistent user experience. Equally, the misalignment may cause legal uncertainty for operators, which can deter investment and innovation. The inconsistent levels of protection also create risks that consumers might unwittingly provide easy access to their personal data, leaving them exposed to unwanted or undesirable outcomes such as identity theft and fraud.

## Debate

*How can policymakers help create a privacy framework that supports innovation in data use while balancing the need for privacy across borders, irrespective of the technology involved?*

---

*How is responsibility for ensuring privacy across borders best distributed across the mobile internet value chain?*

---

*What role does self-regulation play in a continually evolving technology environment?*

---

*What should be done to allow data to be used to support the social good and meet pressing public policy needs?*

---

## Industry Position

**Currently, the wide range of services available through mobile devices offers varying degrees of privacy protection. To give customers confidence that their personal data is being properly protected — irrespective of service or device — a consistent level of protection must be provided.**

Mobile operators believe that customer confidence and trust can only be fully achieved when users feel their privacy is appropriately protected.

The necessary safeguards should derive from a combination of internationally agreed approaches, national legislation and industry action. Governments should ensure legislation is technology neutral and that its rules are applied consistently to all players in the internet ecosystem.

Because of the high level of innovation in mobile services, legislation should focus on the overall risk to an individual's privacy, rather than attempting to legislate for specific types of data. For example, legislation must deal with the risk to an individual arising from a range of different data types and contexts, rather than focusing on individual data types.

The mobile industry should ensure privacy risks are considered when designing new apps and services, and develop solutions that provide consumers with simple ways to understand their privacy choices and control their data.

The GSMA is committed to working with stakeholders from across the mobile industry to develop a consistent approach to privacy protection and promote trust in mobile services.

Resources:
GSMA Mobile and Privacy website
GSMA Report: Safety, Privacy and Security Across the Mobile Ecosystem
GSMA Report: Consumer Research Insights and Considerations for Policymakers
GSMA Report: Mobile Privacy Principles — Promoting a User-centric Privacy Framework for the Mobile Ecosystem
GSMA Report: Privacy Design Guidelines for Mobile Application Development
GSMA Report: Mobile Privacy and Big Data Analytics
GSMA Presentation: IoT Privacy by Design Decision Tree

Deeper Dive

## Smart Privacy Practice and Regulation

A combination of smart data privacy practices and smart data privacy regulation is required to sustain consumers' trust in the digital ecosystem that has evolved rapidly around them.

The GSMA has developed nine Mobile Privacy Principles as well as a range of resources to promote good practice. These resources include the GSMA's Privacy Design Guidelines for Mobile Application Development, considerations that should be taken into account when engaging in Big Data analytics and a privacy-by-design decision tree for use in developing IoT products and services. They seek to strike a balance between protecting privacy and enabling organisations to achieve commercial, public policy and societal goals.

If organisations adopt comprehensive policies, processes and practices to protect the privacy of individuals — and can easily demonstrate these safeguards are effective — they will strengthen trust among consumers and regulators. Equally, if governments adopt smart data privacy rules, they can establish a regulatory environment that stimulates the digital economy while also unleashing its benefits for consumers and citizens.

While governments must ensure smart data privacy laws take account of citizen's privacy concerns, they must also recognise that these rules can have important consequence beyond the protection of privacy. As a result, when drafting these rules, governments must take into consideration how these laws sit within an economic and societal context.

Policymakers around the world have been studying the EU's General Data Protection Regulation (GDPR) and other regional and national frameworks or laws to inform their own legislative proposals. Among the lessons learned are that smart data privacy rules are:

- Horizontal, meaning they apply to all processing of personal data rather than focusing on just one technology or sector. This reduces the need for sectoral rules or operating licences that subject network operators to an additional set of competing privacy obligations.
- Principles-based, allowing innovation to thrive without having to reinvent the rules every time new technologies or business methods are introduced.
- Risk-based, encouraging companies to focus on preventing harm (for example, by setting a threshold for reporting of data breaches rather than mandating that all breaches are reported), or encouraging organisations to implement privacy-by-design and privacy impact assessment processes.
- Based on the idea of accountability, holding companies to account, but allowing them to innovate and comply in a way that makes sense for their business and rewarding those that embed a culture of privacy in their organisations.
- Open to data flows, allowing data to cross borders provided there are sufficient safeguards to protect an individual's privacy (see the Cross-Border Flows of Data section in this handbook).

## Mobile Privacy Principles

The GSMA has published a set of universal Mobile Privacy Principles, which describe how mobile consumers' privacy should be respected and protected.

- **Openness, transparency and notice**
  Responsible persons (e.g., application or service providers) shall be open and honest with users and will ensure users are provided with clear, prominent and timely information regarding their identity and data privacy practices.
- **Purpose and use**
  The access, collection, sharing, disclosure and further use of personal information shall be limited to legitimate business purposes, such as providing applications or services as requested by users, or to otherwise meet legal obligations.
- **User choice and control**
  Users shall be given opportunities to exercise meaningful choice and control over their personal information.
- **Data minimisation and retention**
  Only the minimum personal information necessary to meet legitimate business purposes should be collected and otherwise accessed and used. Personal information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal retention obligations.
- **Respect user rights**
  Users should be provided with information about, and an easy means to exercise, their rights over the use of their personal information.
- **Security**
  Personal information must be protected, using reasonable safeguards appropriate to the sensitivity of the information.
- **Education**
  Users should be provided with information about privacy and security issues and ways to manage and protect their privacy.
- **Children and adolescents**
  An application or service that is directed at children and adolescents should ensure that the collection, access and use of personal information is appropriate in all given circumstances and is compatible with national law.

# Privacy and Big Data

## Background

Increases in computing power and falling prices of information technology systems make it possible to process huge volumes of data, from a variety of sources and in a range of formats, at greater speed than ever before. As a result, it is now possible to analyse all of the data from one or more large datasets, rather than relying on smaller samples of data. Importantly, this allows meaningful insights to be drawn, where appropriate, from mere correlations in the data rather than having to identify causal connections. These capabilities are often referred to as Big Data analytics techniques.

At the same time, the Internet of Things (IoT) is equipping an ever-increasing number of devices with sensors that collect and communicate data.

Together, these capabilities represent a sea change in society's ability not only to create new products and services, but also to solve some of the most pressing public policy needs of our time — from road management in congested and polluted urban areas to understanding and preventing the spread of diseases.

Mobile network operators (MNOs) will increasingly use the information they collect for Big Data initiatives. They have an important role to play as responsible stewards of that data and potentially as facilitators in a future marketplace for access to this type of data.

However, Big Data capabilities also give rise to questions about security and privacy and how these important concerns can be addressed.

## Debate

*How can MNOs and policymakers help society realise the benefits of Big Data analytics in a privacy protective manner and in compliance with applicable laws?*

---

*How can the GSMA further trust among stakeholders involved in the collection and analytics of data?*

---

## Industry Position

**The mobile industry recognises the societal benefits that can result from Big Data and wants to unlock the huge potential of Big Data analytics in a way that respects well-established privacy principles and fosters an environment of trust.**

New laws are not necessary to address Big Data analytics and the IoT. Rather, MNOs recognise that existing privacy principles apply in these areas. Rules that restrict the legitimate use of data or metadata should be qualified and proportional to the risk of privacy harm that consumers might suffer if their data is misused. These rules should also be applied consistently across different industry sectors and types of technology.

MNOs are well-placed to understand the potential risks to individuals and groups from Big Data analytics and can implement measures to avoid or mitigate those risks.

New insights derived from the data will often give rise to new uses — or 'purposes of processing' — that had not been considered or identified when the data was initially collected. Accordingly, privacy frameworks must recognise this potential and make such uses possible.

MNOs can address these types of challenges and increase trust between industry stakeholders and consumers by:

- Building on previous privacy initiatives, such as the GSMA Mobile Privacy Principles and the Privacy Design Guidelines for Mobile Application Development.
- Finding innovative ways to provide meaningful choice, control and transparency to individuals about what data is collected and how it is used. For example, this could be addressed through user-friendly dashboards or signals from IoT devices that are easily discoverable by smartphones.
- Thinking carefully about the impact on individuals (and groups) of the insights derived from Big Data and the actions or decisions that may be taken based on those insights.
- Reducing the risk of re-identification of individuals after data has been processed where this may raise privacy concerns.
- Establishing clarity on responsibilities between parties when collaborating on Big Data analytics projects.
- Incorporating ethical decision-making into governance models.

Equally, governments can ensure their country and citizens gain the most benefit from the potential of Big Data by:

- Understanding how Big Data analytics works and the context in which it takes place.
- Accommodating innovative approaches to transparency and consent.
- Developing and adopting practical industry guidelines and self-regulatory measures that seek to harness, rather than hinder, Big Data analytics.

Resources:
GSMA Report: Mobile Privacy and Big Data Analytics
GSMA Report: Mobile Privacy Principles — Promoting Consumer Privacy in the Mobile Ecosystem
GSMA Privacy Design Guidelines for Mobile Applications website
OECD Data-driven Innovation for Growth and Well-being website
FTC Report: Big Data — A Tool for Inclusion or Exclusion?

# Signal Inhibitors (Jammers)

## Background

Signal inhibitors, also known as jammers, are devices that generate interference or otherwise intentionally disrupt communication services. In the case of mobile services, they interfere with the communication between the mobile terminal and the base station. Their use by private individuals is banned in countries such as Australia, the United Kingdom and the United States.

In some regions, such as Latin America, signal inhibitors are used to prevent the illegal use of mobile phones in specific locations, such as prisons. However, blocking the signal does not address the root cause of the problem — wireless devices illegally ending up in the hands of inmates who then use them for illegal purposes.

Moreover, signal inhibitors don't prevent mobile devices from connecting to Wi-Fi networks, as they don't affect the frequency bands used by Wi-Fi routers. As a result, signal inhibitors don't block people from using over-the-top voice applications to make calls to phone networks.

Mobile network operators invest heavily to provide coverage and capacity through the installation of radio base stations. However, the indiscriminate use of signal inhibitors compromises these investments by causing extensive disruption to the operation of mobile networks, reducing coverage and leading to the deterioration of service for consumers.

## Debate

*Should governments or private organisations be allowed to use signal inhibitors that interfere with the provision of mobile voice and data services to consumers?*

---

*Should the marketing and sale of signal inhibitors to private individuals and organisations be prohibited?*

---

## Industry Position

**In some Latin American countries, such as Colombia, El Salvador, Guatemala and Honduras, governments are promoting the deployment of signal inhibitors to limit the use of mobile services in prisons. The GSMA and its members are committed to working with governments to use technology as an aid for keeping mobile phones out of sensitive areas, as well as cooperating on efforts to detect, track and prevent the use of smuggled devices.**

However, it is vital that a long-term, practical solution is found that doesn't negatively impact legitimate users, nor affect the substantial investments that mobile operators have made to improve their coverage.

The nature of radio signals makes it virtually impossible to ensure that the interference generated by inhibitors is confined, for example, within the walls of a building. Consequently, the interference caused by signal inhibitors affects citizens, services and public safety. It restricts network coverage and has a negative effect on the quality of services delivered to mobile users. Furthermore, inhibitors cause problems for other critical services that rely on mobile communications. For example, during an emergency they could limit the ability of mobile users to contact emergency services via numbers such as 999, 911 or 112, and they can interfere with the operation of mobile-connected alarms or personal health devices.

The industry's position is that signal inhibitors should only be used as a last resort and only deployed in coordination with operators. This coordination must continue for the total duration of the deployment of the devices — from installation through to deactivation — to ensure that interference is minimised in adjacent areas and legitimate mobile phone users are not affected.

Furthermore, to protect the public interest and safeguard the delivery of mobile services, regulatory authorities should ban the use of signal inhibitors by private entities and establish sanctions for private entities that use or commercialise them without permission from relevant authorities. The import and sale of inhibitors or jammers must be restricted to those considered qualified and authorised to do so and their operation must be authorised by the national telecommunications regulator.

Nevertheless, strengthening security to prevent wireless devices being smuggled into sensitive areas, such as prisons, is the most effective measure against the illegal use of mobile devices in these areas, as it would not affect the rights of legitimate users of mobile services.

Resources:
GSMA Public Policy Position: Signal Inhibitors in Latin America
GSMA Report: Signal-Blocking Solutions — Use of Jammers in Prisons
GSMA Report: Safety, Privacy and Security Across the Mobile Ecosystem

## GSMA Intelligence

GSMA Intelligence is an extensive and growing resource for GSMA members, associate members and other organisations interested in understanding the mobile industry. Through industry data collection and aggregation, market research and analysis, GSMA Intelligence provides a valuable view of the mobile industry, and the wider mobile ecosystem, around the globe.

### Global coverage

GSMA Intelligence publishes data and insights spanning 240 markets, 1,400 mobile network operators and over 1,300 mobile virtual network operators (MVNOs). Comprising more than 30 million individual data points, GSMA Intelligence combines historical and forecast data from the beginnings of the industry in 1979 with forecasts out to 2025. New data is added every day.

### Numerous data types

The data includes metrics on mobile subscribers and connections, operational and financial data, and socio-economic measures that complement the core data sets. Primary research conducted by the GSMA adds insight into more than 4,600 network deployments to date. White papers and reports from across the GSMA and weekly bulletins are also available as part of the service.

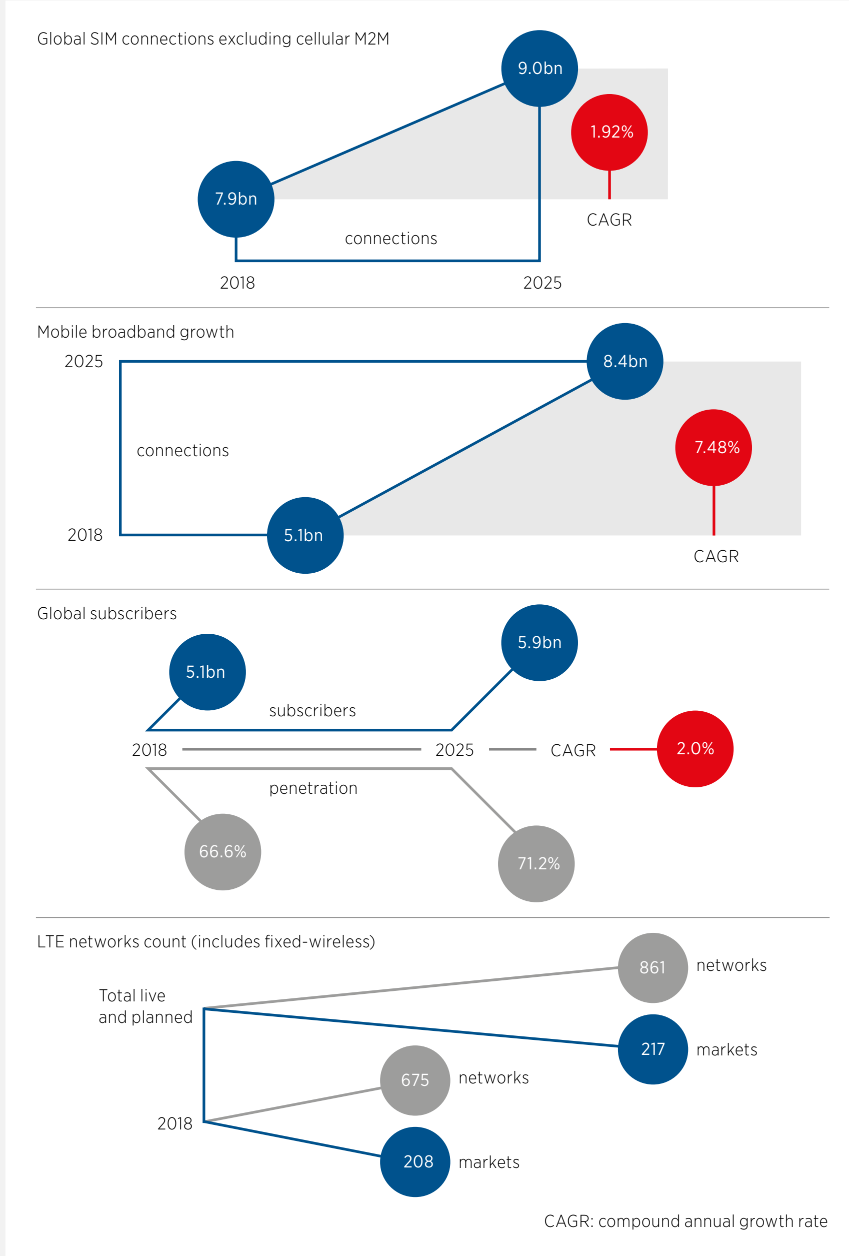
### Powerful data tools

Information in GSMA Intelligence is made easy to use by a range of data-selection tools: multifaceted search, rankings, filters, dashboards, a real-time data and news feed, as well as the ability to export data into Excel and add graphs and charts to presentations.

**https://gsmaintelligence.com**
**info@gsmaintelligence.com**

## Global Market

Source: GSMA



## Unique subscriber penetration by region

Source: GSMA Intelligence

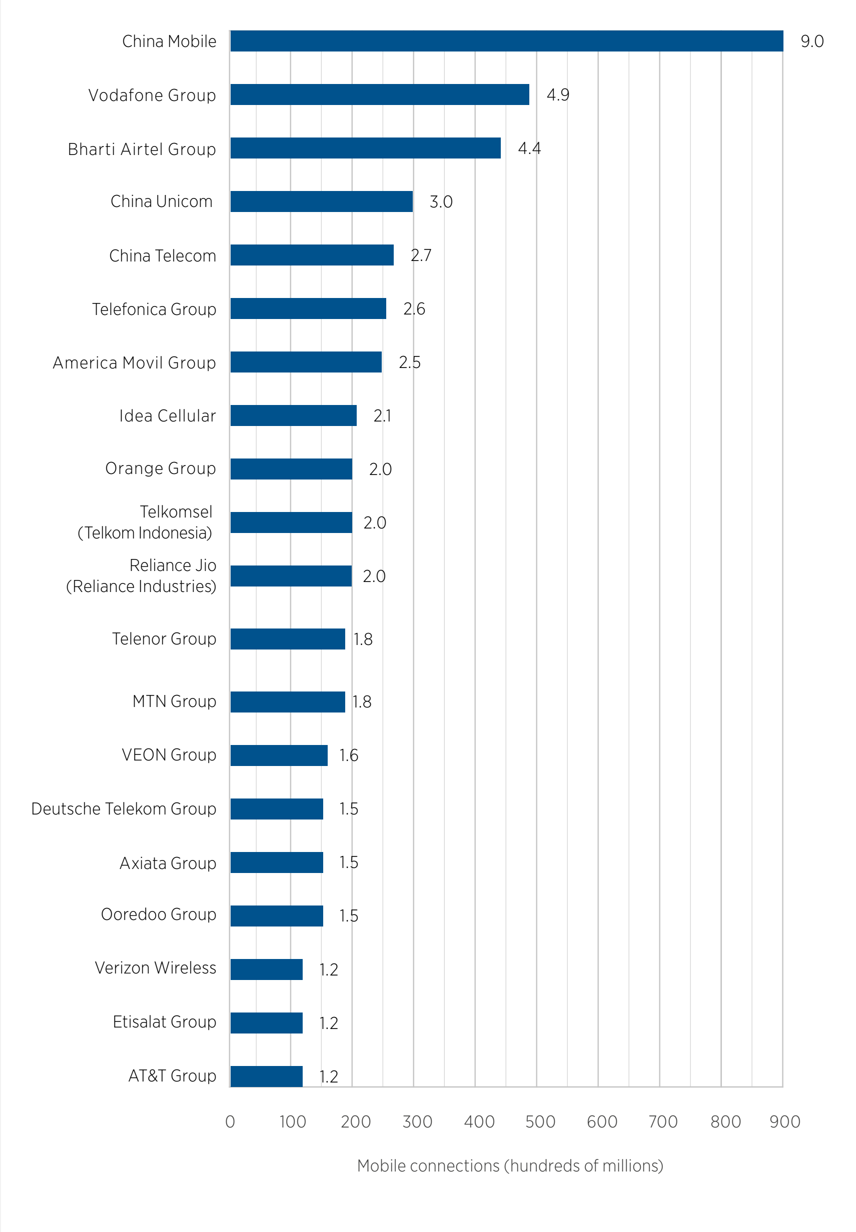
The global unique subscriber base grew by 3.1 per cent in the previous 12 months. This growth is forecast to continue, but at a slower rate of two per cent until 2025. Growth is far from uniform across the regions of the world and is now largely driven by developing markets, which are forecast to add over 706 million subscribers over the next six years, compared to only 64 million new additions in developed markets over the same period.

Unique subscriber penetration rates vary significantly across regions. Europe has the highest penetration rate on average, followed by North America and then the Commonwealth of Independent States (CIS). Sub-Saharan Africa had the lowest penetration rate in 2018 at 45 per cent of the population, despite having seen the fastest subscriber growth of any region over the past decade.



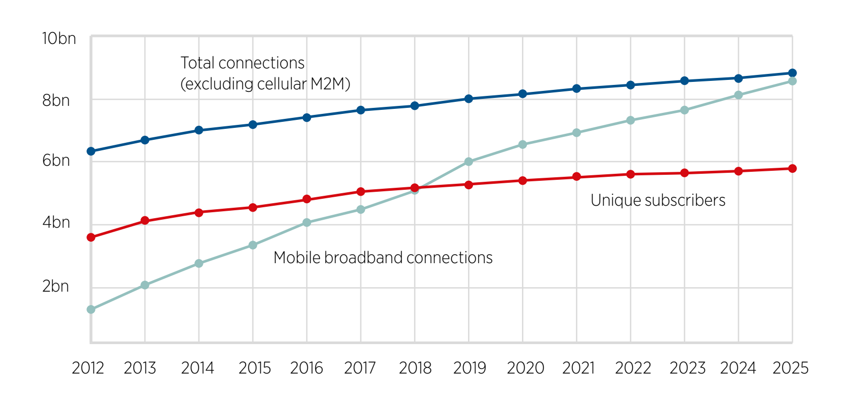

## Mobile operator group global ranking by connections Q2 2018

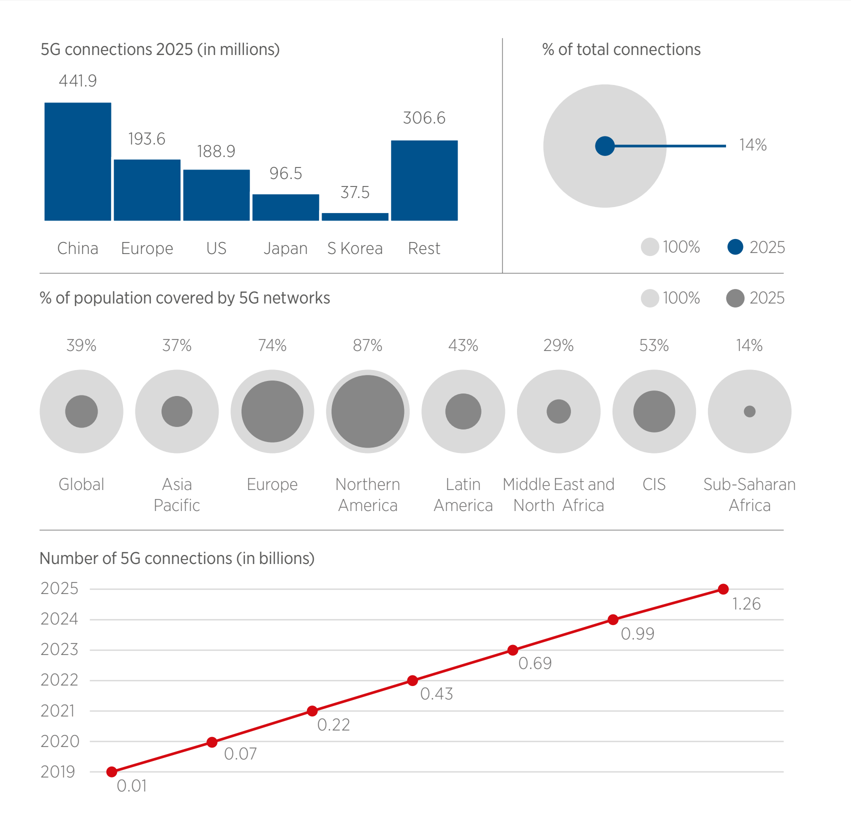
Source: GSMA Intelligence, company reports



## Global connection trends

Source: GSMA Intelligence

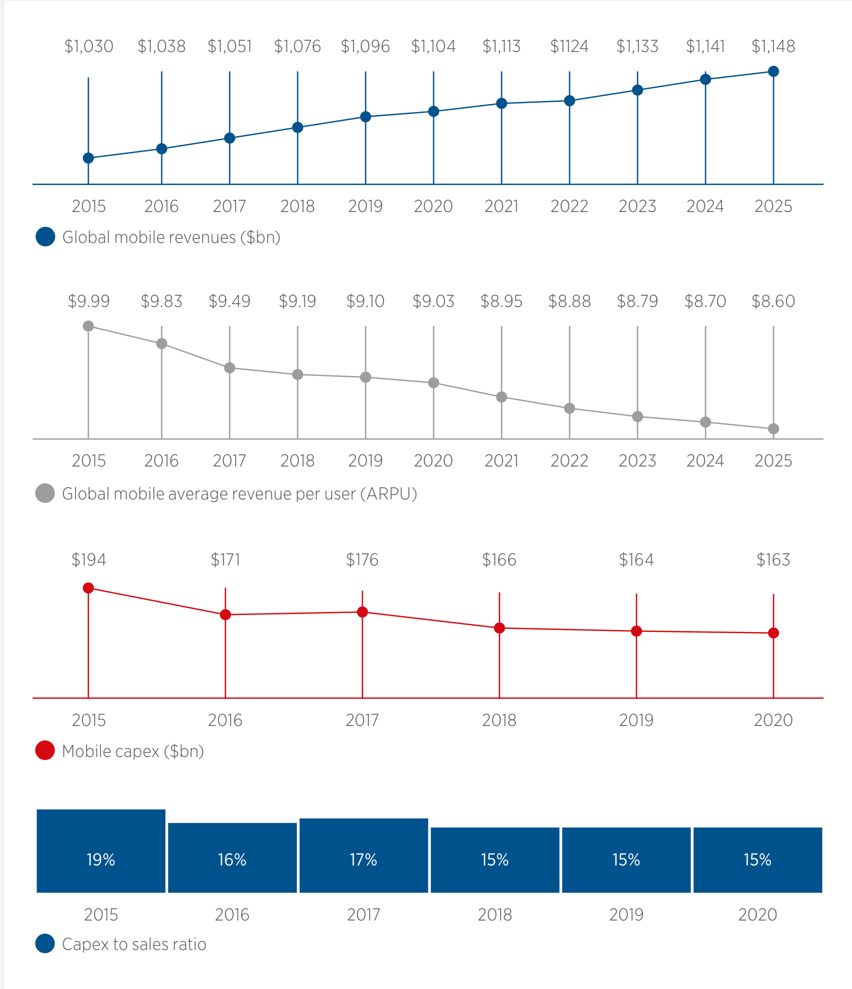



## Financial Data

GSMA Intelligence forecasts that between 2018 and 2025, mobile operators will grow revenues by a CAGR of 0.8 per cent to reach $1.15 trillion. Slowing subscriber growth, coupled with declining levels of ARPU are the prime factors driving this trend.

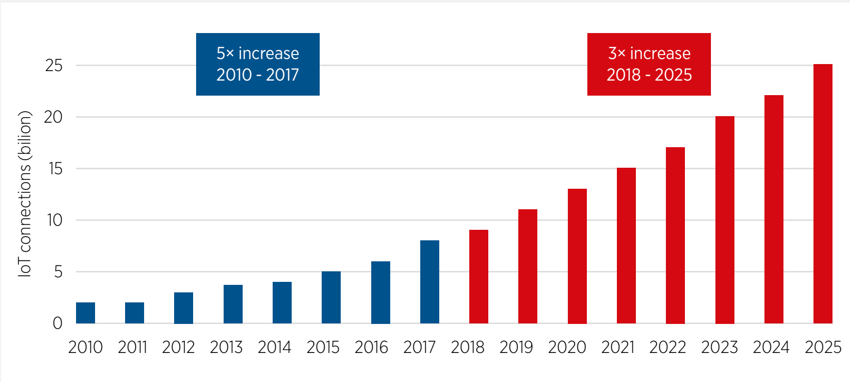
Between 2018 and 2020, mobile operators across the world will spend $492 billion on capex, compared to $541 billion over the preceding three years. The key reason for the disparity is the large decline in capex in China following the completion of 4G rollout in the country; the combined annual capex for Chinese operators during 2016 was almost $18 billion lower than the annual average between 2013 and 2015.



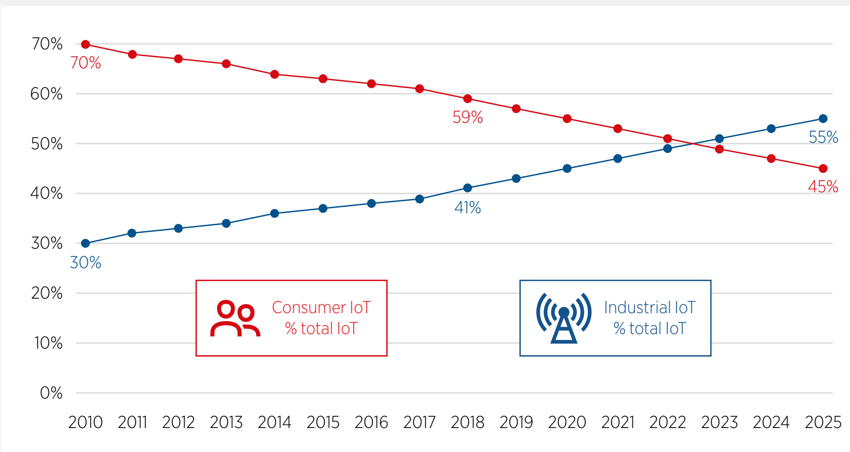
GSMA Intelligence forecasts that the total number of IoT connections (cellular and non-cellular) globally will reach 25.2 billion in 2025, up from nine billion in 2018. The size of the market will triple over the forecast period.

While IoT is rapidly becoming a mainstream technology in consumer markets (for consumer electronics and smart home devices), the industrial IoT segment will be the largest source of connections growth in the future.

### Total IoT connections, 2010-2025




### Consumer IoT vs Industrial IoT connections as proportion of total IoT

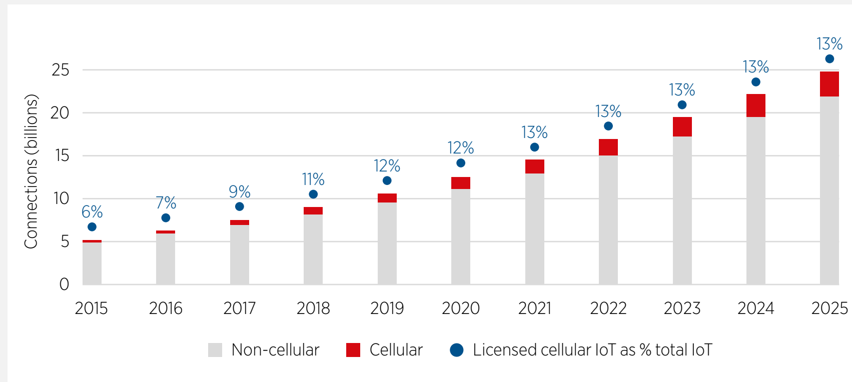



### Definition

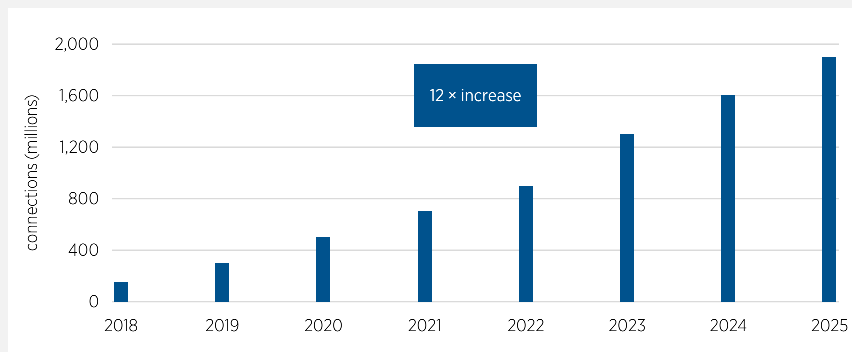
GSMA Intelligence defines Internet of Things (IoT) devices as those capable of two-way data transmission (excluding passive sensors and RFID tags). It includes connections using multiple communication methods such as cellular and short-range connectivity. It excludes PCs, laptops, tablets, e-readers, data terminals and smartphones.

The majority of IoT devices — typically in indoor environments — will be connected by unlicensed radio technologies designed for short-range connectivity. These include technologies such as Wi-Fi, Z-Wave and ZigBee. IoT devices that require mobility, lower latency and ultra reliability will primarily be connected by cellular networks using licensed spectrum. Cellular networks address the need for more secure, managed connectivity allowing devices to connect directly to the cloud (as opposed to a gateway). Managed connectivity will be one of the key drivers of growth. Licenced LPWA networks enable a slew of IoT devices that require longer battery life and lower data throughputs to be connected. Currently, there are 62 commercial launches of mobile IoT across several countries, including the US, China and parts of Europe. GSMA Intelligence forecasts that by 2025, propelled by the growth of NB-IoT and LTE-M, licensed cellular networks will serve 3.3 billion IoT connections globally or 13 per cent of the total number of IoT connections. The growth in licenced LPWA connections is particulary noteworthy — GSMA Intelligence expects it to account for almost 60 per cent of total licenced IoT connections, representing a twelvefold increase between 2018 and 2025.

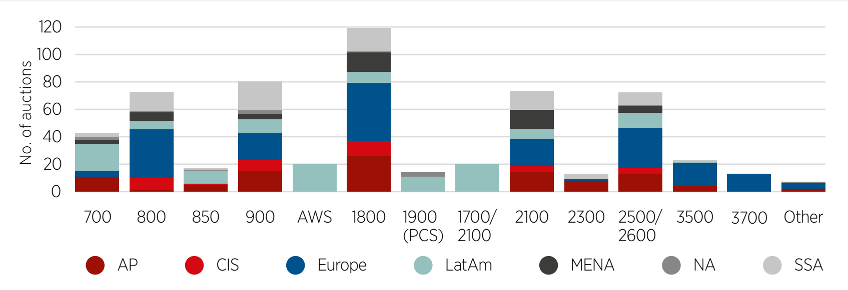
### IoT connections by technology, cellular share of total IoT




### Licensed LPWA connections

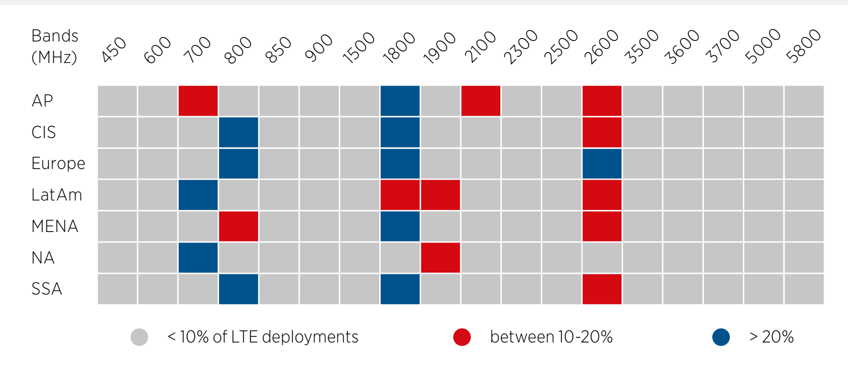


## Spectrum assignments across regions by bands, 2013-2018

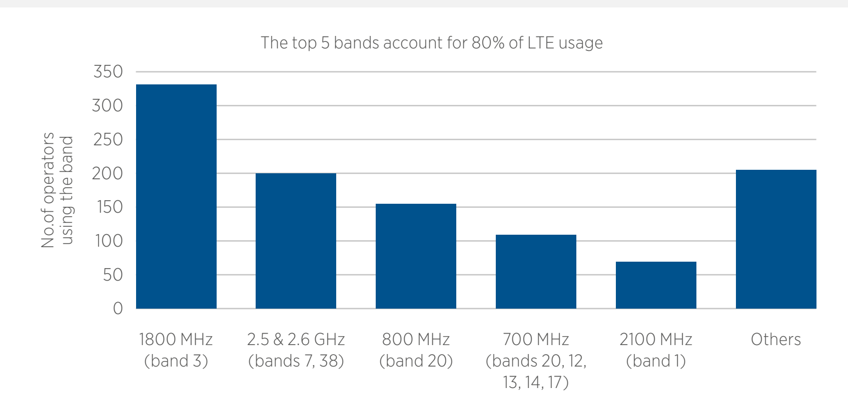



## Share of LTE deployments by frequency band, by region (July 2018)

Source: GSMA Intelligence



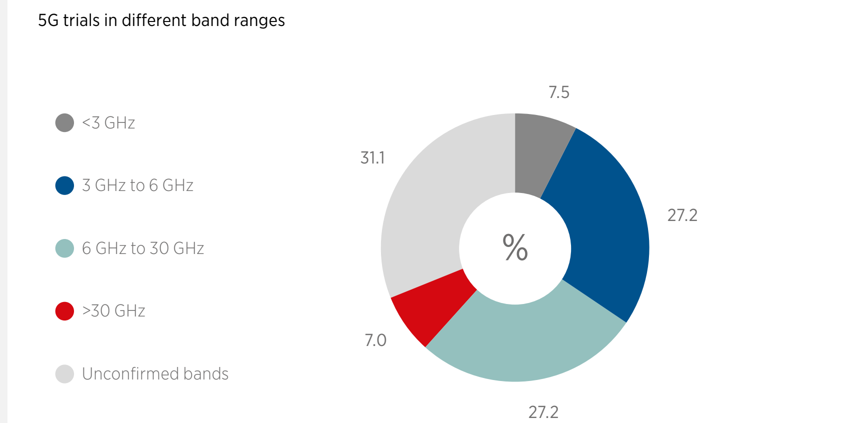

## Frequency Bands used for LTE (July 2018)




## mmWave bands that will be used for initial 5G deployments

| Region | Band (GHz) |
|---|---|
| Europe | 24.25-27.5 GHz, 40.5-43.5 GHz |
| China | 24.25-27.5 GHz, 3 GHz in 37-43.5 GHz |
| Korea | 24.25-29.5 GHz, 3 GHz in 37-43.5 GHz |
| Japan | 24.25-29.5 GHz, 3 GHz in 37-43.5 GHz |
| US | 24.25-25.25 GHz, 27.5-28.35 GHz, 37-40 GHz |

## Trials in a range of spectrum bands




**121 operators**

are trialling
5G technology across

**61 countries**

**73 operators**

have announed plans to launch
5G services across

**46 countries**

Amount of MHz licensed for mobile use around the world (July 2018)

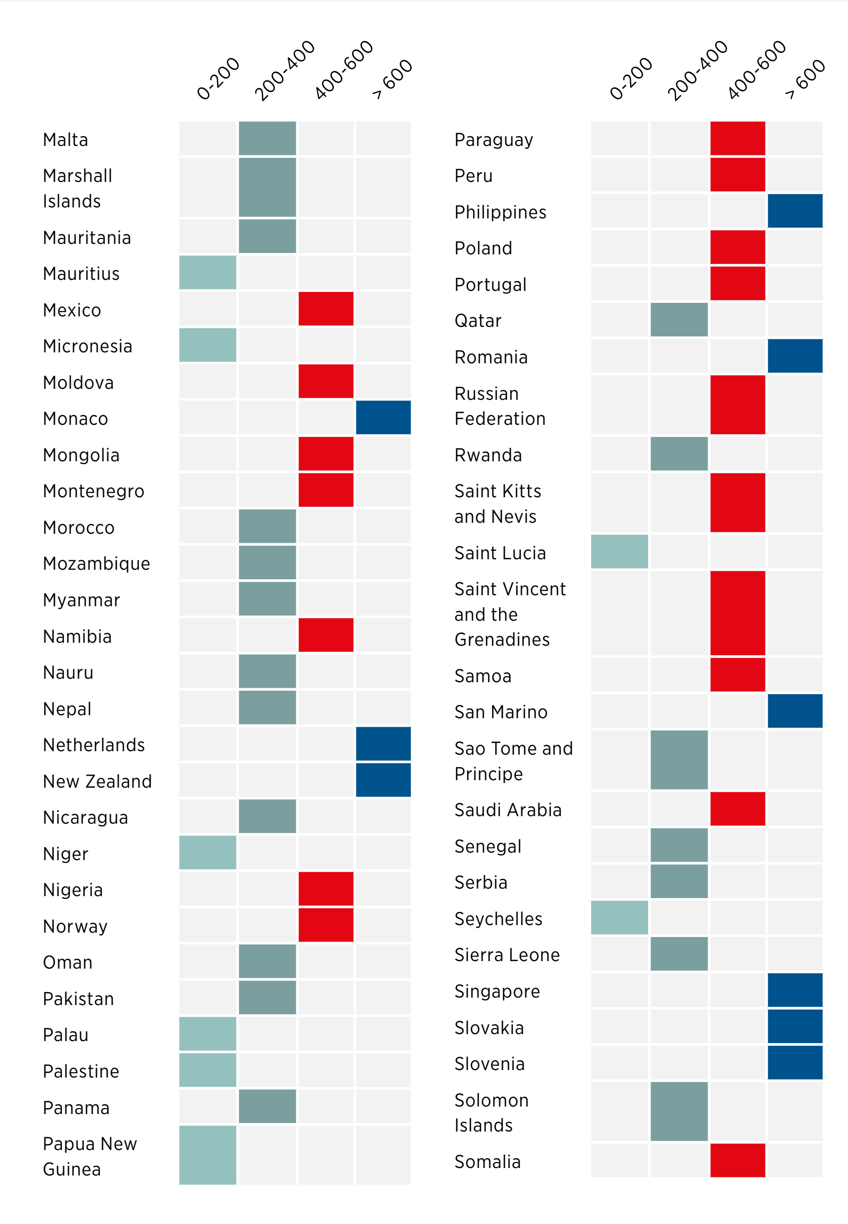
| | 0-200 | 200-400 | 400-600 | > 600 |
|---|---|---|---|---|
| Afghanistan | | ■ | | |
| Albania | | | ■ | |
| Algeria | | ■ | | |
| Andorra | | | | ■ |
| Angola | | ■ | | |
| Antigua and Barbuda | | | ■ | |
| Argentina | | | ■ | |
| Armenia | | ■ | | |
| Australia | | | ■ | |
| Austria | | | | ■ |
| Azerbaijan | | ■ | | |
| Bahamas | | ■ | | |
| Bahrain | | ■ | | |
| Bangladesh | | ■ | | |
| Barbados | | ■ | | |
| Belarus | | ■ | | |
| Belgium | | | ■ | |
| Belize | ■ | | | |
| Benin | | | ■ | |
| Bhutan | | ■ | | |
| Bolivia | | ■ | | |
| Bosnia and Herzegovina | | ■ | | |
| Botswana | ■ | | | |
| Brazil | | | ■ | |
| Brunei Darussalam | ■ | | | |
| Bulgaria | | ■ | | |
| Burkina Faso | | ■ | | |

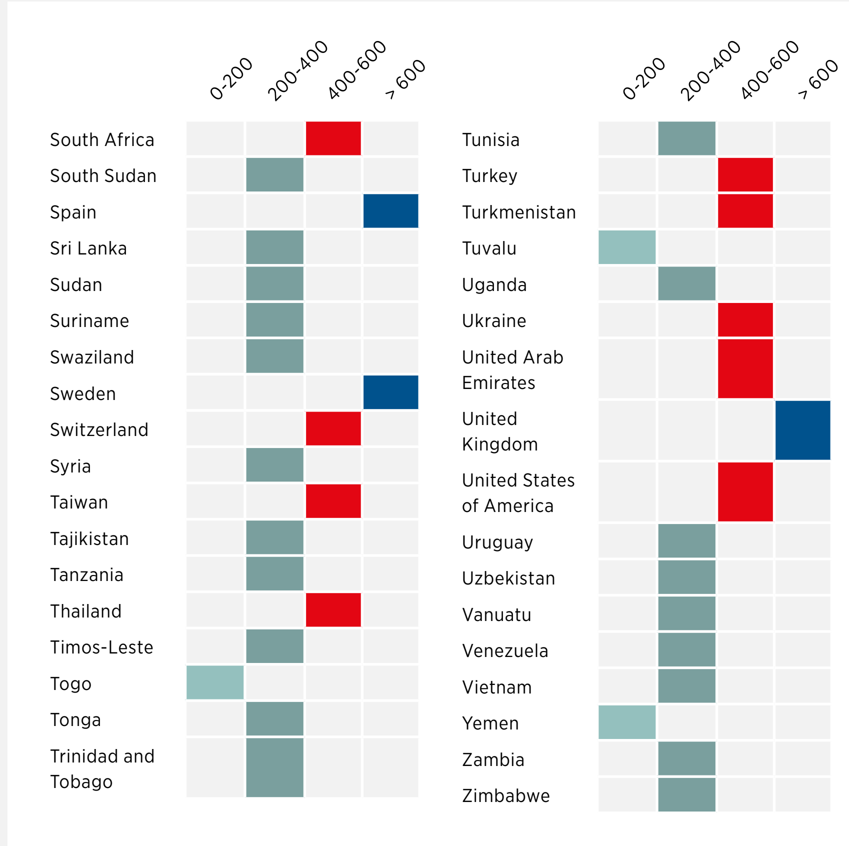
| | 0-200 | 200-400 | 400-600 | > 600 |
|---|---|---|---|---|
| Burundi | ■ | | | |
| Cabo Verde | | ■ | | |
| Cambodia | | ■ | | |
| Cameroon | | ■ | | |
| Canada | | | ■ | |
| Central African Rep. | | ■ | | |
| Chad | | ■ | | |
| Chile | | | ■ | |
| China | | | ■ | |
| Colombia | | | ■ | |
| Comoros | ■ | | | |
| Congo | | ■ | | |
| Congo, Dem. Rep. | | ■ | | |
| Costa Rica | | ■ | | |
| Cote d'Ivoire | | | ■ | |
| Croatia | | ■ | | |
| Cuba | ■ | | | |
| Cyprus | | | ■ | |
| Czech Rep. | | | | ■ |
| Denmark | | | | ■ |
| Djibouti | ■ | | | |
| Dominica | | | ■ | |
| Dominican Rep. | | ■ | | |
| Ecuador | | ■ | | |
| Egypt | | ■ | | |
| El Salvador | ■ | | | |

| | 0-200 | 200-400 | 400-600 | > 600 |
|---|---|---|---|---|
| Equatorial Guinea | ■ | | | |
| Eritrea | ■ | | | |
| Estonia | | | | ■ |
| Ethiopia | ■ | | | |
| Fiji | | ■ | | |
| Finland | | | | ■ |
| France | | | | ■ |
| Gabon | ■ | | | |
| Gambia | ■ | | | |
| Georgia | | ■ | | |
| Germany | | | | ■ |
| Ghana | | | ■ | |
| Greece | | | ■ | |
| Grenada | | | ■ | |
| Guatemala | | ■ | | |
| Guinea | ■ | | | |
| Guinea-Bissau | ■ | | | |
| Guyana | ■ | | | |
| Haiti | ■ | | | |
| Honduras | | ■ | | |
| Hong Kong | | | ■ | |
| Hungary | | | ■ | |
| Iceland | | | ■ | |
| India | | ■ | | |
| Indonesia | | | ■ | |
| Iran | | ■ | | |
| Iraq | | ■ | | |
| Ireland | | | | ■ |

| | 0-200 | 200-400 | 400-600 | > 600 |
|---|---|---|---|---|
| Israel | | ■ | | |
| Italy | | | | ■ |
| Jamaica | ■ | | | |
| Japan | | | | ■ |
| Jordan | | ■ | | |
| Kazakhstan | | ■ | | |
| Kenya | | ■ | | |
| Kiribati | ■ | | | |
| Korea, North | ■ | | | |
| Korea, South | | | | ■ |
| Kosovo | ■ | | | |
| Kuwait | | ■ | | |
| Kyrgyzstan | | | ■ | |
| Laos | | ■ | | |
| Latvia | | | | ■ |
| Lebanon | ■ | | | |
| Lesotho | ■ | | | |
| Liberia | | ■ | | |
| Libya | | ■ | | |
| Liechtenstein | | | ■ | |
| Lithuania | | | ■ | |
| Luxembourg | | | ■ | |
| Macau | ■ | | | |
| Macedonia | | ■ | | |
| Madagascar | | ■ | | |
| Malawi | | ■ | | |
| Malaysia | | | ■ | |
| Maldives | | ■ | | |
| Mali | ■ | | | |

Amount of MHz licensed for mobile use around the world (cont.)




Amount of spectrum in some countries was estimated by GSMA Intelligence

## Global LTE frequency bands

| Band Number | Type | Mhz | Name | Uplink | Downlink | Regions |
|---|---|---|---|---|---|---|
| 1 | FDD | 2100 | IMT Core Band | 1920 – 1980 | 2110 – 2170 | Global except N America |
| 2 | FDD | 1900 | PCS 1900 | 1850 – 1910 | 1930 – 1990 | Americas, Asia |
| 3 | FDD | 1800 | 1800 | 1710 – 1785 | 1805 – 1880 | Global except Americas |
| 4 | FDD | 1700 | AWS | 1710 – 1755 | 2110 – 2155 | Americas |
| 5 | FDD | 850 | 850 | 824 – 849 | 869 – 894 | Americas, APAC |
| 7 | FDD | 2600 | IMT-Extension | 2500 – 2570 | 2620 – 2690 | Global except N America |
| 8 | FDD | 900 | E-GSM | 880 – 915 | 925 – 960 | Global except N America |
| 9 | FDD | 1800 | Japan UMTS 1700 / Japan DCS | 1749.9 – 1784.9 | 1844.9 – 1879.9 | Japan |
| 10 | FDD | 1700 | Extended AWS blocks A-I | 1710 – 1770 | 2110 – 2170 | Americas |
| 11 | FDD | 1500 | Lower PDC | 1427.9 – 1447.9 | 1475.9 – 1495.9 | Japan |
| 12 | FDD | 700 | Lower SMH blocks A/B/C | 699 – 716 | 729 – 746 | N America |
| 13 | FDD | 700 | Upper SMH block C | 777 – 787 | 746 – 756 | N America |
| 14 | FDD | 700 | Upper SMH block D | 788 – 798 | 758 – 768 | N America |
| 17 | FDD | 700 | Lower SMH blocks B/C | 704 – 716 | 734 – 746 | N America |
| 18 | FDD | 850 | Japan lower 800 | 815 – 830 | 860 – 875 | Japan |
| 19 | FDD | 850 | Japan upper 800 | 830 – 845 | 875 – 890 | Japan |
| 20 | FDD | 800 | EU Digital Dividend | 832 – 862 | 791 – 821 | Europe, Middle East, Africa |
| 21 | FDD | 1500 | Upper PDC | 1447.9 – 1462.9 | 1495.9 – 1510.9 | Japan |
| 22 | FDD | 3500 | FDD 3500 | 3410 – 3490 | 3510 – 3590 | n/a |
| 23 | FDD | 2000 | S-Band (AWS-4) | 2000 – 2020 | 2180 – 2200 | N America |
| 24 | FDD | 1600 | L-Band (US) | 1626.5 – 1660.5 | 1525 – 1559 | n/a |
| 25 | FDD | 1900 | Extended PCS blocks A-G | 1850 – 1915 | 1930 – 1995 | N America |
| 26 | FDD | 850 | Extended CLR | 814 – 849 | 859 – 894 | N America |
| 27 | FDD | 850 | SMR | 807 – 824 | 852 – 869 | N America |
| 28 | FDD | 700 | APT | 703 – 748 | 758 – 803 | Latin America, APAC |
| 29 | FDD* | 700 | Lower SMH blocks D/E | N/A | 717 – 728 | N America |
| 30 | FDD | 2300 | WCS blocks A/B | 2305 – 2315 | 2350 – 2360 | N America |
| 31 | FDD | 450 | LTE 450 Brazil | 452.5 – 457.5 | 462.5 – 467.5 | Brazil |
| 32 | FDD* | 1500 | L-Band (EU) | N/A | 1452 – 1496 | Europe |
| 33 | TDD | 2100 | TDD 2000 Lower | 1900 – 1920 | | Global except N America |
| 34 | TDD | 2100 | TDD 2000 Upper | 2010 – 2025 | | Global except N America |
| 37 | TDD | 1900 | PCS Center Gap | 1910 – 1930 | | Global (certain countries) |
| 38 | TDD | 2600 | IMT Extension Gap | 2570 – 2620 | | Global except N America |
| 39 | TDD | 1900 | China TDD 1900 | 1880 – 1920 | | China |

## Global LTE frequency bands (cont.)

| Band Number | Type | Mhz | Name | Uplink | Downlink | Regions |
|---|---|---|---|---|---|---|
| 40 | TDD | 2300 | TDD 2300 | 2300 – 2400 | | Global (certain countries) |
| 41 | TDD | 2500 | BRS / EBS | 2496 – 2690 | | N America, China, Japan |
| 42 | TDD | 3500 | C-band | 3400 – 3600 | | Global |
| 43 | TDD | 3700 | C-band | 3600 – 3800 | | Europe |
| 44 | TDD | 700 | APT | 703 – 803 | | n/a |
| 45 | TDD | 1500 | L-Band (China) | 1447 – 1467 | | n/a |
| 46 | TDD | 5200 | NII | 5150 – 5925 | | n/a |
| 47 | TDD | 5900 | V2X | 5855 – 5925 | | n/a |
| 48 | TDD | 3500 | US CBRS 3500 | 3550 – 3700 | | n/a |
| 49 | TDD | 3500 | eLAA 3500 | 3550 – 3700 | | n/a |
| 50 | TDD | 1500 | TDD L-band | 1432 – 1517 | | n/a |
| 51 | TDD | 1500 | TDD L-band | 1427 – 1432 | | n/a |
| 52 | TDD | 3300 | TDD 3300 | 3300 – 3400 | | n/a |
| 65 | FDD | 2100 | Extended IMT | 1920 – 2010 | 2110 – 2200 | n/a |
| 66 | FDD | 1700 | Extended AWS blocks A-J (AWS-1/AWS-3) | 1710 – 1780 | 2110 – 2200 | n/a |
| 67 | FDD* | 700 | EU 700 | N/A | 738 – 758 | Europe |
| 68 | FDD | 700 | ME 700 | 698 – 728 | 753 – 783 | Middle East |
| 69 | FDD* | 2600 | IMT-E (duplex spacing) | N/A | 2570 – 2620 | n/a |
| 70 | FDD | 1700 | AWS-3 A1/B1 + EPCS H | 1695 – 1710 | 1995 – 2020 | n/a |
| 71 | FDD | 600 | US 600 | 663 – 696 | 617 – 652 | n/a |
| 72 | FDD | 450 | 450 EU BB-PPDR | 451 – 456 | 461 – 466 | n/a |
| 73 | FDD | 450 | 450 Region 3 | 450 – 455 | 460 – 465 | n/a |
| 74 | FDD | 1500 | FDD L-band | 1427 – 1470 | 1475 – 1517 | n/a |
| 75 | FDD* | 1500 | Extended SDL L-band | n/a | 1432 – 1517 | n/a |
| 76 | FDD* | 1500 | Extended SDL L-band | n/a | 1427 – 1432 | n/a |

* Supplemental Downlink only

ISBN 978-1-9998932-2-4

www.gsma.com/publicpolicy/handbook