Mobile Policy Handbook

An insider's guide to the issues

2017

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

A country's citizens benefit most when the private and public sectors work together in a spirit of openness and trust. This is why the GSMA is 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 fifth edition of the Mobile Policy Handbook, a number of new sections have been added, including one on the Sustainable Development Goals that reflects the mobile industry's commitment to the UN 2030 Agenda. New policy topics and industry positions have been introduced on privacy and Big Data, service restriction orders, smart cities, and spectrum for the Internet of Things. 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

Two technologies have transformed the lives of billions of people over the past two decades: mobile communications and the internet. Initially, these technologies developed in parallel, but now they are on a fully converged path.

This convergence is having a profound impact on the daily lives of billions of people around the world. For example, ubiquitous mobile broadband connectivity and the mass adoption of increasingly powerful smartphones are the key enablers of the rise of the sharing economy, which is changing the way many people consume goods and services.

Equally profound is the revolution in machine-to-machine (M2M) communications. We are still at the beginning of this development, but already billions of automated messages flow between widely connected devices, over the internet.

These dominant trends drive much of the GSMA's work with policymakers, bringing into new focus issues such as data protection and privacy, the Internet of Things, network economics and mobile government. Never before have the roles of the communications ministry and regulator been so critical to the success of national economic and social policies — with implications for business, education, health, access to financial and government services, and so much more.

As the mobile internet becomes the key to the transformation of many other sectors, policymakers face new and exciting challenges and will need to navigate uncharted waters. We hope this handbook provides a compass that is referred to regularly on that voyage.

#betterfuture

The UN's 2030 Agenda for Sustainable Development was unanimously adopted by world leaders at a historic summit in September 2015. The agenda details 17 Sustainable Development Goals (SDGs) that act as the world's to-do list to end poverty, reduce inequalities and tackle climate change.

The mobile industry is playing a critical role in supporting efforts to deliver on these goals by working with governments and the international community to expand connectivity, lower barriers to access and ensure that tools and applications are developed with vulnerable communities in mind.

The GSMA has also launched the SDGs in Action mobile app, which can be downloaded from www.sdgsinaction.com. Developed in collaboration with the UN and Project Everyone, the app provides a global forum through which industry, governments and individual citizens can collectively realise the promise of the SDGs.

1. NO POVERTY
By expanding access to mobile internet and mobile money solutions for the unbanked, the industry is accelerating economic growth and helping move people out of poverty. A key ambition is to reduce the significant disparity in need between geographic regions.

2. ZERO HUNGER
Agriculture is the main contributor to GDP and the largest employer in emerging markets, but yields remain a third lower than in developed markets. Mobile connectivity enables smart solutions that increase the productivity and profitability of both smallholders and industrial farmers.

3. GOOD HEALTH AND WELLBEING
Over 400 million people currently do not have access to affordable healthcare. By providing connectivity and supporting innovative healthcare applications and services, the mobile industry is helping to increase the quality, reduce the cost and extend the reach of basic healthcare.

4. QUALITY EDUCATION
Mobile connectivity can increase access to education for people in even the most remote locations. A primary focus of these efforts is to ensure that education is inclusive of women and the poor.

5. GENDER EQUALITY

Currently, more than 1.7 billion females in low- and middle-income countries don't own mobile phones. The industry is working to reduce the gender gap in the use of mobile internet and mobile money services, and better connect women and girls to services, communities, information and opportunities.

6. CLEAN WATER AND SANITATION

Intelligent management solutions reduce consumption in the drive towards ensuring the availability of water and sanitation for all. Alternate payment solutions, such as those that rely on mobile money, are also helping deliver affordable utility services in emerging markets.

7. AFFORDABLE AND CLEAN ENERGY

Mobile connectivity can enable intelligent energy management to reduce consumption around the world. It can also help create new pathways and payment options to bring electricity supply to the 1.2 billion people globally who currently lack access.

8.DECENT WORK AND ECONOMIC GROWTH

Mobile connectivity creates jobs directly and indirectly by accelerating economic growth and enabling innovation. For example, 17 million jobs were directly supported by the mobile ecosystem in 2015, and this is expected to rise to 20 million by 2020.

9. INDUSTRY, INNOVATION AND INFRASTRUCTURE

The industry plays a significant role in developing infrastructure, both as a provider of critical infrastructure and as a catalyst for the evolution of other sectors, including industrial processes and manufacturing. Furthermore, by supporting enhanced information exchange, it helps foster research and development ecosystems.

10. REDUCED INEQUALITIES

For many marginalised groups, mobile is the first step to inclusive participation in a connected society. Mobile also has a key transformational role in providing formal identity and banking. For example, via mobile money services the industry increases financial inclusion and facilitates remittances that are affordable and widely accessible.

11. SUSTAINABLE CITIES AND COMMUNITIES

The mobile industry provides mission-critical communications for key services in every community. Mobile network operators provide life-saving connectivity in the face of natural disasters, conflict and war. Connectivity also drives innovation to reduce environmental footprints.

12. RESPONSIBLE CONSUMPTION AND PRODUCTION

Mobile connectivity helps foster collaboration and innovation, and is a key enabler of smart transportation solutions. The connectivity the industry provides enables intelligent insight to help people improve their consumption patterns and reduce their environmental impact.

13. CLIMATE ACTION

Mobile operators are reducing energy use and adopting more energy efficient practices. Our networks can be used for the sharing of best practice methodology and encourage the use of green technologies to reduce carbon emissions by approximately 40 million tonnes annually.

14. LIFE BELOW WATER

By providing the connectivity for environmental monitoring solutions that rely on Internet of Things technology, the mobile industry is helping conserve and sustain marine resources. The industry is also expanding connectivity to remote fishing communities to increase their access to market information.

15. LIFE ON LAND
Mobile networks are enabling smarter agriculture initiatives aimed at improving crop yields while reducing water consumption. Monitoring solutions that rely on mobile connectivity are also being used to prevent deforestation.

16. PEACE, JUSTICE AND STRONG INSTITUTIONS
Increased connectivity promotes understanding and tolerance by connecting different cultures and religions. Mobile networks make it easier for citizens to connect to their communities and institutions, establish an identity, participate in the formal economy and receive government services.

17. PARTNERSHIPS FOR THE GOALS
Mobile operators across the world have embraced the introduction of the UN Global Goals. The 2016 GSMA Mobile Industry Impact Report sets a benchmark through which the industry will assess its success in contributing to the Sustainable Development Goals (SDGs) and serves as a blueprint for other industries as they commit to achieving the SDGs.

Resources:
GSMA Report: 2016 Mobile Industry Impact — Sustainable Development Goals
GSMA App: Sustainable Development Goals — The SDGs in Action
Project Everyone website

Mobile for Development

The astonishing growth of mobile puts the industry in a unique position to enhance the lives of underserved people in emerging markets. More than 90 per cent of the one billion additional mobile subscribers forecast by 2020 will come from developing markets. Mobile has already become a powerful platform for digital and financial inclusion, as mobile networks are often the most widespread and reliable infrastructure in these markets, where huge swathes of the population are underserved by basic services.

For example, two billion people worldwide lack access to formal financial services, 1.8 billion lack access to improved sanitation, 643 million don't have access to electricity and 262 million rely on drinking water that hasn't been protected from outside contamination, yet the majority of these people live within areas that are covered by mobile networks.

By partnering with the mobile industry, governments and philanthropic communities, GSMA Mobile for Development (M4D) works to trial, develop and scale mobile solutions that can help address these gaps. To date, M4D has worked in more than 50 countries and reached 26 million individuals.

The M4D strategy focuses on the three key areas of connectivity, financial services and digital identity. It also continues to work to demonstrate the positive socio-economic impact mobile can have in areas such as healthcare provision, improving access to energy and water, and reducing the gender gap in the use of mobile services. Operators, other ecosystem players, governments and regulators all have a role to play in addressing these challenges. These efforts and more are detailed over the following pages.

Connected Society

Background

Approximately 62 per cent of the world's population is not connected to the internet, and the majority of these people are rural consumers in developing countries. This leaves them excluded from social and economic opportunities, and negatively impacts the economic development of the countries in which they live.

For example, management consulting firm McKinsey estimates that the internet could account for as much as ten per cent of Africa's annual gross domestic product by 2025 (up from around one per cent today), due to the internet's transformational effects on retail, agriculture, education and healthcare.

In the developing world, mobile is the cheapest and most convenient way of accessing the internet, and is often the first internet touch point for rural consumers. According to GSMA Intelligence, mobile penetration in the developing world has increased steadily from approximately 25 per cent to 44 per cent over the past five years.

However, despite this rapid increase, a number of barriers still stand in the way of these populations fully benefiting from the mobile internet. These include infrastructure challenges, affordability, and consumer impediments such as digital literacy and the lack of locally relevant content.

Programme Goals

The GSMA's Connected Society programme supports the mobile industry in its efforts to bring mobile internet access to underserved populations in developing countries.

Working towards this aim, the programme delivers evidence-based research, case studies and advisory services to help mobile operators, policymakers and other stakeholders break down barriers related to infrastructure, affordability, digital literacy and local content.

The programme also works closely with the GSMA Connected Women initiative to close the gender gap in mobile phone ownership. Furthermore, it collaborates with the GSMA Disaster Response programme in its goal of helping humanitarian organisations, governments, non-governmental organisations (NGOs) and the broader mobile ecosystem develop coordinated and highly effective disaster response mechanisms for the mobile industry.

Public Policy Considerations

The growth of the mobile sector has enabled broader access to Information and Communications Technology (ICT). However, barriers to accessing the mobile internet and services remain, especially in developing countries. There are a number of areas that governments and other key stakeholders can focus on to help bridge this digital divide.

Affordability. Mobile-specific taxes raise barriers to mobile phone ownership and usage. This is especially true in developing markets where affordability is critical to increasing digital inclusion and access to the mobile internet. By adopting phased reductions in mobile-specific taxes, governments can benefit from the additional economic growth driven by the mobile internet, while limiting short-term losses in tax revenue.

Digital literacy. The majority of people in developing markets are accessing the internet for the first time through a mobile phone. However, many of these people are illiterate and have limited digital skills. To address this barrier the GSMA has created the Mobile Internet Skills Training Toolkit (MISTT), a resource to help people acquire the skills needed to access the mobile internet and enjoy the benefits and opportunities of being online.

Governments can also play a role in supporting the needs of these citizens by ensuring robust education systems at primary and secondary school level and introducing mobile technology to people at a young age as part of the standard learning curriculum.

Infrastructure. Around 1.6 billion of the 4.2 billion people who are still offline live outside the coverage area of 3G mobile networks. Closing this mobile coverage gap is primarily an economic rather than technical challenge. These offline populations typically live in sparsely populated, rural areas that suffer from low income levels and weak or non-existent 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. However, the public sector, and national governments in particular, can help by aligning key policies around best practice approaches to spectrum allocation and pricing, infrastructure sharing, sector-specific taxation, access to public infrastructure, licence conditions and market structure.

Locally relevant content. In many developing nations there is a lack of content to make the mobile internet relevant to local audiences. Governments have a crucial role to play in addressing this. For example, they can invest and support key enabling infrastructure such as affordable international bandwidth and local content-hosting platforms, and foster a progressive policy environment that supports digital entrepreneurs and innovation. Furthermore, by ensuring that government services are accessible online or via mobile, they can not only improve the efficiency of delivery of these services, but also create incentives for citizens to use the internet.

Resources:
GSMA Report: Digital Inclusion and Mobile Sector Taxation in Mexico
GSMA Report: Mobile Internet Usage Challenges in Asia — Awareness, Literacy and Local Content
GSMA Report: Rural Coverage — Strategies for Sustainability
GSMA Report: Benefits of Network Competition and Complementary Policies to Promote Mobile Broadband Coverage
GSMA Report: Digital Inclusion 2014
GSMA Report: Unlocking Rural Coverage — Enablers for commercially sustainable mobile network expansion
GSMA Mobile Internet Skills Training Toolkit website

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. However, the World Bank estimates that at least one billion people in developing countries lack any form of officially recognised ID, either paper or electronic based. This problem disproportionally impacts rural residents, poor people, women, children, and other vulnerable groups in Africa and Asia.

This '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 child in three doesn't have 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 international community has recognised the 'identity gap' as a critical barrier to achieving inclusive and sustainable social and economic development. This is reflected formally through the UN Convention on the Rights of the Child and the Sustainable Development Goals, which highlight the lack of birth registration as a barrier to the provision of an official or legal proof of identity. Countries where a large percentage of the population lack official ID have an opportunity to bypass outdated and cumbersome approaches to ID provision and instead create new identity ecosystems based on innovative, digital technology. Countries that have already adopted digital identity systems show clearly how these systems bring not just efficiency gains and financial savings, but also increase social inclusion by making it easier for citizens to access basic services and rights.

As more services and transactions take place in the digital sphere, digital identity will become increasingly fundamental to participation and inclusion. 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.

Public Policy Considerations

When births go unregistered at the national level or people lack official documentation, there is the potential for millions of citizens to be denied access to government, banking and other vitally important services. With children being born into an increasingly connected world and mobile use growing rapidly in developing nations, it makes sense for governments to support innovative and scalable solutions that can provide trustworthy digital identity and authentication for their citizens. Mobile identity platforms can help governments achieve this aim and accelerate the move towards digital public services in both developed and developing countries.

However, an enabling regulatory environment needs to be put in place if mobile is to deliver formal identity and authentication to over a billion people who are currently unregistered, and ultimately drive improved social, political and economic inclusion. To help create the right environment, governments need to ensure there is consistency between the different legal and regulatory instruments that affect the management of digital identity, and work to break down any legal, policy and regulatory barriers that may inhibit the roll out of mobile identity services.

Governments also carry a responsibility to foster and help create the trusted environment within which mobile identity operates. The creation of a digital identity plan that acknowledges the central role of mobile in the digital landscape can help this situation, but governments should also engage with mobile operators, key stakeholders and the wider identity ecosystem to help drive interoperability and innovation.

Emerging principles for a robust digital identity ecosystem, include:

- Universal coverage and availability (including accessibility for all).
- Appropriate and effective design that takes into account interoperability and sustainability.
- The need to build and sustain trust by assuring privacy and personal data protection and offering consumers oversight and control of their data.

Resources:
GSMA Digital Identity Programme website
GSMA Report: Digital Identity — Towards Shared Principles for Public and Private Sector Cooperation
GSMA Mandatory Registration of Prepaid SIM cards website
GSMA Personal Data website
GSMA Mobile Connect website
GSMA Case Study: Mobile Birth Registration in sub-Saharan Africa
GSMA Case Study: Birth Registration in Tanzania
GSMA White Paper: Mobile Identity — Unlocking the Potential of the Digital Economy

Disaster Response

Background

Mobile networks, and the connectivity they provide, are increasingly identified as a lifeline in disasters due to their ability to support critical communication between humanitarian agencies, affected populations and the international community.

The power of mobile was evident in the aftermath of the 2010 Haitian earthquake, which saw a proliferation of new coordination and response strategies that were built around mobile platforms.

Since then, experiences in the Philippines with Typhoon Haiyan, the Ebola crisis in West Africa and the earthquakes in Nepal and Italy, have continued to provide examples of the critical importance of access to communication and information for populations affected by disaster and crisis.

As 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 in the wake of disaster.

Programme Goals

The GSMA Disaster Response programme works with mobile operators to determine how they can improve preparedness and network resilience before disaster strikes, and help affected citizens and humanitarian organisations following a crisis.

Through research and engagement with mobile and humanitarian stakeholders, the GSMA is working to define and share best practices and create a robust, coordinated disaster response mechanism for the mobile industry.

This work has culminated in the Humanitarian Connectivity Charter, launched in early 2015. The Charter represents a set of shared principles and activities focused on strengthening access to communication and information for those affected by crisis in order to reduce the loss of life and positively contribute to humanitarian response.

Mobile operators who have signed the Charter currently represent subscribers in over 75 countries.

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:

- Governments — along with relevant multilateral agencies — and operators should agree a set of regulatory guidelines that can be adopted to best respond to and recover from an emergency.
- The guidelines should set out unambiguous rules and clearly defined lines of communication between all levels of government and operators in emergency situations.
- The guidelines should provide operators with flexibility to adjust to unforeseen circumstances rather than insisting that rules designed for non-emergency situations apply no matter what the circumstance.
- The guidelines should help improve communication and coordination among various government entities involved in responding to an emergency and facilitate a timely and efficient response.

Resources:
GSMA Disaster Response website
GSMA Humanitarian Connectivity Charter website
GSMA Report: Business Continuity Management — Planning for disaster resilience in mobile networks
GSMA Report: Partnership Guidelines — Building effective partnerships between MNOs and NGOs in complex environments and crises
GSMA Report: Nepal Earthquake Response and Recovery Overview
GSMA Case Study: DEWN — Dialog's Disaster and Emergency Warning Network
GSMA Report: Disaster Response — Mobile Money for the Displaced
GSMA Case Study: Business As Usual — How AT&T deals with Natural Disasters
GSMA Guidelines: The Protection of Privacy in the Use of Mobile Phone Data for Responding to the Ebola Outbreak

Ecosystem Accelerator

Background

The ubiquity and accessibility of mobile technology has helped it cut across geographies, cultures and income levels to drive innovation. In many developing markets, mobile is the only reliable infrastructure and when used in innovative ways it truly has the power to transform lives.

Unsurprisingly, there are an increasing number of innovative start-ups springing up in developing markets. However, according to Disrupt Africa, tech start-ups in Africa only managed to raise $185 million of funding in 2015, most of it (70 per cent) in South Africa, Nigeria, and Kenya.

Many of these fledging companies are focused on mobile products and services and tend to have bold ideas, agile working practices and a strong understanding of their customer base. Yet they often struggle to attract the resources needed to achieve scale and commercial sustainability.

On the other hand, mobile operators have significant assets — million-strong customer bases, large distribution networks, and a high degree of marketing and technical expertise — but because of their size they often aren't as quick to bring innovative ideas to market and sometimes struggle to open up new sources of revenue.

If both parties can be brought together there is potential to unlock many mutual benefits: start-ups could be a great source of local innovation and potential new revenue sources for operators, while operators can provide the added credibility, support, and expertise that start-ups often lack. End users will in turn benefit from the positive socio-economic impact generated by this ecosystem.

Programme Goals

The GSMA Ecosystem Accelerator programme works to bridge the gap between mobile operators and start-ups.

By opening the dialogue between innovators and operators, the programme helps operators to contribute their assets and expertise to the most promising ideas. In turn, this will help start-ups to secure the funding and direction they require in order to achieve scale with their products and services. In fostering these partnerships, the Ecosystem Accelerator programme aims to bring the most impactful mobile solutions to the people and places that need them the most, generating the greatest socio-economic impact at the local level.

Ultimately, it's the way human beings, with our vast stores of ingenuity, deploy the power of the technology and tools that makes the biggest difference.

— Bill Gates, Co-chair, Bill and Melinda Gates Foundation

The GSMA has also introduced the Ecosystem Accelerator Innovation Fund. This fund will support innovative start-ups in emerging markets, and is open to start-ups from Africa and Asia who operate within these regions. The Fund — and the programme overall — is backed by the UK Department for International Development (DFID) and supported by the GSMA and its members.

The Fund will run several rounds between 2016 and 2020, with each round having specific areas of focus. For example, the first funding round — in late 2016 — disbursed approximately £2 million and was open to start-ups focused on the 'sharing economy' and those that develop services for small and medium enterprises.

Public Policy Considerations

The innovative ideas and agile working practices that start-ups bring to business mean they often have a huge impact on both economies and societies. This can already be seen in the transformative effect that the new 'sharing economy' is having on consumption patterns and communities around the world.

As a result, there is now an onus on governments to put in place policies that help start-ups to act and move quickly. For example, governments can help by breaking down bureaucratic barriers, improving access to capital, and fostering a culture of innovation where risk-taking is not punished.

Governments can also have an impact by becoming more involved in supporting tech hubs, given their potential to create 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 stakeholders in the start-up ecosystem also need to collaborate to ensure that new mobile-based solutions achieve scale and sustainability. For example, mobile operators can help by opening up Application Programming Interfaces (APIs) to third-party developers and start-ups to encourage even more innovation in the mobile ecosystem.

Resources:
GSMA Video: Ecosystem Accelerator Programme
GSMA Ecosystem Accelerator Innovation Fund website
GSMA Report: APIs — A bridge between mobile operators and start-ups in emerging markets
GSMA News: Ecosystem Accelerator blog — A few things we learned about tech hubs in Africa and Asia

Mobile For Development Utilities

Background

The rapid expansion of GSM networks means mobile now has further reach than the electricity grid, piped water networks and sewerage networks in most emerging markets. While mobile network coverage has grown at an astonishing rate of 11 per cent per year since 2000, energy and water access lags behind with yearly growth figures of between one and two per cent. Much also needs to be done to bridge the current sanitation gap, as 2.4 billion people still lack access to improved sanitation solutions. The result is a widening gap between access to mobile and access to basic utility services. In fact, by 2014 mobile networks covered more than 772 million people without access to electricity, more than 289 million people without access to clean water and 1.8 billion without access to improved sanitation.

This lack of access to affordable and sustainable utility infrastructure has a profound impact on people's lives. For example, according to figures from charity WaterAid, poor sanitation takes the lives of over 1,400 children per day. And poorer people living off the electricity grid in emerging markets often end up relying on expensive and harmful energy sources, such as kerosene, that 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.[1]

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 access 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 the opportunity for the mobile industry to leverage its network technology and infrastructure to help solve these challenges in emerging markets.

The programme was established in 2013 thanks to funding from the UK Government Department of International Development. The programme has also launched the M4D Utilities Innovation Grant Fund, which aims to accelerate the development of promising mobile technologies and business models that target improved access to energy, water and sanitation services. The fund has so far provided 34 grants across 24 countries to innovators in the utility sector.

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 and water access

through the use of innovative mobile technologies.

- Driving further industry interest and support for increasing access to energy and water 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. Through the use of M2M technologies, water pumps can be monitored remotely and repair call-outs triggered automatically when a fault occurs, reducing down time. Governments should ensure that taxation levels on M2M connections are set at appropriate levels 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 here by ensuring consumers don't face higher taxes on mobile handsets and services than on other goods and services.

[1] GSMA, Sustainable Energy and Water Access through M2M Connectivity (2011)

Resources:
GSMA Mobile For Development Utilities website
GSMA Mobile For Development Utilities Annual Report 2016 website
GSMA Mobile for Development Utilities Innovation Fund website
GSMA Connected Society Programme website

Mobile Health

Background

Over 400 million people in the world lack access to affordable basic healthcare. Mobile is the most viable solution for delivering healthcare in countries where there is a large, unmet demand. This is because mHealth services can make a real difference when there are few alternatives available to end users.

Despite the many mHealth services that exist today, few currently demonstrate scale, replication or significant impact. A study by the GSMA which reviewed almost 700 mHealth services showed that less than one per cent of these significantly impact health outcomes. Four key barriers were identified: fragmentation of service delivery, lack of scale across the full reach of mobile networks, limited replication and a misalignment of the value proposition between mobile and health stakeholders.

The GSMA mHealth programme aims to address these barriers and in doing so foster commercially sustainable mHealth services that truly meet public health needs.

Programme Goals

The GSMA mHealth programme is currently funded by UK Aid and aims to boost maternal and child health via mobile solutions that promote improved maternal health and nutrition practices. It has a target of reaching one million mothers by August 2018 across eight markets: Ghana, Malawi, Mozambique, Nigeria, Rwanda, Tanzania, Uganda and Zambia. By the end of 2016 the programme had already reached over 750,000 end users across sub-Saharan markets.

The programme's emphasis is on identifying high-potential mHealth services and helping them to achieve scale and adoption. There are three key areas of focus:

- **Product development.** The GSMA supports product owners with user-centric research in their markets in order to inform the product design, pricing model and full value proposition of the mHealth services. By combining qualitative and data-driven insights, the GSMA works with the service partners to support product improvement and product roadmap decisions.

- **Content development.** By engaging with key global and local players in the field of nutrition, the programme fosters the development of publicly available, digital market-specific and culturally-sensitive mHealth content for eight sub-Saharan markets.

- **Industry engagement.** The 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.

Public Policy Considerations

Use cases for mHealth solutions are varied, from mobile services designed for basic phones to sophisticated medical devices with embedded SIMs that collect and transmit patient data back to healthcare providers. As such, there are a wide range of potential regulatory touch points. Clear policy and regulation for mHealth are essential to ensure safety, promote confidence among end users and healthcare professionals, and provide industry with the certainty needed for it to invest in innovation and bring new products and services to market.

Regulatory themes that are of specific interest in emerging markets include:

- **Consent and data protection.** Building trust through suitable approaches to securing consent for data collection and then subsequent protection of that data once it has been collected is important globally, but is often particularly sensitive in developing markets. Frequently, there is a fear of social stigma if information on an individual's diagnosis is inappropriately shared.
- **Systems and interfaces.** In developed countries there has been a proliferation of different standards and systems around mHealth, which often make integration difficult. In contrast, the situation in emerging markets means there is a unique opportunity to define standards that promote interoperability and enable scalability.

Policy themes are more globally applicable, and include:

- **Patient empowerment.** Developing policies that appropriately promote user autonomy and drive mHealth adoption.
- **Reimbursement.** Moving towards reimbursement schedules that reward health outcomes and support innovation.
- **Implementation.** Establishing government programmes that address market barriers, build evidence for the benefits of mHealth and encourage the implementation of mHealth systems and services.

Resources:
GSMA Report: mHealth Regulation Impact Assessment — Africa
GSMA Report: The Use of Mobile to Drive Improved Nutrition Outcomes — Successes and Best Practices from the mHealth Industry
GSMA Report: Mobile for Development mHealth — SIM-based Medical Applications

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. One of the keys to this success has been operators' ability to use their large airtime distribution networks to provide customers with easily accessible mobile money agents who perform cash-in and cash-out transactions. This has helped registered customer accounts grow by 31 per cent to reach a total of 411 million registered accounts globally in 2015.

In their 2015 annual letter, Bill and Melinda Gates cited mobile money as one of four top solutions to end severe poverty by 2030. Certainly market figures 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 2015, there were 271 services in 93 countries helping to transform the financial lives of more than 134 million active users.

Programme Goals

Two billion people remain unbanked, without access to safe, secure and affordable financial services. The GSMA Mobile Money programme helps mobile operators and industry stakeholders to increase financial inclusion for these people by enhancing the utility and sustainability of mobile money services.

The programme is working to develop a robust, highly-interconnected mobile money ecosystem where transactions for numerous sectors (such as retail, utilities, health, education, agriculture and transport) are digitised. Diversifying customer usage patterns to include not just merchant payments, but also transactions such as cross-border mobile money 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 huge range of digital transactions. By making mobile money more central to the financial lives of users, greater financial inclusion, economic empowerment and economic growth can be achieved.

Public Policy Considerations

Regulation has a major impact on the uptake of mobile money services. Evidence shows that enabling regulatory frameworks accelerate the development and adoption of digital financial services. In contrast, mobile money deployments in countries with non-enabling regulation show a smaller number of mobile money accounts and less agent activity.

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 by significantly expanding 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.

Furthermore, mobile money can 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, by bringing more people from the informal to the formal economy, governments can expand their tax base and increase their revenue generation potential.

Governmental bodies can also benefit in a number of 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 and 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.
- Not mandate a technical or commercial model for 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: 2015 State of the Industry — Mobile Money
GSMA News: What is the availability of mobile money services in 2015?

Women and Mobile

Background

While mobile connectivity has grown rapidly, it hasn't touched populations in an equal way. In today's increasingly connected world, many women are being left behind. According to a 2015 study[1] commissioned by the GSMA, there are 200 million fewer women than men who own a mobile phone in low- and middle-income countries. 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 often disproportionately affected by barriers to both access and use of mobile products and services. These barriers include the cost of handsets and services, network coverage, concerns around security and harassment, as well as a lack of technical literacy. Social norms are also an issue and can delay — or even prevent — a woman from acquiring a mobile phone and related services.

Closing the gender gap in mobile phone ownership and usage has the potential to unlock substantial benefits for women, as well as the mobile industry and broader economy. Mobile can help empower women, by making them safer and more connected, while also opening up access to information and life-enhancing opportunities, such as health information, financial services and employment opportunities.

The gender gap is not going to close on its own. Its root causes are driven by a complex set of social, economic and cultural barriers. These obstacles can only be overcome with targeted intervention by all stakeholders, including policymakers, in close collaboration with the entire mobile industry. Working together, leaders can make significant strides to redress this gender imbalance, supporting the United Nations Sustainable Development Goals (SDGs) and in particular SDG number five, which aims to achieve gender equality and empower all women and girls.

Programme Goals

The GSMA Connected Women programme is focused on accelerating digital and financial inclusion for women. Its mission is to reduce the gender gap in the use of mobile internet and mobile money services in low- and middle-income countries and unlock significant commercial and socio-economic opportunities.

The programme 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. When women thrive, societies, businesses and economies thrive.

Public Policy Considerations

Policymakers and regulators can adopt many strategies to ensure women are not excluded from the benefits of mobile. 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 curricula or the introduction of training programmes. It may also be appropriate to address harassment over mobile phones and mobile internet through awareness campaigns or legal and policy frameworks.

Data on women's mobile phone access and usage, and on ICT more broadly, is also not widely available or tracked in many low- and middle-income countries. Without data, policymakers and the mobile industry cannot make informed decisions to help increase women's access to, and use of, mobile phones. To address this, policymakers can consider options to track mobile access and use by gender, along with other ICTs, in national statistics databases.

Women are also under-represented in the technology sector as employees and leaders. This is important as the technology sector is a high-growth field which is important to countries' innovation, connectedness and competitiveness in global markets. Women today compose 40 per cent of the global workforce and account for more than half of university graduates, yet we see only three to five per cent of senior positions in technology being held by women.[2]

Developing and supporting policies or schemes to address this under-representation is important as it has a measurable economic cost. For example, according to a 2013 European Commission survey on women in ICT, organisations in Europe that have women in senior management positions generate a 35 per cent higher return on equity, while female employment overall provides an annual economic boost of €9 billion.

[1] GSMA Connected Women. Bridging the gender gap: Mobile access and usage in low- and middle-income countries (2015)

[2] MacLeod Consulting, Implications of the ICT Skills Gap for the Mobile Industry (2013)

Resources:
GSMA Connected Women website
GSMA Report: Bridging the gender gap — Mobile access and use in low- and middle-income countries
GSMA Report: Accelerating digital literacy — Empowering women to use the mobile internet
GSMA Report: Accelerating the digital economy — Gender diversity in the telecommunications sector

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 4.7 billion unique mobile subscribers globally, equivalent to 63 per cent of the world's population. By 2020, almost three-quarters of the global population will have a mobile subscription, with around one billion new 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 move to an all-IP network environment, 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 strategic importance of Internet Protocol (IP) to future mobile networks is clear and embracing this future is vital for mobile operators as they compete to win and retain customers. Moving to all-IP based infrastructure and services enables operators to deliver a broader, deeper communications portfolio — incorporating voice, data, video and messaging services.

With the increasingly widespread deployment of Long Term Evolution (LTE) networks, the move to global interconnected IP-communication services such as Voice over LTE (VoLTE), Video over LTE (ViLTE) and Rich Communication Services (RCS) is accelerating at a rapid pace.

Through its Network 2020 programme, the GSMA is working with leading operators and equipment vendors to further accelerate the launch of IP-based services around the world.

The mobile industry is also 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.

5G — The Path to the Next Generation

Background

Mobile telecoms 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.

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. This will include areas such as the definition of interconnect in 5G, as well as the identification and alignment of suitable spectrum bands. Once a stable definition of 5G is reached, the GSMA will work with its members to identify and develop commercially viable 5G applications.

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 in order to deliver enhanced capabilities, including new usage scenarios. To ensure 5G services provide good coverage that extends beyond small urban hotspots, it will be important to make sure that there is sufficient spectrum available for this important purpose (i.e., sub-1 GHz spectrum). Progressive refarming of existing mobile bands should be both possible and permitted to accommodate future 5G usage, as well as to maximise spectrum usage efficiency.

The GSMA believes that three key frequency ranges are currently worthy of consideration for different 5G deployment scenarios: sub-1 GHz, 1-6 GHz and above 6 GHz. 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 Report: Understanding 5G — Perspectives on future technological advancements in mobile
GSMA Public Policy Position: 5G Spectrum

IP Communication Services

Background

IP communications 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 over 500 of the world's mobile network operators having now launched Long Term Evolution (LTE) networks, and LTE coverage currently exceeding half of the world 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 September 2016, there were 82 VoLTE services commercially available in 46 countries.
- **ViLTE.** This will enable operators to deploy a commercially viable, carrier-grade, person-to-person video calling service. Like VoLTE, it is based on IMS technology.
- **VoWiFi.** This allows operators to offer secure voice calling over WiFi. As of September 2016, there were 35 VoWiFi services commercially available in 21 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 September 2016, RCS was being offered by 48 mobile operators in 35 countries.

The GSMA, via its Network 2020 programme, is working with leading operators and equipment vendors to accelerate the launch of IP-based services around the world. The work of the Network 2020 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 open industry standards for IP-based calling, messaging, file and video-sharing services, generically based on IMS technology.

Interconnect. VoLTE, ViLTE, VoWiFi and RCS support interconnection of these services between customers on two different mobile 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 standard called Long Term Evolution (LTE). LTE networks incorporate 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 it will take a number of years to phase out 2G and 3G networks and fully migrate customers to LTE-based networks and 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, 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 capacity (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 capabilities 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 Network 2020 — 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 cellular machine-to-machine (M2M) connections is expected to have reached just under one billion by 2020. However, this will still represent a small portion of the overall market, as Juniper Research predicts that the total number of IoT devices will have grown to 38.5 billion by 2020.

The GSMA, through its Connected Living 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.

Encouraging the Growth of IoT

Background

The Internet of Things (IoT) promises to deliver a huge range of benefits to citizens, consumers, businesses and governments. Referring to machines, devices and appliances of all kinds that are connected to the internet through multiple networks, the IoT has tremendous potential to shrink healthcare costs, reduce carbon emissions, increase access to education, improve transportation safety and much more.

Through its Connected Living programme, the GSMA aims to accelerate the delivery of these types of connected devices and services, and thereby enable a world in which consumers and businesses enjoy rich new services, connected by an intelligent and secure mobile network.

The IoT market is already developing at a rapid pace. According to figures from Machina Research, by the end of 2016 the number of cellular IoT connections will have reached nearly 486 million, with that figure set to soar to just under 1.2 billion by 2020. Understandably, governments and regulators are increasingly interested in how they can capture the benefits of the IoT and channel them to their citizens.

However, IoT business models, markets and services are fundamentally different from traditional telecoms services, such as voice and messaging. In most cases, IoT services have a closed user group and the customers are not typically end users of the service, but businesses that need to be able to roll out IoT solutions globally. Also, IoT services are characterised by a significantly lower average revenue per connection than traditional voice and messaging services.

Therefore, if governments are to create a supportive environment for the IoT, they must recognise these differences when considering policy and regulatory frameworks. This means policy and regulation should be flexible, balanced and technology-neutral to ensure they support large-scale deployments and encourage investment.

In 2016 the GSMA introduced the IoT Knowledgebase, an online tool for policymakers and regulators that is designed to help them unlock IoT opportunities for their country, understand new IoT business models and learn about emerging policy and regulatory best practice from around the world.

Public Policy Considerations

There is huge potential for the IoT to transform economies and societies, but the technologies and ecosystem that support IoT are still at an early stage of development. If governments are to realise the significant socio-economic benefits that IoT can deliver, they must foster an investment-friendly and technology-neutral environment that will allow it to grow and flourish.

Governments can achieve this by putting in place policies that provide the right incentives for growth and innovation. They can also lead by example through the adoption of IoT solutions in the public sector or by funding research and development programmes.

As the IoT ecosystem is composed of a large number of diverse players, policy frameworks must be based on the fair regulation of equivalent services. Regulatory clarity is also hugely important to give service providers and IoT device manufacturers the confidence to make the necessary investments in this emerging technology for it to achieve global scale.

Governments and regulators can play a significant role here too, by supporting and promoting interoperable specifications and standards across the IoT industry. This is important to the future growth of the IoT, as interoperable platforms and services reduce deployment costs and complexity, facilitate scalability and enable consumers to enjoy intuitive connected experiences.

As the IoT is projected to grow hugely in the coming years, governments also need to adopt a flexible framework for both licensed and unlicensed spectrum, to ensure mobile operators can deploy the most appropriate technology mix.

The IoT presents significant opportunities for data-driven innovation to achieve economic, social and public policy objectives and improve people's daily lives. However, for this to happen, data protection and privacy legal frameworks need to be practical, proportionate and applied consistently to all parties in the IoT value chain. This will help create a climate of trust between industry and end users.

Resources:
GSMA IoT Knowledgebase for Policy and Regulation website
GSMA Report: Mobilising the Internet of Things

Global Deployment Models for IoT

Background

The Internet of Things (IoT) is ushering in an era where unprecedented numbers of devices will become connected all around the globe. The scale and reach of this machine-to-machine (M2M) connectivity will allow new services to develop that can help societies make more efficient use of resources across a range of industries and sectors, including healthcare, agriculture, transportation and manufacturing.

However, if governments and societies are to tap into these benefits, companies operating within the IoT ecosystem will need to be able to deploy their services on a global, rather than local, scale. It is only by following global deployment models that the nascent IoT industry can pass on to consumers the benefits they get from economies of scale for service delivery.

Global approaches to service deployment have a number of advantages. For example, they accelerate the speed and quality of deployment and also drive down the cost of servicing smaller, local markets where the creation of a bespoke local service would otherwise be uneconomical. Furthermore, they help guarantee the delivery of a consistent, high-quality experience to the end user.

Mobile operators are already taking the lead in supporting global service launches in early market categories such as automotive, health and consumer electronics. With the emergence of new products in adjacent categories, including healthcare and wearable devices, the importance of being able to support large-scale, global deployments is likely to increase.

Operators can choose from a range of different global deployment models, including M2M international roaming, the embedded SIM technology developed by the GSMA's Connected Living programme, or a hybrid of the two. New deployment models may also emerge in the future.

The choice of deployment model may depend on a number of factors, such as:

- The particular needs of the mobile operator, IoT service provider and end user.
- The scale and geographical footprint of the deployment.
- The type of IoT application and its unique service requirements.
- The device lifetime and its accessibility.

Public Policy Considerations

The IoT has the potential to bring substantial social and economic benefits to citizens and businesses through more efficient use of resources, the creation of new jobs and services, increases in productivity and improvements in service delivery.

However, IoT business and distribution models are very different to those used to deliver traditional telecoms services, such as voice and messaging. Typically, they are global in nature, with elements of the value chain spread across various countries and regions.

The great diversity in the range of services on offer and the partners involved in IoT, as well as this geographical spread in the value chain, make it hugely important for the industry to be able to develop and select the most suitable deployment models for different types of IoT services.

This is why policymakers and regulators should avoid regulation that tries to steer the industry towards a one-size-fits-all approach to deployment. Instead, governments should encourage innovation in IoT deployment models and understand that operators will be required to adopt flexible commercial and technical solutions in different countries and regions around the world.

Governments can support the global nature of the IoT market in other ways, such as by backing interoperable platforms and services to reduce deployment costs and complexity, ensuring that all players in the IoT market are operating on a level regulatory playing field, and working together across jurisdictions to ensure consistency and clarity on legal, data protection and privacy regulation.

Resources:
GSMA Report: Understanding the Internet of Things
PWC Report: Realising the benefits of mobile-enabled IoT solutions

Connected Vehicles

Background

The integration of mobile communications into vehicles is changing people's relationship with the car. Increasingly, drivers and passengers are able to obtain real-time information about their trip (such as weather conditions or traffic flow data) and enjoy car-appropriate infotainment (such as internet radio and video services for passengers). Large-scale deployments of connected car solutions already exist in many parts of the world, and the variety of services is growing significantly.

Mobile network operators, which have traditionally provided connectivity for vehicle services, are beginning to move up the value chain, offering extended connectivity support (e.g., applications management), expanded core assets (e.g., customer service management, billing systems and fraud management) and sector-specific services (e.g., telematics service provision, disaster recovery and datacentre hosting).

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

The primary platform for these activities is the Connected Vehicle Forum. This group was established by the GSMA with the aim of promoting dialogue across all stakeholders in the automotive and ITS ecosystem and looks to find innovative ways that mobile technology can be leveraged by these sectors.

Currently a key area of focus is 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.

The Embedded SIM Specification has global backing (from operators, SIM suppliers and a wide variety of equipment and vehicle manufacturers) and offers a number of key advantages that make it particularly suitable for connected vehicle applications:

- It is live and commercially available now from leading global mobile operators.
- It offers the same level of security achieved today by traditional SIMs.
- It reduces risks of tampering, as the SIM is soldered into the vehicle.
- It simplifies production and reduces the need for a mechanical SIM holder and slot.

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.

Governments can help encourage the development of the connected vehicle and intelligent transport ecosystems by:

- Introducing incentives for growth and innovation.
- Promoting research and development programmes for connected and autonomous vehicles.
- Supporting services, applications and industry-led standards and interoperability.
- Promoting trust and confidence in automotive and intelligent transport solutions among end users.

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 and emergency regulations.

It is important that policymakers and regulators appreciate and understand these differences, implement policies that allow global business models to develop and ensure that policies apply consistently to all players in the value chain.

Currently, security and emergency regulations have been introduced in three locations: Europe, Russia and Brazil.

- In Europe, the regulations relate to eCall, an in-vehicle emergency call system that automatically triggers an emergency call in the event of a severe road accident. The proposed legislation requires all new vehicles sold in the EU to be eCall-ready by March 2018.
- The GSMA is involved in two EU-led task forces for eCall: Lifecycle Management of the SIM and the Periodic Inspections Tests. The former relates to the provisioning of the in-car SIM (from its activation through to defining the events that trigger the SIM 'end-of-life') and the latter concerns the testing processes that will be put in place to ensure that all cars sold in the EU by March 2018 have a fully functioning eCall system.
- In Russia, ERA GLONASS has similar goals to eCall and extends to insurance reconstruction and dangerous goods transport services, while Brazil's SIMRAV project focuses on reducing vehicle theft and lowering vehicle insurance rates through the mandatory use of stolen vehicle location services.

Resources:
GSMA Report: Mobilizing Intelligent Transportation Systems
GSMA Report: Automotive IoT Security — Countering the most common forms of attack
GSMA Transforming the Connected Car Market website
GSMA Case Study: EE Brings Safer Driving to the UK's Roads
GSMA White Paper: Split Charging and Revenue Management Capabilities for Connected Car Services
GSMA White Paper: Connecting Cars — BYoD, Tethering Challenges

Mobile Health and IoT

Background

The pressures on healthcare systems have never been greater, due to factors including rising expectations, ageing populations and, particularly in emerging economies, the combined challenges of infectious disease and increasing incidence of chronic illness. Mobile health solutions provide an opportunity to help healthcare providers deliver better, more consistent and more efficient healthcare, increasing access to health services and empowering individuals to manage their own health more effectively.

According to a 2015 report by PWC, mHealth could save over one million lives in sub-Saharan Africa over the next five years and the use of Internet of Things (IoT) technology in healthcare could reduce healthcare costs by €99 billion in the European Union and add €93 billion to the region's gross domestic product by 2017.

Many mobile health propositions have gained acceptance and are being more widely adopted. The market is developing, and this growth is accompanied by a rapid increase in the number of solutions that potentially offer new modalities of care. Greater consideration is therefore being given to the policy and regulatory frameworks that will govern their promotion and use.

Public Policy Considerations

Use cases for mHealth solutions are varied, from medical devices that collect patient data to applications that deliver health services and information – providing support in the area of prevention (including lifestyle and wellness), diagnosis and management. As such, there are a wide range of potential regulatory touch points.

Although significant progress has been made over the last few years, there is an ongoing need for clarity in policy and regulation related to mHealth to ensure safety, promote confidence among patients and healthcare professionals, and provide industry with sufficient certainty to bring new products and services to the market.

Policy themes include:

Patient-centered healthcare. Developing policies that promote patient-centred care and user autonomy to help drive mHealth adoption.

Access. Promoting initiatives to integrate mHealth services into healthcare systems and care pathways to encourage the development of value-based care models that reward health outcomes and support innovation.

Implementation. Building evidence and establishing government programmes to enable large-scale implementations of mHealth solutions.

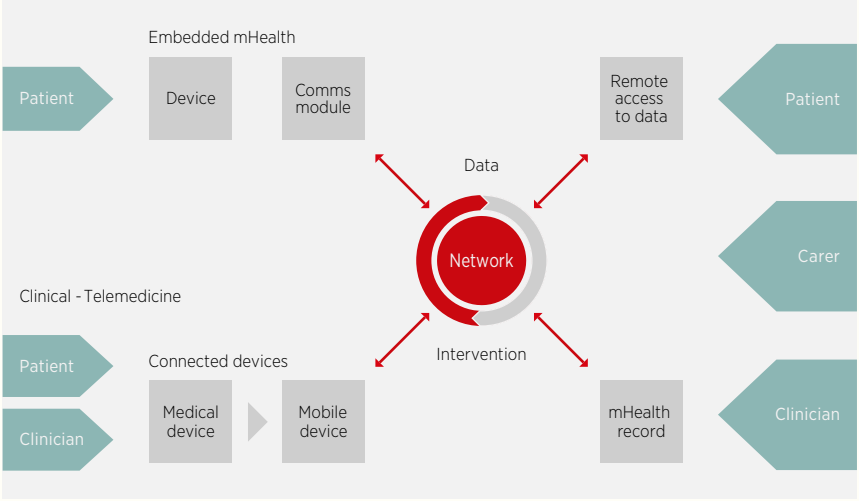
Systems, interfaces and interoperability. Promoting interoperability and standards that support scalability and a plug-and-play experience.

Regulatory themes include:

Medical devices. Developing and implementing clear and proportionate regulatory frameworks that aim to ensure patient safety while stimulating innovation.

Data protection. Ensuring an appropriate regulatory framework is in place for data protection and privacy is of key importance. Regulatory measures should be proportionate and facilitate the use of data in creating patient-centred and sustainable healthcare systems.

Consumer use – Telehealth



Source: PA Consulting Group

Resources:
GSMA Response: The European Commission Green Paper on mHealth
GSMA Joint Statement: The Healthcare Coalition on Data Protection
GSMA and Continua Alliance Report: mHealth Policy and Medical Device Regulation
PWC Report: Realising the benefits of mobile-enabled IoT solutions
GSMA White Paper: Global views on Potential of Mobile Health Solutions to Address Chronic Disease Challenges
GSMA & PA Consulting Group: Policy and Regulation for Innovation in Mobile Health
PWC Report: Socio-economic Impact of mHealth, European Union
PWC Report: Socio-economic Impact of mHealth, Brazil and Mexico

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 (for example, 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: 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. This trend is set to continue, as the World Health Organization forecasts that the global urban population will grow approximately 1.84 per cent per year between 2015 and 2020, 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 re-design 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 be used 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:

- Cultivate local or central government commitment. To build a successful strategy, the city or government must consult with a wide variety of stakeholders, including citizens, technology partners and urban planners. Above all, the city's high-level leadership must be fully committed to delivering smart city services to ensure the benefits continue to be realised far into the future.

- Each local government is accountable to its citizens for the success of smart city services. Every city is different and will have distinct requirements based on its location, culture and funding models. Mobile operators understand this and can help cities develop clear objectives that can be tracked against agreed KPIs in order to deliver these types of projects.

- Define a vision for the future. A city leader with vision, commitment and a budget can be a powerful force to create new services for local citizens and businesses. A mobile operator working as a partner can help this leader build a realistic set of technical objectives, programmes and KPIs around this vision, to establish an achievable roadmap of future services.

- Create investment opportunities. To maximise the potential of smart cities, it is important to create an investment environment that encourages the introduction of new concepts and applications that can be monetised. The city itself may provide funding to potential partners, or it might create a positive working environment that helps attract the right talent.

- Once smart cities are up and running, their environmental, resource and operational efficiencies help bring in investment from new businesses. Innovative funding models involving the private sector can also sometimes reduce or entirely displace the required capital expense.

- Engage citizens. Smart city services generally need to engage local residents to ensure success. When citizens see the benefits of these services, which may save them time and money and improve their quality of life, they can engage, support and promote them among their local communities, creating a virtuous circle. Transparency around the usage of data can quicken this process.

Resources:
GSMA Smart Cities website
GSMA Report: Keys to the Smart City
GSMA Video: Smart City Tainan case study

Personal Data

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. Personal data and user authentication are requisite elements of being online and it's 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 based on trust. Interactions — whether they be social, commercial, financial or intellectual — require a proportionate level of trust in the other party or parties involved. Without such trust, users will find other ways to browse, bank and buy. Currently, user authentication is inconsistent and inconvenient for users, and people are forced to keep track of numerous login names and passwords. Regulators and policymakers are also increasingly promoting the use of strong customer authentication processes to combat fraud and identity theft, as they realise that failing to address these problems will create barriers to market digitalisation and social inclusion.

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 to enable consumers, businesses and governments to interact in a private and secure environment.

The GSMA is working with mobile network operators and 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 safe and secure and doesn't share personal information without the user's permission.

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 digital identity solution introduced by the GSMA with the support of leading mobile operators. It offers a safe, seamless and convenient consumer experience, a consistent user interface and low barriers to entry across the digital identity ecosystem — thereby enabling global scale of mobile identity services. Since the solution was first introduced at Mobile World Congress 2014, 42 operators across 22 countries have implemented Mobile Connect, making it available to nearly three billion customers.

By combining the inherent security of mobile devices, the SIM and operator business processes and networks, Mobile Connect enhances user security and reduces the risk of identity theft. Mobile Connect opens up a range of opportunities for both mobile operators and consumer-focused service providers to build a rich suite of offerings for their customers, while ensuring the user's private and confidential information is kept safe.

- For consumers, Mobile Connect enhances users' privacy and allows them to log in to websites and applications quickly without the need to remember usernames and passwords, thereby simplifying the login experience for a range of services. With Mobile Connect, the user is authenticated through their mobile phone, rather than through personal information, making logging in safer and more secure. The solution employs both the user's mobile number and a unique PIN. These are combined with the secure network of the mobile operator to ensure the validity of the mobile device and user for more sensitive use cases, such as logging in to e-government and banking services.
- For service providers, Mobile Connect offers the advantages of an improved consumer experience (including reduced drop-off rates when signing on to new services), lower cost of managing credentials, and validation of important consumer attributes such as age, address or other network-related information.

Mobile Connect is based on an open standard solution — the OpenID Connect protocol — and offers broad interoperability across mobile operators and service providers, further ensuring a seamless experience for consumers. Mobile Connect can also provide different levels of security, ranging from low-level website access to highly-secure, bank-grade customer authentication. The flexibility of Mobile Connect promises to make passwords a thing of the past, while at the same time delivering better privacy and security.

Programme Goals

Mobile Connect puts operators at the heart of digital services by enabling them to offer strong authentication and digital identity solutions. By simply matching the user to their mobile phone, Mobile Connect allows users to log-in to websites and applications or perform transactions quickly, without the need to remember passwords and usernames.

A core principle of Mobile Connect is the protection of the privacy of end users, both by allowing for anonymous authentication and by offering users transparency on any information being shared. The solution has built-in mechanisms that makes it possible for users to manage their consent, giving them back control of their personal data.

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 digital 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 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, mobile operators, with their differentiated identity and authentication assets, have the ability to provide sufficient authentication to enable consumers, businesses and governments to interact in a private, trusted and secure environment and provide more secure and convenient access to services.

Resources:
Mobile Connect website
GSMA Personal Data website
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
GSMA Report: Mobile Identity — Unlocking the Potential of the Digital Economy
GSMA Case Study: Norwegian Mobile BankID — Reaching Scale Through Collaboration
GSMA Case Study: Swisscom Mobile ID — Enabling an Ecosystem for Secure Mobile Authentication

Business Environment

Governments have a responsibility to create a business environment that supports innovation and allows industry to thrive so it can have a positive social and economic impact. The mobile sector is highly dynamic, so flexible, light-touch regulation is essential. The market is best able to drive and shape the industry's evolution, as highly prescriptive regulatory policy cannot keep pace with the swift advance of mobile technologies, services and consumer demand.

One example is found in the current asymmetry that exists between the regulatory requirements placed upon mobile operators versus those of the internet players that provide IP-based voice and messaging services.

The mobile sector is among the most intensely regulated industry sectors, subject not only to common rules governing consumer protection and privacy, but a raft of sector-specific rules related to interoperability, security, emergency calls, lawful intercept of customer data, universal service contributions and more. It is also one of the most heavily taxed sectors around the world, facing a variety of industry-specific taxes, levies and fees.

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 antennas that transmit and receive radio signals, providing voice and data services to their customers in the area.

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 approval of small cell antennas and modifications to existing sites?

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 Base Station Planning Permission in Europe website
World Health Organization Electromagnetic Fields website
FCC Report: Acceleration of Broadband Deployment by Improving Wireless Facilities Siting Policies, et al
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

Facts and Figures

Radio Frequency Policies for Selected Countries

Country	RF Limit at 900MHz (W/m^2)	Requirement for RF licensing	Exemptions or simplified procedures for...	Location restrictions	Consultation during siting process
Australia	4.5	Compliance declaration	Small antennas, changes	None	Yes
Brazil	4.5	Approval	–	50m[a]	Local
Canada	2.7[b]	Approval	Small antennas, changes	None	Yes
Chile	4.5/1	Approval	Small antennas, changes	>50m[c]	Yes
Egypt	4	Approval	–	20m[d]	No
France	4.5	Approval	Small antennas, changes	Voluntary, to minimise exposure[e]	Local
Germany	4.5	Approval	Small antennas, changes	None	Yes
India [f]	0.45	Compliance declaration	–	None nationally, local variation	No
Italy	1/0.1	Approval	Small antennas	Lower limits[g]	Yes
Japan	6	Approval	Small antennas	None	Local

Country	RF Limit at 900MHz (W/m^2)	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 antennas	None	Yes
Netherlands	4.5	Compliance declaration	Small antennas, changes	None	Yes
New Zealand	4.5	Compliance declaration	Small antennas, 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 antennas, changes	None	Local
Turkey [h]	1.5	Approval	–	None	Local
United Kingdom	4.5	Compliance declaration	Small antennas, changes	None	Yes
United States	6	Approval	Small antennas, changes	None	Local

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

The end result is that mobile operators are currently caught between the two worlds and consumers may not receive the full benefit of these competitive markets.

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 due to 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 iindustry-, 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 has published a report called Resetting Competition Policy Frameworks for the Digital Ecosystem that includes 15 detailed recommendations, summarised on the following pages.

Resources:
GSMA Handbook: Competition Policy in the Digital Age
European Parliament Report: Challenges for Competition Policy in a Digitalised Economy

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 the 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

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.

Resetting Competition Policy Frameworks – Recommendations

The GSMA advocates that governments adopt the following recommendations to ensure their competition policy frameworks remains 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. Traditionally, the main policy tool used to support this market structure has been spectrum licensing. From 2000 onwards, policymakers have licensed an increasing number of mobile network operators in an effort to drive competition and improve market performance.

The policy tool of spectrum licensing has led to the current situation where the number of countries with a single mobile provider has reduced from about half of the countries in the world in 2000 to a small number of states representing less than three per cent of the world's population today.[1]

There is great demand from both users and policymakers for high-speed, high-quality, robust and secure mobile networks and this has driven mobile operators to make large investments in network infrastructure and services. These investments are ongoing as the mobile industry typically follows a ten year (or shorter) technology cycle, so while operators are currently investing heavily in 4G networks, in a few years' time the focus of investment will shift to 5G technology.

The high level of competition in the markets for mobile services has seen the tariffs charged to mobile users fall dramatically, so users now get more for their money. At the same time, operators are constantly investing in network improvements to provide consumers with a better quality of service.

While preserving competition to drive innovation and wider societal benefits, policymakers must not create or maintain artificial and uneconomic conditions that force prices down to untenable levels, deterring operators from investing in their networks.

National regulatory authorities must also recognise the competitive nature of today's mobile markets, avoid interventions aimed at engineering market structures and allow market mechanisms to determine the optimal mobile market structure.

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.

[1] Frontier Economics, Assessing the case for Single Wholesale Networks in mobile communications (2014)

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 under-utilised 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

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 a number of key European countries, including Austria, Germany, Ireland and the United Kingdom. On one side, some argue that consolidation has a detrimental effect on prices and quality, while others believe that if consolidation does not take place, mobile markets will not achieve the necessary scale, attract sufficient investment and benefit from the technology upgrades required to support the digitisation of society, drive innovation and spur future economic growth.

In the past two years there have only been a limited number of economic papers published that have analysed how mergers impact investment. We have reviewed the key papers[1] among these and summarised our findings below.

The key finding is that post-merger, there is evidence that concentration leads to greater investments at the company level. While many believe that consolidation is likely to lead to a reduction of investment by operators (due to a lowering of competition intensity), the evidence actually points towards 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.

Initial evidence from the Austrian market following the merger between Hutchison 3G and Orange shows that the extra investment capacity resulting from the merger has been used to speed up 4G roll out to meet the increasing demand for mobile broadband. It shows that 4G coverage in Austria expanded at a faster rate than in countries that did not undergo a merger.

[1] CERRE (2015), Frontier (2015), Houngbonon & Jeanjean (2015), Houngbonon & Jeanjean (2016), HSBC (2015), WIK (2015)

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	

- Only WIK (2015) concludes that consolidation does not raise investment. However, our assessment framework indicates that this study covers a restricted number of countries and a limited timeframe, and that it does not take into account the circular relationship between market structure and investment.

- Investment per operator is found to consistently increase with concentration according to CERRE (2015), Houngbonon & Jeanjean (2016) and Frontier (2015). The first two studies score particularly well in taking account of relevant factors that shape investment — they use datasets that have a global outlook and also take into consideration all feedback effects. They also use investment per company as a metric, which we conclude is a better metric than country aggregates as it reflects operator behaviour. The issue with country aggregates is that it leaves you with a 'black box' of data where operators' investment decisions cannot be fully observed.

- Another set of studies — Houngbonon & Jeanjean (2015) and HSBC (2015) — suggests that consolidation only boosts investment per operator if profit margins are below a certain threshold, which is the case in most developed markets. Our assessment framework indicates that this evidence base is robust for the same set of reasons outlined in the point above.

Environment and Climate Change

Background

Governments, industry and the wider public broadly accept the need to reduce greenhouse gas emissions to limit global warming and climate change. This has been reinforced by the ratification in 2016 of the Paris Agreement on Climate Change.

As mobile use expands, so does the demand for energy, particularly by the network infrastructure. More than 80 per cent of a typical mobile network operator's energy requirements are associated with powering the network. Nevertheless, the mobile industry is responsible for a small fraction of global greenhouse gas (GHG) emissions, at less than 0.5 per cent. However, energy is a significant cost for mobile operators, especially in emerging markets.

Mobile network operators and manufacturers have been improving the energy efficiency of mobile network infrastructure and turning to renewable energy sources such as solar, wind and hybrid power systems to power off-grid, rural base stations.

An analysis of 65 mobile networks showed that total network energy consumption increased only four per cent from 2010 to 2011, despite considerable growth in mobile traffic and connections. Total energy per unit traffic declined by approximately 30 per cent, and energy per connection declined by three per cent.

The mobile industry's goal is for GHG emissions per connection to drop by 40 per cent between 2009 and 2020.

The European Union (EU), in particular, is pushing for the information and communication technology (ICT) sector to use detailed carbon accounting to help the EU meet GHG reduction targets.

Debate

In addition to the mobile industry's continued focus on reducing its own emissions, should it also work towards ICT-enabled emission reduction in other sectors? If so, how can governments help, especially in the light of the Paris Climate Agreement?

What is the role of government in using mobile technology to reduce emissions generated by its own public services, for example by promoting green ICT solutions?

How can the mobile industry's impact in contributing to achieving the Sustainable Development Goals be expanded and strengthened?

Industry Position

The mobile industry acknowledges its role in managing greenhouse gas emissions, but also believes governments should encourage mobile machine-to-machine (M2M) communications in sectors where the potential to reduce emissions is greater.

Research has identified the potential for the mobile industry to reduce GHG emissions in other sectors — including transportation, buildings and electrical utilities — by at least four to five times its own carbon footprint. The savings principally come from smart grid and smart meter applications, as well as smart transportation and logistics.

The mobile industry is taking active steps to increase the energy efficiency of its networks and reduce emissions. With mobile network operators spending around $17 billion on energy use annually, energy efficiency and emission reduction are strategic priorities for them globally.

The GSMA's Mobile Energy Efficiency Benchmarking service enabled network operators to evaluate the relative energy efficiency of their networks. More than 40 mobile operators participated in the service, accounting for more than 200 networks and over half of all global mobile subscribers.

The GSMA's Mobile Energy Efficiency methodology has been adopted in the International Telecommunication Union (ITU) recommendation for environmental impact assessment of ICT networks and services. The GSMA has also contributed to the European Telecommunications Standards Institute's work on developing international standard ES 203 228, which defines an energy efficiency measurement method for base stations.

The Green Power for Mobile programme, a joint initiative of the GSMA and the International Finance Corporation (IFC) — a member of the World Bank Group — promoted the use of renewable and green energies to extend mobile coverage beyond the available grid.

Resources:
GSMA Mobile Energy Efficiency website
GSMA Report: 2016 Mobile Industry Impact — Sustainable Development Goals
GSMA Reports: Mobile's Green Manifesto 2009 and 2012 update
GeSI Smarter 2030 analysis website
GeSI & Carbon Trust Report: Mobile Carbon Impact
Broadband Commission Report: Means of Transformation — Harnessing Broadband for the Post 2015 Development Agenda
Broadband Commission Report: The Broadband Bridge — Linking ICT with Climate Action for a Low-carbon Economy

Case Study

A Green Power Feasibility Study for Airtel Madagascar

Globally, a 16 per cent increase in off-grid and poor-grid telecommunications sites is expected in the next six years. Adoption of alternative and renewable power generation is necessary for mobile operators to keep operation costs in check and responsibly manage the volume of carbon emissions their networks generate. To this end, the GSMA Green Power for Mobile programme works with mobile operators to provide market analysis and consulting, technical assistance and business model design.

In 2013, the GSMA conducted a green power feasibility study for Airtel Madagascar to demonstrate the technical feasibility and financial viability of green power alternatives to the operator's existing power approach, in order to reduce Airtel's dependence on diesel generators and hence reduce CO_2 emissions. The feasibility study acknowledged a number of challenges faced by the operator, including:

- Poor access to network base stations.
- Low penetration of grid power and high cost of grid extensions.
- High cost of diesel for off-grid base station generators.
- Lack of domestic suppliers for renewable energy and technologies.
- Lack of policy support for renewable energy deployment.

Given these conditions, the GSMA advised Airtel to implement a hybrid grid-battery approach for its on-grid sites, to reduce dependence on a diesel generator to power the base station. For off-grid sites, three options were identified: extending grid power to the base station, installing a renewable power solution, or implementing a diesel generator and battery combination.

Following the GSMA's site-by-site analysis, Airtel was advised to implement a solar-hybrid energy solution for 147 sites, extend grid power to 48 sites and implement a diesel-battery hybrid for 21 sites. Other recommendations included implementing smart-energy monitoring and equipment-control mechanisms for all sites, and installing smart controls to select the appropriate power source (i.e., solar, grid power, batteries and diesel generator).

Airtel Madagascar has begun implementing the recommended changes, and the GSMA calculates that the operator will reduce its energy bill by over 90 per cent across the 147 sites where a green solution is deployed. In the case of off-grid or poor grid sites, energy costs can constitute as much as 75 per cent of a site's annual operation cost. Airtel Madagascar used to spend approximately $25,000 per year on energy generation and management for one site, plus approximately $9,000 covering rent, overhead and battery replacement costs. After the solar-hybrid implementation, Airtel's energy generation and operation costs will drop to around $3,000 per site per year.

In addition to the financial advantages of this green energy approach, the environmental outcomes will be considerable when the upgrades are complete:

- A reduction in diesel consumption of 1.12 million litres per year.
- A 75 per cent reduction in diesel generator dependency.
- Green energy solutions offering an average return on investment within 2.25 years.
- Reduced CO_2 emissions by 3,120 tons per year.
- 978,876 kWh per year generated from renewable energy sources.

Gateway Liberalisation

Background

International gateways (IGWs) are the facilities through which international telecommunications traffic enters or leaves a country.

In emerging markets, fixed-line telecoms incumbents were granted monopolies over IGWs, the assumption being that an IGW monopoly allows a country to manage its international charges and, in so doing, enables the incumbent to fund a national network roll out.

Through changes in technology and the deployment of new services such as VoIP, it has become possible to bypass monopoly gateways. Such examples of bypass have significantly increased competition and lowered international prices.

Unfortunately, some countries have levied a new telecommunication specific tax in the form of a surcharge on international inbound traffic (SIIT), which amounts to double taxation for inbound calls.

The presence of monopoly international gateways tends to also inflate the price for mobile roaming services.

In the late 1990s and 2000s, most countries liberalised IGW. By the end of 2013, less than 15 per cent of markets remained monopolies and typically these are very small island nations, or underdeveloped, troubled states.[1]

Debate

Which structure for international gateways, monopoly or liberalised, best serves a country and its citizens?

The evidence shows that liberalisation actually stimulates investment and that the fear of loss of international revenues is illusory... Combined with the wider economic benefits to a country and its government, IGW liberalisation is a rational and best practice regulatory response to the IGW monopoly.

— GSMA Research report on the Benefits of Gateway Liberalisation, 2007

Industry Position

Competition in international gateway services should be encouraged, as it leads to reduced consumer costs, more international bandwidth and improved quality of service to operators.

IGW liberalisation delivers macroeconomic benefits by lowering the cost of business, ensuring diversity of supply and international competitiveness, attracting investment and increasing connectedness in the global economy.

Countries that have attempted to maintain IGW monopolies are vainly attempting to hold back the tide, as illegal bypass can account for up to 60 per cent of traffic. Although bypass delivers cheap prices to consumers, it does so at the cost of service quality and the risk of service interruption when local services relying on illegal technologies are shut down.

For developing countries to fully participate in a globalised world, their IGWs must be fully liberalised to allow competition and private investment.

By allowing IGW monopolies to operate, governments are faced with significant regulatory and law-enforcement costs to prevent illegal bypass, while losing out on the tax revenue that could be generated by legal services.

Where the liberalisation of an IGW is intended, international best practice suggests that competitive safeguards can be put in place to ensure that the environment evolves in a fair manner. There may be a need to regulate incumbent operators to ensure reasonable access to 'bottlenecks' (such as cable stations, duct work and backhaul), which are under the control of the incumbent.

[1] Arthur D Little research for GSMA 2015

Resources:
GSMA Report: Gateway Liberalisation — Stimulating Economic Growth
GSMA Report: Mobile Taxation — Surcharges on International Incoming Traffic

Infrastructure Sharing

Background

Common in many countries, infrastructure sharing arrangements allow mobile operators to jointly use masts, buildings and even antennas, 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 cooperation 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
ITU Mobile Infrastructure Sharing website
ZDnet: Could Tower-Sharing Be the Solution to Rural Networks' Problems?
London Business School Review: Indus Towers — The India-way of Business

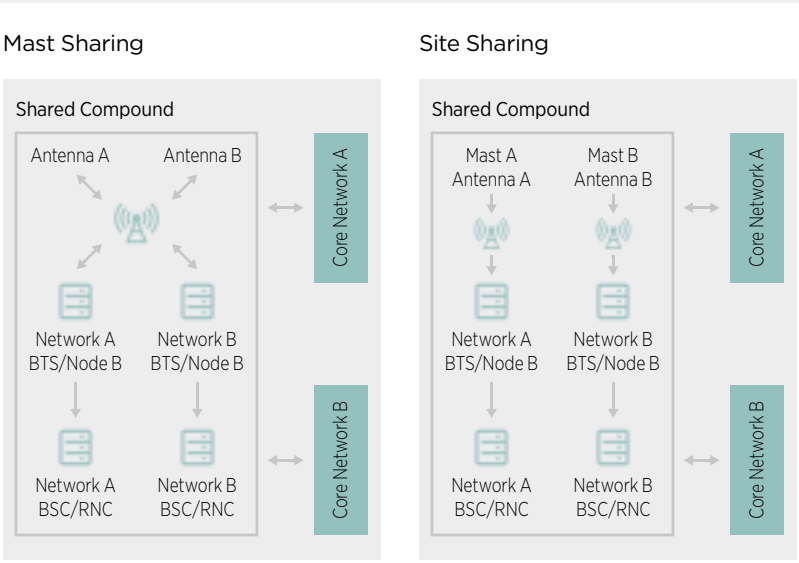
Deeper Dive

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, antennas, 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 antennas 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.

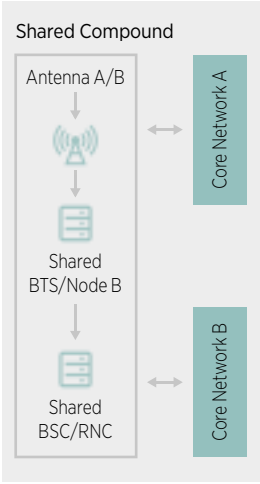
Infrastructure sharing optimises the utilisation of assets, reduces costs and avoids duplication of infrastructure (in line with town and country planning objectives).



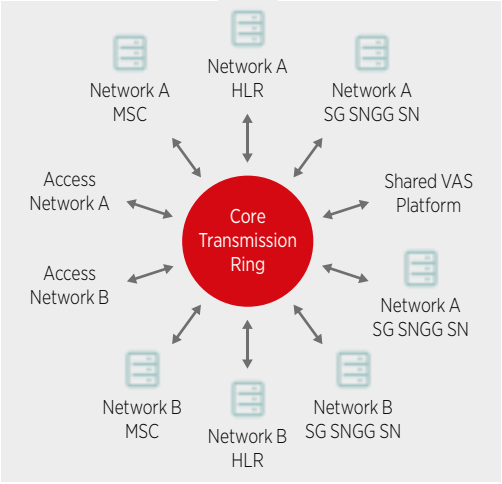
It may also:

- 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.

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. The European Union's copyright provisions from 2001 are outdated and the debate on how to best adapt them to the realities of today's digital world has been going on for years.

Views in the debate vary widely. Rights holders advocate strong laws and cooperation of internet service providers and telecom companies in fighting piracy. Civil society organisations defend consumers' fundamental rights (e.g., freedom of expression and access to the internet) and strongly oppose any measures to combat piracy. Collecting societies, which have the authority to license copyrighted works and collect royalties as part of compulsory licensing or individual licences negotiated on behalf of its members, oppose content licensing reform and defend national licences.

In September 2016, as part of its Digital Single Market strategy, the European Commission published its long-awaited proposals on copyright provisions, and also on the modernisation of transmission rights. A proposal on temporary cross-border portability of content within the EU is also on the table. Lively debates can be expected in the European Parliament and the Council.

Debate

Should mobile network operators be expected to monitor and address the unlawful use of copyrighted content on their networks?

Is a device levy a legitimate way to compensate artists and publishers for their creative works?

What is the best way for Europe or other regions to enable intellectual property to be used by mobile subscribers in multiple countries?

Industry Position

The mobile industry recognises the importance of proper compensation for rights holders and prevention of unauthorised distribution. Expanding the legitimate content market is key in fighting illegal file sharing.

Communications service providers, including mobile network operators and ISPs, should not be held liable for illegal, pirated content on their networks and services, provided they are not aware of its presence and follow certain rules to remove or disable access to the illegal content as soon as they are notified by the appropriate legal authority.

The development of new content licensing models should fall to the rights holders. Obligations on ISPs to monitor piracy should take a light touch, if they are employed at all.

Handset levies or a 'global licence' are not the right policy instrument to compensate rights holders for piracy. Content licensing reform is needed to enable new business models for rights holders and commercial users, and attractive content offers for consumers.

Resources:
European Commission Modernisation of EU copyright rules website
MEP Julia Reda: EU copyright evaluation report – full current text
European Commission Management of Copyright and Related Rights Directive website
European Commission Orphan Works Directive website

Intellectual Property Rights — Patents

Background

The mobile ecosystem has been a major driver of economic progress and welfare globally. In the period to 2020, mobile's contribution will grow at a faster rate than the rest of the global economy, contributing 4.2 per cent to the world's GDP by the end of the decade. 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.

Meanwhile, 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 engaged in purchasing patents so they can focusing on aggressive litigation against manufacturers and operators already using the technology, rather than developing and licensing technology.

Unfortunately, the complexity of mobile operators' networks, the scale of investments needed to build them, the level of revenues generated by them, and the reliance of these networks on technology based on standards, has made mobile network operators a prime target for so called patent trolls in Europe, America and Asia.

The multiple costs associated with both ligation from PAEs, and their use of the threat of injunction as leverage in demands for disproportionately high licensing fees, are having a seriously negative effect not just on the affected mobile network operators' business, but also mobile telecommunications innovation and standardisation, as well as the future of mobile operators' networks in general.

In light of the increasingly litigious environment resulting from the business model used by PAEs and the adversarial nature of the associated licensing negotiations, there is a need for greater clarity in relation to the licensing in, and adjudication of, such PAE cases for licensors and implementers alike. This should take account of:

- 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:
European Commission Report: Patent Assertion Entities in Europe

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. The latest regulation prohibits retail roaming surcharges from being applied to domestic prices across the EU from mid-June 2017, provided that the wholesale roaming market review is completed by that date. 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.

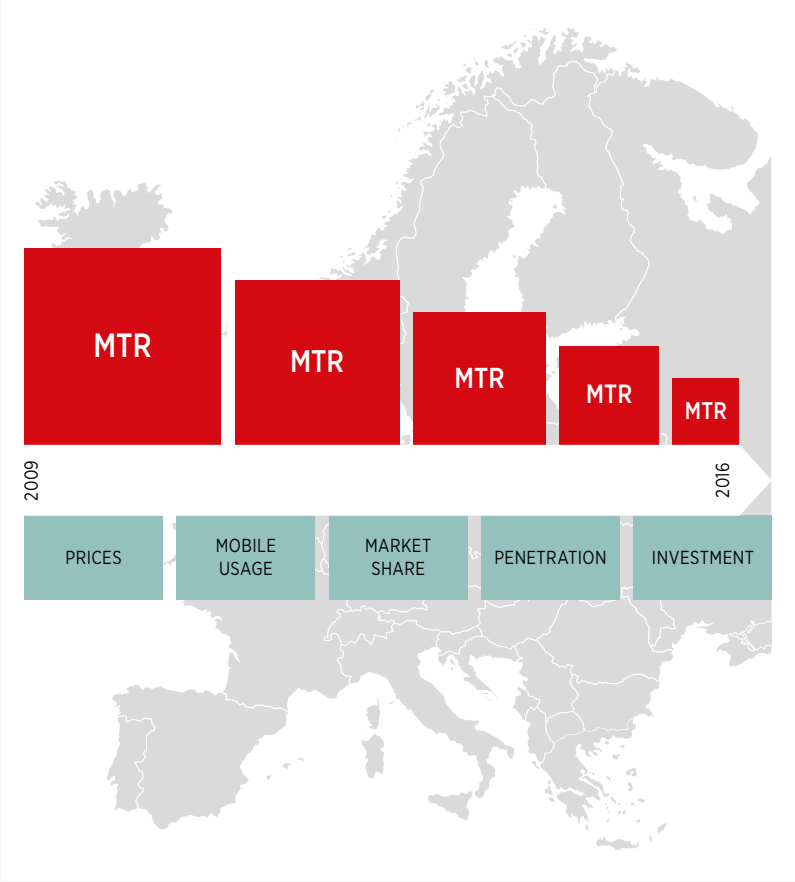
The GSMA believes the setting of MTRs is best done at a national level, where local market differences can be properly reflected in the cost analysis, therefore extraterritorial intervention is not appropriate.

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

Case Study

Impact of Accelerated MTR Reductions in Europe

In 2009, the European Commission recommended an accelerated reduction in mobile termination rates, proposing that Member States implement rates based on the pure Long Run Incremental Cost (LRIC). It reasoned that the MTR cuts would reduce mobile prices and therefore increase usage, while also helping smaller mobile network operators to be price competitive.



Frontier Economics was commissioned in 2012 by Vodafone to determine whether the policy — to the extent that it has been applied in EU countries — has had the intended effect. Among the findings are these points:

1. There is no evidence that faster MTR cuts have led to lower mobile prices.

Although mobile prices in Europe have been falling, there is no support for the view that this has been driven by MTR cuts.

2. There is no evidence that MTR cuts are increasing usage.

Since 2009, usage has not increased at an accelerated rate, and countries with the largest MTR cuts have not had the largest increases in usage.

3. There is limited evidence of any link between MTR reductions and the market share of smaller operators.

While nearly all of the smallest operators experienced an increase in their market share, no link with the MTR reductions was observed.

4. Accelerated MTR cuts could be detrimental to network investment and mobile penetration.

While it is too early to conclude whether the MTR cuts are having a detrimental effect, there is some indication that mobile penetration and investment are being adversely affected.

Source: Frontier Economics, 'The Impact of Recent Cuts in Mobile Termination Rates Across Europe', May 2012

Net Neutrality

Background

In 1973, work began on establishing a global network of networks, an 'internetworking' project that became the internet. The objective was to design a network that was self-sustaining, and that would be able to run applications not yet designed. The solution was simple and rested on two rules: there can be no central control, and the network cannot be optimised for any single application.

Today's net neutrality debate has evolved from these two rules. Networks that were connected to the internet had to communicate via common protocols, primarily the Transition Control Protocols and the Internet Protocol (TCP/IP), an architecture that rendered network performance as best efforts and assumed the intelligence would be either in applications or at the user interface (i.e., on computer terminals).

While there is no single definition of net neutrality, it is often used to refer to issues concerning the optimisation of traffic over networks. Some argue that it is necessary to legislate that all traffic carried over a network be treated in the same way.

Others advocate that flexibility to offer varying service levels, for different applications, enhances the user experience.

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.

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.

With finite capacity, mobile networks 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 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 Communications 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. According to industry research, global instant messaging volumes from OTT providers already exceed SMS volumes. Research also shows that Voice over-IP (VoIP) now accounts for over 40 per cent of international voice traffic. Fuelling this trend, OTTs are increasingly developing techniques to influence users' decisions about whether calls and messages should go through the Public Switched Telephone Network (PSTN) or the internet.

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 are able to sit outside the scope of sector-specific national or regional regulatory and fiscal obligations (e.g., data 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.

— European Commission Vice President Andrus Ansip, March 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 the fact OTTs currently play to 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:
TeleGeography Report & Database: 2014
Deloitte Report: Technology, Media & Telecommunications Predictions 2016

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 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

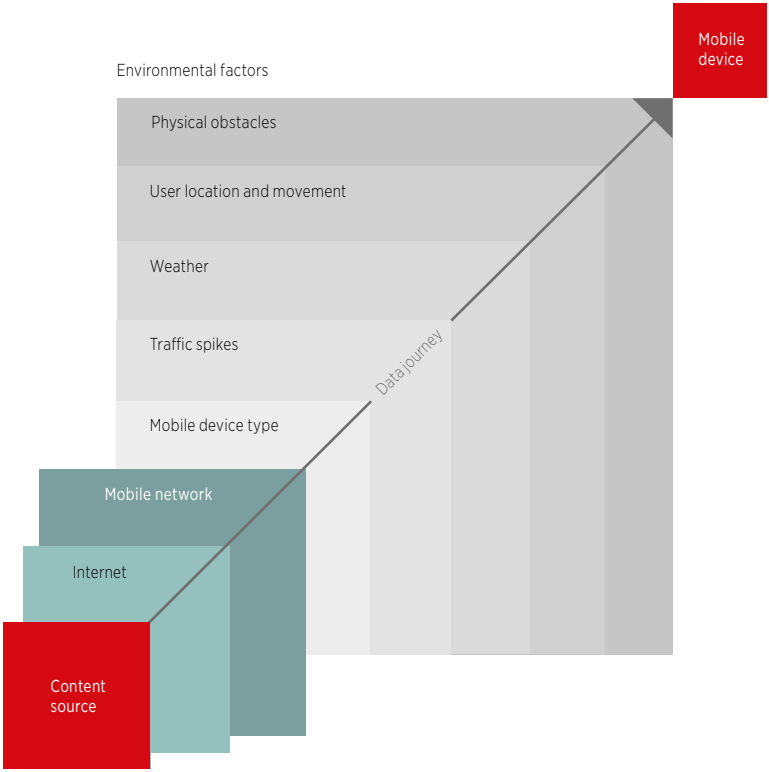
Offering a dependable quality of service is a priority for mobile network operators, as it allows them to differentiate the internet access service they provide from that of their competitors and meet customer expectations. However, mobile operators have little control over many of the parameters that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

Factors beyond operators' 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 antennas.
- 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 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 a single wholesale network (SWN) 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 by competing networks. Only 30 countries today, representing less than three per cent of the world's population, are served by a single mobile network. Since 2000, network competition has produced unprecedented growth and innovation in mobile services, particularly in developing countries. For example, the number of unique mobile subscribers has almost tripled in developed countries from 339 million in 2000 to over 880 million today, while in developing countries the number of subscribers has increased from 131 million to more than 2.5 billion.[1]

Supporters of SWNs argue that they can address some issues better than the traditional model of network competition in some markets. These concerns generally include inadequate or slow coverage in rural areas, inefficient use of radio spectrum and concerns 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 will lead to worse outcomes for consumers than network competition.

Some SWN supporters claim that SWNs will deliver greater network coverage than network competition can, but this claim often reflects the existence of public subsidies and other forms of support for the SWN, which are not available to competing network operators. The claim is therefore unsupported. Network competition can deliver coverage in areas where duplicate networks are uneconomic through voluntary network sharing and the commercial incentive of being first to market in a particular area.

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, single networks have been much slower to expand coverage, perform upgrades and to embrace new technologies such as 3G, and SWNs can be expected to prompt less innovation than network competition.

To achieve the objectives of their proponents, SWNs would need to evolve into regulated monopolies, leading to worse long-term outcomes for consumers. As monopolies, SWNs will always have incentives to keep prices high and reduce expenditures, including network deployment to increase coverage. Although regulation can attempt to ensure SWNs mimic the outcomes of a competitive market, it will not fully succeed.

SWNs may co-exist for some period with existing networks. As SWNs are likely to be supported by governments, this will likely lead to a distortion of competition. Co-existence is also likely to increase uncertainty, which will have a dampening effect on investment in mobile broadband services.

The evidence suggests that the design, financing and implementation of SWNs are likely to prove challenging and that there is a significant risk of failure.

Although a publicly funded SWN could deliver coverage in areas into which privately funded competing networks would not be willing to expand, the correct approach is to consider how public subsidies could be used to extend the benefits of network competition to those areas. This can be achieved in a variety of ways, including coverage obligations and other forms of subsidy, such as the award of contracts to cover particular areas using public funds.

[1] Source: GSMAi

Resources:
GSMA & Frontier Economics Report: Assessing the case for Single Wholesale Networks in mobile communications

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 Resource website
GSMA Report: Digital Inclusion and Mobile Sector Taxation 2016

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 operators' 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:

- Across 30 selected markets, the total tax and fee payments from the mobile sector amounted to $52 billion in 2014. Of this total, $18 billion was accounted for by sector-specific tax and fee payments.

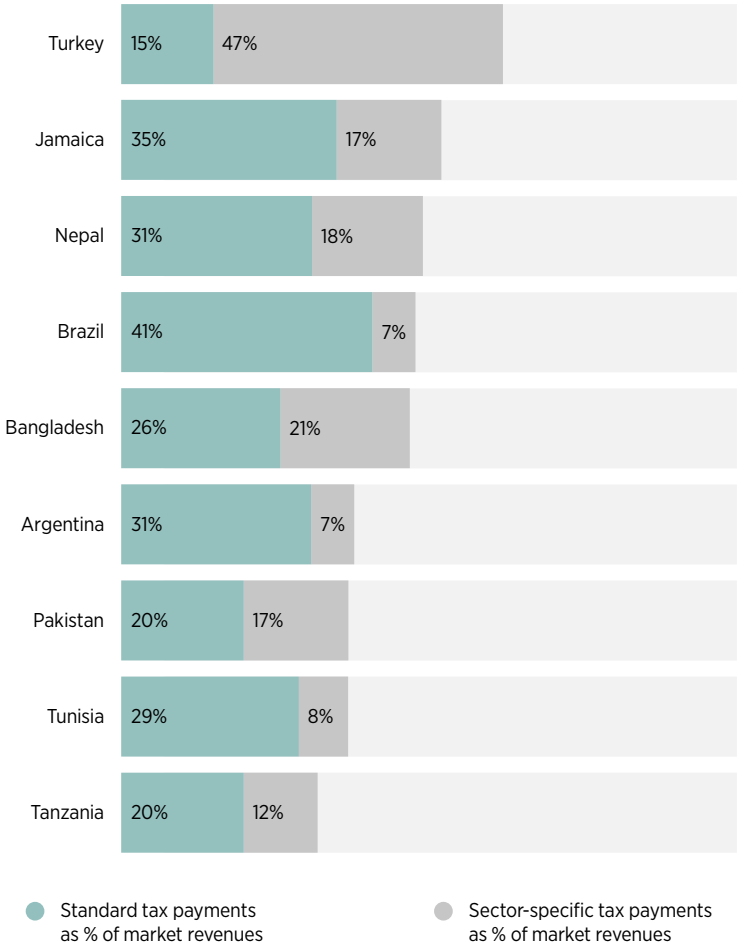
- Total mobile tax payments on both consumers and operators represent on average 29 per cent of market revenue, excluding non-recurring payments such as spectrum auction fees.

- In Turkey, mobile tax and fee payments represent 62 per cent of sector revenues, with the majority of this related to sector-specific taxation.

Moreover, the mobile sector's relative contribution in terms of tax and fee payments as a share of total government tax revenues is higher than the sector's share of GDP in 20 out of the 23 developing countries. In nine countries, taxes and fees on the mobile sector are nearly twice, or in some cases more than twice, the sector's share of GDP.

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. In 2014, the price of mobile broadband constituted on average 37 per cent of the annual income for the poorest 20 per cent of the population.

Estimated tax and fee payments as a proportion of market revenues across selected countries, 2014



Source: Deloitte analysis based on mobile operator and GSMA Intelligence data for 2014

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 countries' citizens and increasingly large accumulations of undisbursed funds.

According to a 2013 report commissioned by the GSMA, less than one-eighth of the 64 USFs studied are achieving their targets, and more than one-third have yet to disburse any of the funds they have collected. Nevertheless, the levies continue to be required from the sector.

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.

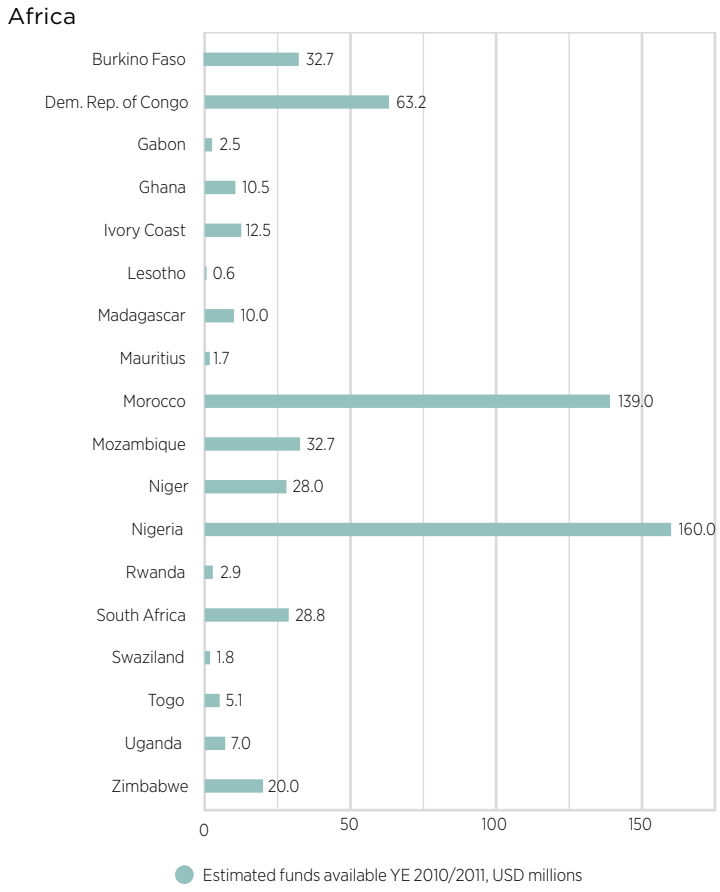
Governments should consider incentives that facilitate market-based solutions. They can help by removing sector-specific taxes, stimulating demand and developing the supporting infrastructure. Alternative solutions such as public-private partnerships should be explored in preference to USFs for the extension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

Resources:
GSMA Report: Survey of Universal Service Funds, Key Findings
GSMA Connected Society: Are Universal Service Funds an effective way to achieve universal access?

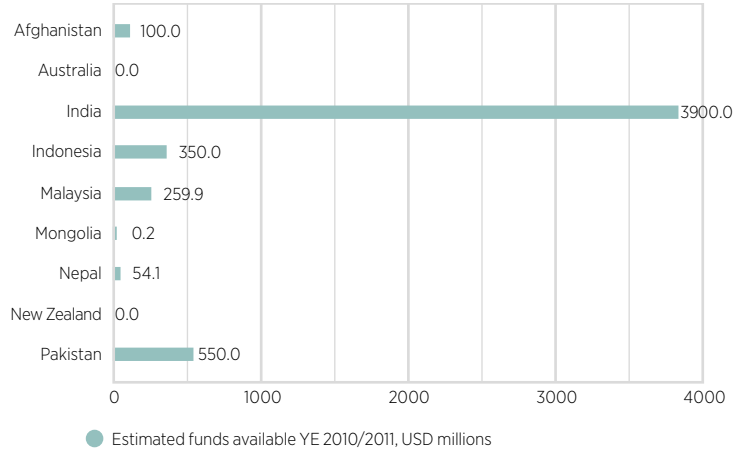
Facts and Figures

Estimated Universal Service Funds Available

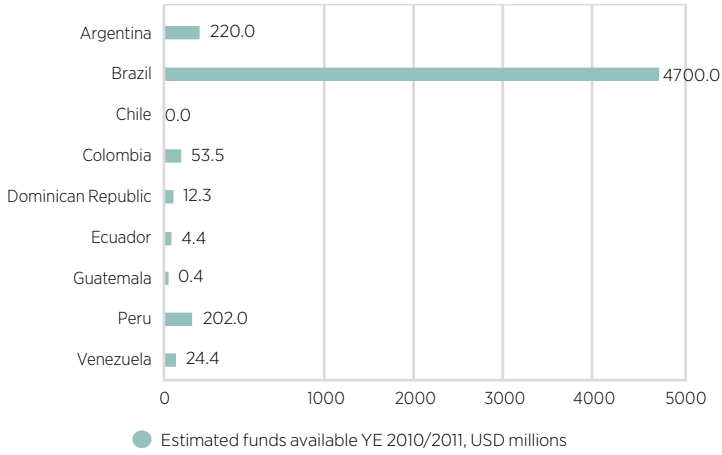
Despite the admirable goals that led to the creation of USFs during the early stages of telecoms liberalisation, there is now considerable doubt about their practicality and efficacy. A large proportion of USF monies collected remain undisbursed, and the structure of many USFs is too rigid to respond to rapid technological changes and societal requirements.



Asia Pacific



Americas



Source: GSMA, Survey of Universal Service Funds, April 2013

Spectrum Management and Licensing

Mobile data traffic continues to skyrocket and as the nascent Internet of Things industry grows, it too will place significant extra strain on mobile networks.

To meet this increasing demand, operators need access to sufficient, internationally harmonised spectrum. Here, effective spectrum licensing plays a key role, as it helps the industry attract the investment needed to further expand mobile access and enhance the quality and range of services offered.

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. On this issue, we work with national governments and regulators, regional organisations and the International Telecommunication Union (ITU).

Governments must also play their part in the development of mobile communications. Those that simply seek to maximise state revenues from spectrum pricing, for example, risk much greater costs to society if competition in communications markets is undermined and network investment is stifled as a result. 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 the World Radiocommunication Conference 2019 (WRC-19) on the horizon, governments should build upon the foundations of WRC-15 to strengthen the future of mobile communications. In particular, emerging 5G technology offers enormous potential for both consumers and industry. Discussions about TV white space, which typically consists of unused spectrum in broadcasting bands, should not take focus away from these core issues.

2.6GHz Frequency Band

Background

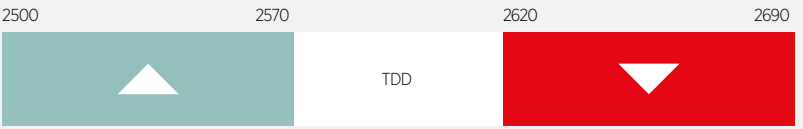
The International Telecommunication Union (ITU) has identified the 2.6GHz band (2500–2690MHz) globally for mobile broadband. It is a 'capacity band' that responds to the soaring demand for data-heavy content, such as video. The band has the potential to be used in a harmonised manner on a global basis. The harmonised use will result in economies of scale for industry and cheaper handsets for consumers, as well as increased flexibility for roaming.

The ITU has proposed several possible band plans, including:

- Option 1: 2x70MHz for FDD with a 50MHz TDD in the centre gap.
- Option 2: FDD only.
- Option 3: Flexible TDD/FDD arrangement.

Excessive per-MHz spectrum costs are an issue in certain markets, as a result of governments seeking to ration spectrum in order to maximise short-term revenue from the auctions.

2.6GHz Band Plan – Option 1



Debate

Should the 2.6GHz band be released in conjunction with the Digital Dividend band (700MHz/800MHz) to meet urban and rural coverage and capacity needs for mobile broadband?

Which band plan option is best?

Industry Position

We support ITU Option 1 for a globally harmonised 2.6GHz capacity band. Global momentum for the 2.6GHz band is behind ITU Option 1, with countries such as Brazil, Canada, China, Germany, New Zealand, Nigeria, Russia, Saudi Arabia and South Africa having already assigned the spectrum to mobile operators under this band plan. Where auctions have offered flexibility, markets have chosen standard band arrangements. The 2.6GHz band will be critical in meeting the capacity requirements of mobile broadband.

ITU Option 1 is a technology-neutral option, supporting both TDD and FDD technologies. The spectrum available in the 2.6GHz band provides for large carriers such as 2x20MHz, which is ideal for the deployment of LTE:

- To improve network performance, offering faster data transmission and greater capacity.
- To reduce deployment costs.
- To improve handset performance.

Higher frequencies (e.g., 2.6GHz) are better suited to high data rates required to serve large numbers of users in urban areas, airports and other high-traffic locations. Governments should not look to generate excessive fees from the licensing of 2.6GHz spectrum, as this will artificially limit demand, negatively impact network deployment, increase consumer prices and limit the potential economic benefits. Excessive fees can also impede policy goals designed to deliver mobile broadband access to everyone.

Resources:
GSMA Report: The 2.6GHz Spectrum Band — An Opportunity for Global Mobile Broadband
GSMA & Analysys Mason Report: Taiwan — Economic Impact of Wireless Broadband
GSMA Report: The Socio-Economic Benefit of Allocating Harmonised Spectrum in the Kingdom of Saudi Arabia
GSMA & Plum Report: The Benefits of Releasing Spectrum for Mobile Broadband in Sub-Saharan Africa
GSMA & Deloitte Report: Arab States Mobile Observatory 2013

Deeper Dive

Band Characteristics – Capacity vs. Coverage

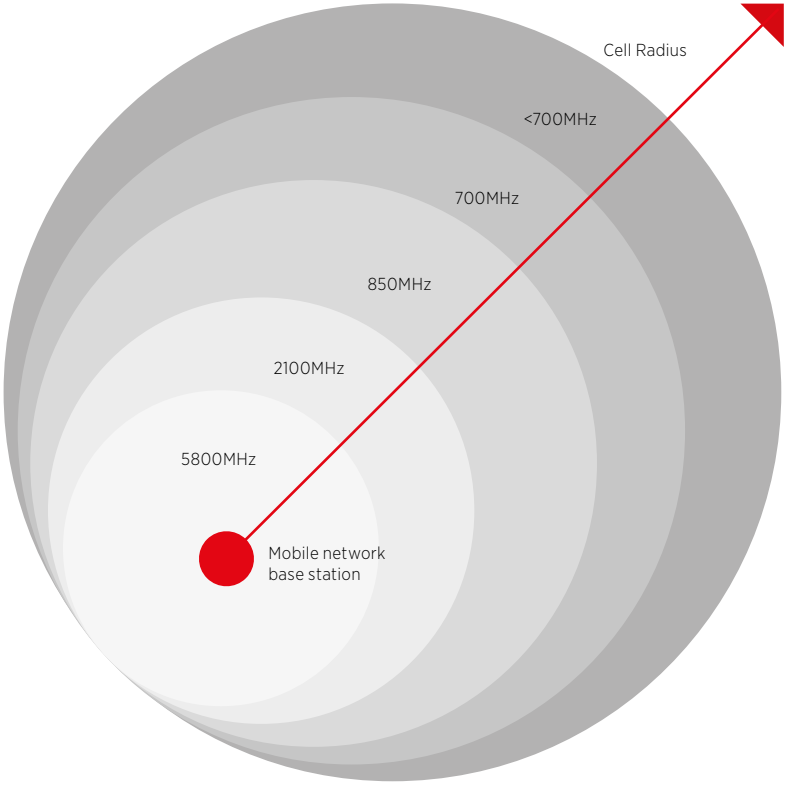
Not all radio frequencies are equal, and mobile network operators require access to a range of frequency bands to cost effectively offer a high-quality service for different locations with different population densities and different demands on the network.

In general, lower-frequency signals reach further beyond the visible horizon, and are better at penetrating rain or buildings. These lower radio frequencies are sometimes called coverage bands because, as a rule, an operator can serve a larger area with one base station.

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 many wireless applications, the best trade-off of these factors occurs in the frequency range of roughly 400MHz to 5GHz, and there is great demand for this portion of the radio spectrum.

Importantly, deploying a network that uses higher-frequency capacity bands requires more base stations to cover the same area, and considerably more investment.

Effects of frequency on range



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

5G Spectrum

Background

5G is expected to support significantly faster mobile broadband speeds and increasingly extensive mobile data usage, while also enabling the full potential of the Internet of Things (IoT). From virtual reality and autonomous cars to the industrial internet and smart cities, 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.

5G is expected to address three key usage scenarios: enhanced mobile broadband, including multi-gigabit per second (Gbps) data rates; ultra-reliable communications, including very low latency (sub-1ms) and very high availability and security; and massive machine-type communications, including the ability to support a huge number of low-cost IoT connections. The aim of 5G is to create a more 'hyper connected' society by integrating LTE (in licensed and unlicensed bands), Wi-Fi and cellular IoT technologies, together with at least one new 5G radio interface, in a more comprehensive and intelligent way.

The success of the services will be heavily reliant on national governments and regulators. Most notably, the speed, reach and quality of 5G services will be dependent on governments and regulators supporting timely access to the right amount and type of spectrum, and under the right conditions. 5G services will initially begin in more developed mobile markets. However, developing markets may follow in quick succession, especially in order to offer a fibre-like wireless experience and improved IoT support.

5G will be defined in a set of standardised specifications which will be agreed by international bodies — most notably the 3GPP and the ITU. The initial 3GPP '5G' standard, which will be a candidate for the ITU's standards, is not expected to be published until 2019, with widespread commercial services expected to follow in the early 2020s. However, smaller scale, pre-standards-based 5G deployments are expected to begin beforehand.

Debate

How can governments and regulators enable widespread 5G coverage rather than just in city centres?

Why is spectrum above 6GHz useful for 5G?

What is the benefit of a globally harmonised approach to 5G spectrum?

Industry Position

Significant new widely harmonised mobile spectrum is needed to ensure 5G services meet future expectations and deliver the full range of potential capabilities.

5G needs spectrum within three key frequency ranges to deliver widespread coverage and support all use cases. These ranges are:

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

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

Above 6GHz. This meets the ultra-high broadband speeds envisioned for 5G. A focus will be on bands above 24GHz, including growing interest in the 24GHz and/or 28GHz bands that could be easily implemented together in a single device due to their close proximity. There is also some interest in exploring bands in the 6-24GHz range.

Governments and regulators hold the key to realising the full potential of 5G when they agree new mobile bands above 24GHz at WRC-19. It is essential that they agree a sufficient amount of harmonised 5G spectrum to enable the fastest 5G speeds, low-cost devices, international roaming and to minimise cross-border interference.

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

There is significant potential for the coexistence of 5G and other wireless services (e.g., satellite and fixed links) in higher-frequency bands (e.g., above 24GHz).

Technology neutral spectrum licences are essential. They allow bands used for existing mobile technologies to be easily refarmed for 5G, ensuring the spectrum is used as efficiently as possible.

It is essential that governments and regulators successfully support the needs of 5G at international spectrum discussions, including WRC-19 and its preparatory meetings, because of the lengthy timeframes involved in making new mobile spectrum available.

Governments and regulators need to adopt national policy measures to encourage long-term heavy investments in 5G networks.

Resources:
GSMA Public Policy Position: 5G Spectrum
GSMA Network 2020 5G website
GSMA Report: Understanding 5G — Perspectives on future technological advancements in mobile

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 800MHz band for use in Europe, the Middle East and Africa, and the 700MHz band (698–806MHz) — 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 700MHz (this time 694-790MHz) for use in Europe, the Middle East and Africa. The second is 600MHz in parts of the Americas and Asia Pacific, such as Colombia, Mexico, the United States, Bangladesh and New Zealand.

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:

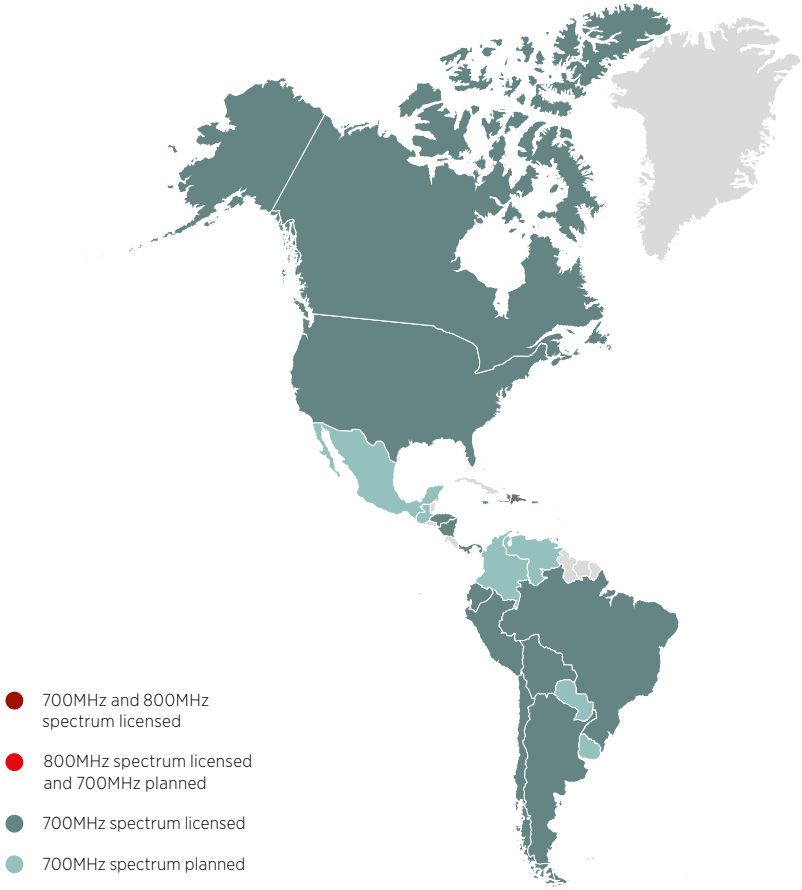
- Asia Pacific and Latin America should adopt the APT 700MHz band plan.
- Europe, the Middle East and Africa should adopt the ITU Region 1 700MHz band, which is compatible with APT 700MHz equipment.
- Every effort should be made to ensure the future implementation of the 600MHz band plan supports global harmonisation.

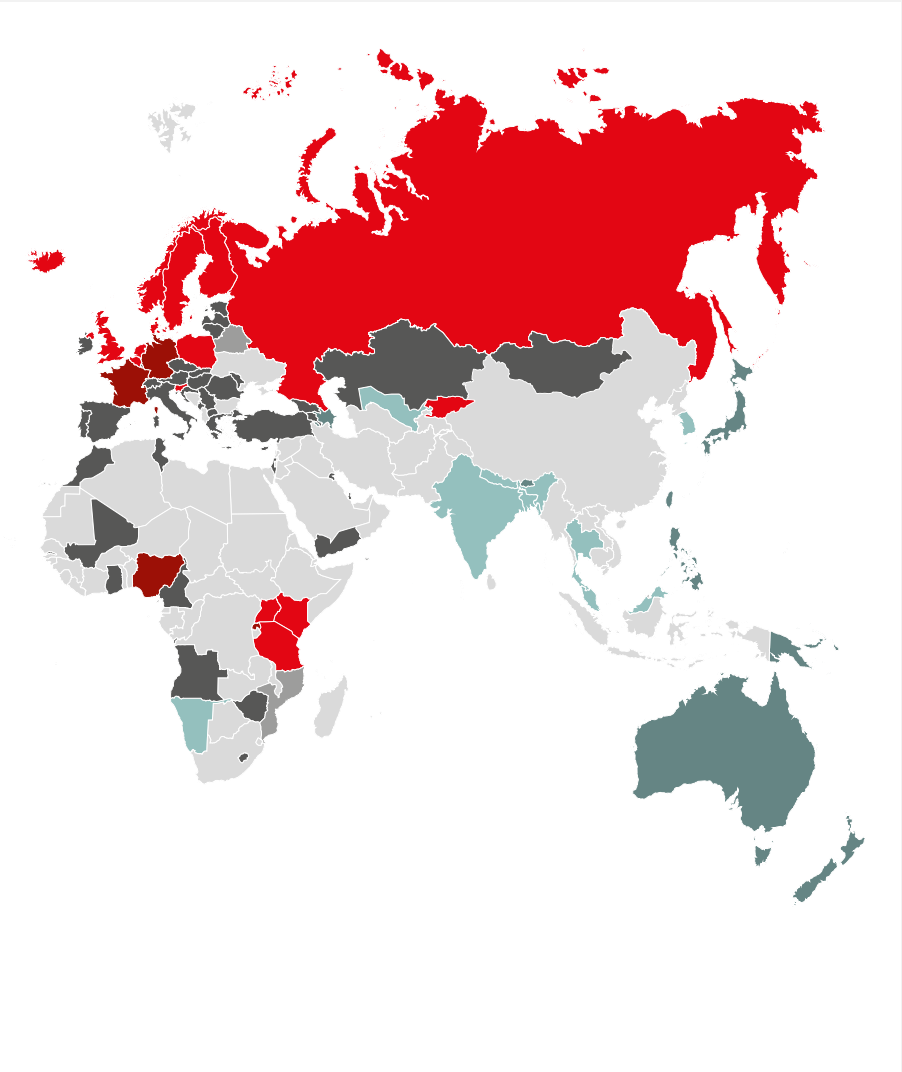
Resources:
GSMA Public Policy Position: Securing the Digital Dividend for Mobile Broadband
GSMA Public Policy Position: Recommended Band Plan for Digital Dividend 2 in ITU Region 1
GSMA Public Policy Position: Asia Pacific Digital Dividend/UHF band plans
GSMA & AHCIET Report: Economic Benefits of the 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 towards the allocation and ultimate licensing of Digital Dividend spectrum for mobile telecommunications.



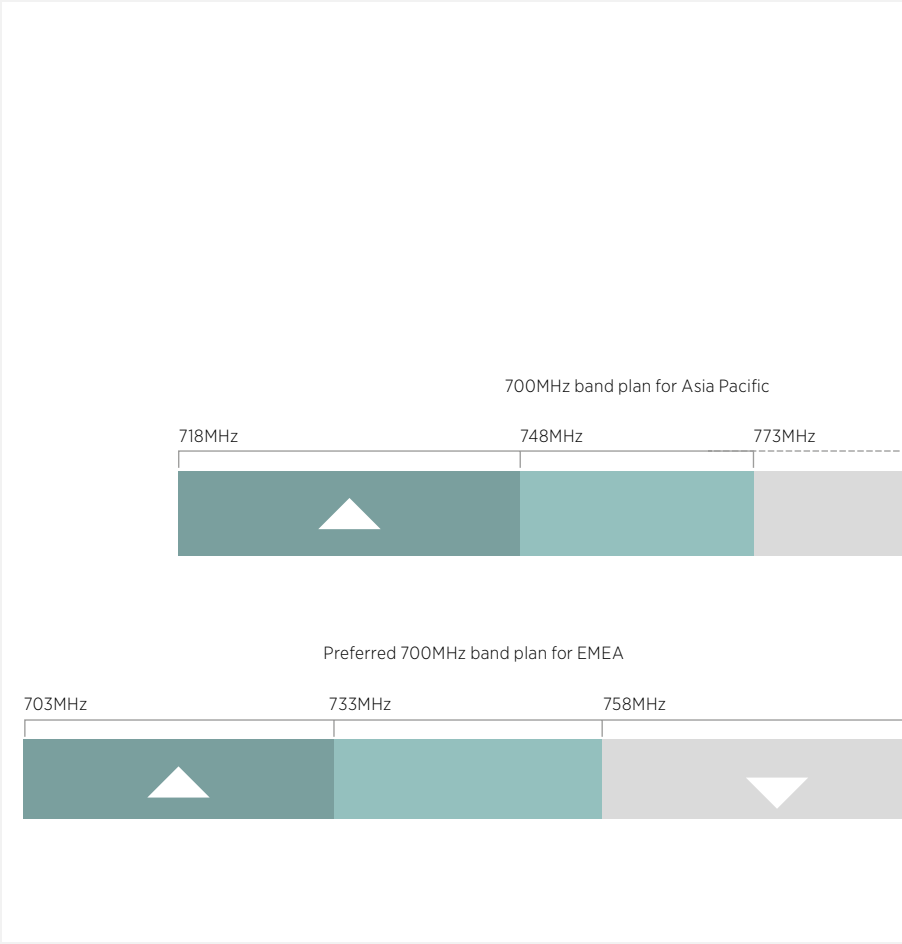


Source: GSMA Intelligence, November 2016

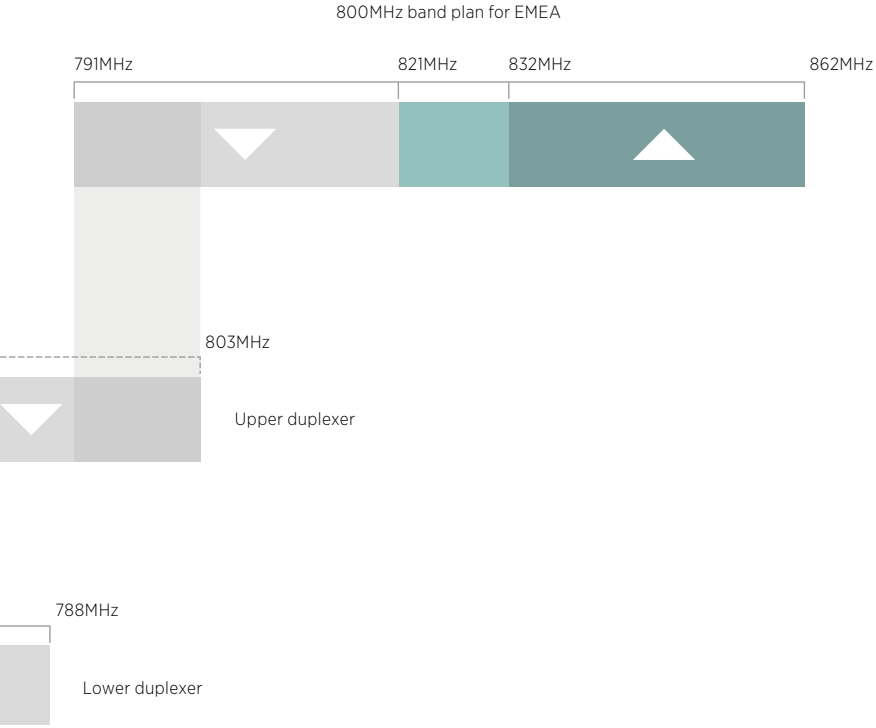
Deeper Dive

Band plans

Global harmonisation of GSM spectrum has been a critical factor in reducing handset costs as it allows device manufacturers to take advantage of economies of scale. This is one of the key reasons why countries should stick to the band plans developed for their respective regions.



The preferred 700MHz and 800MHz band plans for Europe, the Middle East and Africa (EMEA) have been developed to work alongside each other. However, the upper duplexer of the Asia Pacific 700MHz band plan clashes with the EMEA 800MHz band plan (see diagram below). To avoid interference between the two bands and to create a single regional market for devices that will help drive down the cost of handsets, Europe, the Middle East and Africa should adopt the preferred 700MHz band plan for Region 1.



Licensed Shared Access

Background

Licensed Shared Access (LSA) is a concept that allows spectrum that has been identified for international mobile telecommunications (IMT) to be used by more than one entity. Theoretically, this would increase the use of the radio spectrum by allowing shared access when and where the primary licensee, a non-mobile incumbent, is not using its designated frequencies.

LSA complements other authorised ways to access spectrum, including licensed (exclusive) and licence-exempt (unlicensed) use of the spectrum.

Provided that a commercial agreement and an adequate regulatory framework are in place, LSA could allow a portion of assigned spectrum to be used by an LSA user (such as a mobile operator).

As global demand for spectrum intensifies, regulatory strategies such as these are attracting considerable interest and investigation.

Debate

Can operators rely on the LSA concept to share spectrum with the incumbent users?

How can the regulatory/competition issues be addressed with the use of LSA (e.g., to safeguard against one operator getting access to the full LSA spectrum)?

How can LSA be applied effectively, without undermining the urgency of clearing mobile bands for exclusive access?

While we agree that sharing paradigms should be explored as another option for spectrum management, sharing technologies have long promised but remain largely unproven.

— Joan Marsh, Senior Vice President of Federal Regulatory, AT&T

Industry Position

The LSA concept could give mobile network operators access to additional spectrum for mobile broadband, but exclusive access through market-based licensing should remain the main regulatory approach.

LSA does not replace the urgent need to secure additional, exclusive and harmonised spectrum for mobile broadband, and this continues to be the primary objective at the regional and international level.

Authorisation to access additional spectrum using LSA should be granted by national regulatory authorities after public consultation and commercial agreement between the incumbent spectrum user and mobile network operators.

Resources:
GSMA & Deloitte Report: The Impact of Licensed Shared Use of Spectrum
GSMA Public Policy Position: Licensed Shared Access (LSA) and Authorised Shared Access (ASA)
Qualcomm 1000x Data Challenge website
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. As mobile technologies have proliferated, the demand for access to radio spectrum has intensified, leading to considerable debate and advocacy for new approaches to spectrum management.

Licence-exempt spectrum:

Frequency bands that 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.

Shared licensed spectrum:

Any licensed spectrum that is shared among licensed users. This sharing may be agreed on a commercial basis between licensed entities or as a condition of the licensing process.

TV white space:

Television spectrum in the UHF band that, due to predictable geographical or temporal gaps in broadcasting, offers the potential for licence-exempt devices to use the spectrum for broadband services. These services are dependent on dynamic spectrum management technologies and techniques.

Licensed shared access (or authorised shared access):

A proposed sharing scheme that allows licensed use of underutilised spectrum that is already licensed by another service. Licensed shared access (LSA) is proposed as a way to ensure a high quality of service is delivered, as opposed to best-endeavour services that are delivered through licence-exempt spectrum.

While these innovations may find a viable niche in the future, the GSMA's position is that pursuit of these options today risks deflecting attention from the release of sufficient, exclusively licensed spectrum for mobile broadband.

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 than in the past, although they can be more costly due to 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?

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

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.

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 800MHz 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 800MHz 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 800MHz 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 800MHz 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 800MHz 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 800MHz band.

The four mobile operators are shareholders, and each had to contribute £30 million per 5MHz 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.

As of June 2016, at800 had achieved a 99 per cent or 100 per cent pass rate against all KPIs for its twelfth consecutive month. All 545 confirmed 4G interference cases in June 2016 were resolved within the ten working day target, as they had predominately been every month in the previous year. For viewers experiencing disruption that is not related to LTE at 800MHz, 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.

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, which may include achieving:

- 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?

What are the main considerations for auction design, to achieve the government's desired outcomes?

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 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.

Resources:
GSMA & CEG Report: Licensing to Support the Broadband Revolution
GSMA Public Policy Position: Spectrum Auctions
GSMA Managing Spectrum website

Case Study

Reserve Pricing for Spectrum Auctions

Reserve prices play an important role in spectrum-auction design. They discourage non-serious bidders and can also ensure that a minimum price is paid for spectrum licences when competition for the spectrum is weak. When competition for access to mobile spectrum is anticipated to be strong, however, it does not follow that high reserve prices should be set. In fact, it risks alienating potential bidders and could lead to auction failure, leaving valuable spectrum unsold and unused.

High reserve prices are a growing concern. A study[1] found that in the majority of recent auctions (51 per cent) over the past 10 years, the gap between the final price paid and the reserve price is negligible, suggesting the government rather than the market determined the outcome. If operators pay more for spectrum than its competitive market value, there is a risk that this will lead to lower network investment, reduced quality of service, and higher consumer prices.

Rather than focusing on revenue maximisation, governments would be wiser to focus on the positive social and economic outcomes generated by the use of widespread mobile services, while facilitating an appropriate level of industry competition. Lower, realistic reserve prices for spectrum auctions allow the market to determine the appropriate market value of the spectrum being released.

[1] Plum Consulting, Reserve Prices in Spectrum Auctions: Why Size Matters (2016)

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 700MHz, 800MHz, 900MHz, 1800MHz, 2100MHz, 2300MHz and 2500MHz bands, they were not forced to compete as fiercely. Nevertheless, the TRAI set the reserve price for 700MHz, in particular, at an extremely high level, having based it on 1800MHz prices achieved in the hotly contested 2015 auction (700MHz price being four times 1800MHz). 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 700MHz band and bids for 850MHz, 2100MHz and 2500MHz spectrum were also very limited, with many blocks in several circles unsold. The entire 2300MHz spectrum was sold and 80 per cent of 1800MHz spectrum that was put up for auction was also sold.

Poland: An outlier in GDP-versus-spectrum cost

Poland's spectrum auction ran from February to October 2015 and included more than 400 rounds of bidding. Whereas in most European countries there is a clear correlation between GDP purchasing power parity (PPP) and the cost of 800MHz spectrum, Poland is an outlier. In total, the auction raised PLN9.23 billion ($2.5 billion), six times the initial target set by the Office of Electronic Communications (UKE). The spectrum in Poland cost significantly more than in the far more prosperous Germany, but the Polish operators had little choice. Compared to their European counterparts, they had relatively little spectrum and network capacity, yet were seeing strong demand for 4G services in a country where there are only 11 fixed-line subscriptions for every 100 people. The very high prices that Poland's mobile operators had to pay will reduce the funds they have available for expanding their 4G networks and extending broadband to the many Polish homes and offices that lack a fixed line.

Thailand: Expensive rationed spectrum hampers investment

In 2015, Thailand auctioned 1800MHz spectrum in November, followed by 900MHz spectrum in December. The winning bids in the December auction were almost six times the reserve price for the 900MHz spectrum and more than double the final proceedings for the 1800MHz spectrum auction. In total, the auction of just 100MHz 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."

Spectrum Caps

Background

Spectrum caps are limits to how much spectrum can be licensed to any mobile operator. Spectrum caps are increasingly used by regulators in auction rules to encourage spectrum reallocation and to balance operators' portfolios.

The intention is to ensure effective competition and to prevent existing operators from using their economic strength to secure the use of large spectrum assets, which could give them a competitive advantage in the future.

The use of spectrum caps could be considered a 'remedy' under competition policy. This means that spectrum caps should only be imposed if a market assessment leads to two conclusions: first, that competition is ineffective in the market, and second, that the appropriate and proportionate remedy for the market failure identified is the adoption of spectrum caps.

More targeted and proportionate remedies may include options related to network access for Mobile Virtual Network Operators, the introduction of quality of service obligations, approaches that make it easier for consumers to switch operators, or steps to incentivise infrastructure sharing.

New entrants and players with less spectrum typically support caps on new spectrum allocations, while incumbents argue that the approach negatively impacts the quality of service they can deliver to consumers.

Debate

Does the use of caps in spectrum allocation result in the best social and economic outcomes?

What are the issues that might require the use of spectrum caps?

If market failures have been identified, would spectrum caps really be an appropriate way to address these market failures?

Industry Position

In markets where competition is ineffective, the use of spectrum caps may be appropriate, but care must be taken to avoid unintended consequences and poor outcomes for consumers.

Operators should not be penalised for using their spectrum assets successfully or constrained in delivering new services. Operators with the largest market share are usually the ones that need more spectrum to meet customer demand.

If imposed, spectrum caps should allow all operators to deploy networks in a technically and economically efficient manner.

Auction and licensing rules must give operators the opportunity to secure a portfolio of spectrum to deliver economically viable broadband services.

Using spectrum caps specifically to attract new market entrants can lead to spectrum

fragmentation and market inefficiencies which, ultimately, will negatively affect consumers and businesses using mobile services. Licence conditions for network deployment and spectrum use may lead to more effective outcomes for consumers.

Before applying spectrum caps, regulators should conduct a rigorous market analysis to ensure there are, in fact, other operators in the market whose access to spectrum would deliver greater societal benefits.

Summary of potential remedies to address possible market failures and their associated regulatory risks		
Market failure	Possible remedy	Regulatory risk
Significant market power – larger operators may obtain the majority of spectrum.	Spectrum caps.	Setting appropriately sized caps is difficult. Setting caps too low could potentially distort the market. The larger operators may be both the highest-value users and the users with the best incentive to maximise use.
	Obligations relating to coverage or network sharing.	If obligations have a material impact on operators' returns, they could negatively affect investment.
Smaller operators do not have enough spectrum to be credible.	Spectrum set-aside. Spectrum floors.	Setting spectrum reserves is dificult. Reserving too much spectrum could distort the market. The smaller operators may not be the highest value bidders and may be unable to maximise spectrum use. Could choose the wrong spectrum to reserve. Set aside could be restrictive if different types of smaller operators have different spectrum requirements.
	Bidder credits.	Setting the credit at the correct amount requires detailed data. If it's too low, smaller operators or new entrants may not obtain any spectrum. If it's too high, then the outcome is effectively pre-determined.

Resources:
GSMA & CEG Report: Licensing to Support the Broadband Revolution
Arthur D. Little Report: Mobile Broadband, Competition and Spectrum Caps
Article: Forbes.com, 'Sending the Wrong Signals to the Wireless Marketplace'

Deeper Dive

Using Spectrum Caps to encourage new entrants

Once a government or regulator decides to encourage a new entrant into the market, different models are usually employed to ensure access to spectrum and the facilitation of entry conditions. These models may include different network deployment and coverage requirements for the new entrant, obligations imposed on incumbents or established operators to provide facilities sharing, the use of spectrum that has been set aside for the new entrant and the use of spectrum caps.

Spectrum caps were first introduced in the 1990s, particularly in Latin America, to foster competition in mobile markets. The spectrum caps previously imposed in many countries have been modified or even removed as the growing demand for mobile data services triggered the allocation of additional spectrum in new frequency bands. However, tight spectrum caps are still in place in Latin America and are used extensively as a way to manage competition. These range from 40MHz to 80MHz, and many operators have already reached this ceiling.

In Europe, spectrum caps are not used as an absolute limit on the amount of spectrum an operator can hold. However, band-specific bidding caps have been used, as have specific caps for particular spectrum awards. For instance, in the Austrian multi-band auction in October 2013, participants were not allowed to win more than 2x35MHz of spectrum in bands below 1GHz, 2x20MHz in the 800MHz band and 2x30MHz in the 900MHz band, while the total spectrum that any one operator could win within the auction was set at 2x70MHz.

In the United States, the FCC has long considered spectrum concentration in its competitive review of proposed transactions that involve spectrum holdings. In 2004, the FCC decided to move away from spectrum caps to a spectrum screen process, whereby competitive objectives are examined on a case-by-case assessment of spectrum aggregation. This approach triggers an additional review when a spectrum threshold is passed, based on the total amount of spectrum available and the number of existing operators in a market. As a general rule, this limits the amount of spectrum an operator can hold to a third of the spectrum available in the market, ensuring at least three operators.

In addition, spectrum is often set aside when new frequencies are made available, to ensure new market entrants have access to spectrum during assignment processes. For instance, in the 2013 Austrian auction, the Telekom Control Commission (TKK) set aside 2x10MHz of spectrum in the 800MHz band for a new entrant. Similarly, in the Mexican AWS auction in 2010, a national block of 2x15MHz was set aside by COFETEL.

In some cases, reserving spectrum for new entrants has led to an inefficient use of spectrum. For instance, Chile enforced tight caps in the 2009 AWS beauty contest, making spectrum available only to the two new entrants, and effectively excluding the three incumbents from participating in the auction. Unfortunately, the two new entrants only reached a limited market share of connections. One of the new players became an MVNO and the other was recently sold.

Colombia did the same during the sale of the 2.5GHz band in 2010, allowing one new entrant to become the unique 4G-LTE provider in the country. The new entrant enjoyed a 'first-mover advantage' of more than three years, as its competitors didn't launch 4G services until 2013, following the AWS spectrum auction. Despite gaining this competitive edge in 2010, the new entrant needed two years to launch commercial 4G mobile services in 2012, eventually merging with an incumbent player in 2014.

Regulators must be wary of the conditions under which new entrants can thrive before allocating valuable spectrum. Reserving spectrum for new entrants may not create effective competition or sustainable market players, leading to an inefficient use of the resource. This is particularly important in the context of future 4G-suitable spectrum assignments, since 4G services require wider bandwidth. New entrants that do not have the ability to heavily invest in infrastructure to deploy and maintain their networks will hardly manage to compete against established players.

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.

The total number of machine-to-machine (M2M) connections is predicted to grow from five billion in 2014 to 27 billion in 2021.[1] This leap in connectivity is expected to be worth $4 trillion by 2025, up from $892 billion in 2015.[2]

The bulk of the M2M market (72 per cent[3]) uses short-range, unlicensed connections (e.g., Wi-Fi and ZigBee), while the wide-area market is heavily reliant on mobile connectivity. Mobile M2M connections are expected to grow from 256 million at the end of 2014 to 2.2 billion by 2024.[1]

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.

1 Machina Research, M2M Global Forecast & Analysis Report 2014-24 (June 2015)

2 Machina Research, Forecasting the totality of the IoT revenue opportunity (April 2016)

3 GSMA, Public Policy Position: Spectrum for the Internet of Things (September 2016)

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 which 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 Connected Living Programme 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 one's mobile device abroad.
- Fewer issues of cross-border interference.

There are a limited number of bands that can be supported in a mobile device. Each new band supported increases the device cost, reduces the receiver's sensitivity and drains the battery.

Harmonised bands have enabled huge economies of scale, leading to unprecedented use of mobile telecommunications worldwide. Spectrum bands for international mobile telecommunications (IMT) are defined through a rigorous multilateral process that considers their technical and practical merits.

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

The global harmonisation of the 694–790MHz frequency band that has been decided by WRC-15 paves the way for manufacturers and mobile operators to offer mobile broadband at an affordable price in currently underserved areas.

— François Rancy, Director, ITU Radiocommunication Bureau

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.

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

Spectrum Licensing

Background

Spectrum licensing is a powerful lever that national regulatory authorities can use to influence the competitive structure and behaviour of the mobile telecoms sector.

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

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.

Licence fees should be used to help recover the administrative costs of freeing up spectrum for new, higher-value uses, and licensing and managing the spectrum for long-term social and economic benefit. They should not be used to maximise government revenue.

Resources:
GSMA & CEG Report: Licensing to Support the Mobile Broadband Revolution
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 and affect mobile services for, potentially, 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 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?

We know that the choice of the wrong standard can lock our economies into long periods of economic underperformance, while market-led solutions have consistently provided a much better environment for technology selection.

— European Commissioner Viviane Reding, 4 December 2006

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 1800MHz 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 1800MHz 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.

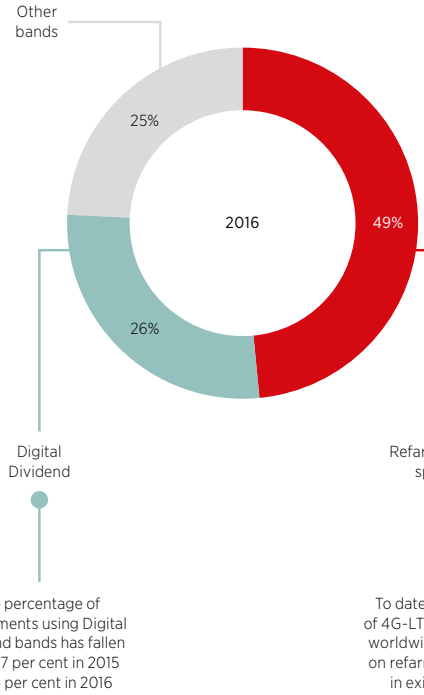
In countries where regulators support technology neutral spectrum licences, operators have been able to refarm the 1800MHz band for LTE services. The 1800MHz band is now the most widely deployed LTE band globally, as well as the most widely supported in mobile devices. According to the Global Mobile Suppliers Association (GSA), the 1800MHz band has the largest device ecosystem of any LTE band, with over 3,889 compatible user devices available as of October 2016.

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

535 operators worldwide now have live LTE networks, covering 170 countries. As many operators use multiple spectrum bands in their LTE networks, this equates to more than 780 individual deployments.



Breakdown of bands	MHz
Digital Dividend	700, 800
Reframed 2G/3G	850, 900, 1500, 1700/2100, 1800, 1900/2100, 2100
Other bands	2300, 2500, 2600, 3500, 3600

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 – 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 (470–790MHz in Europe and 470–698MHz 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 areas, 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 under-utilised government spectrum where feasible.

— Joan Marsh, Senior Vice President of Federal Regulatory, AT&T

Industry Position

TVWS networks make opportunistic use of white spaces to provide generally small-scale services on a secondary and unlicensed basis. That means they 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., 800MHz, 700MHz and increasingly in the future the 600MHz 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 Europe response to Radio Spectrum Policy Group 2010 Work Programme
AT&T Public Policy Blog: The Power of Licensed Spectrum

Consumer Protection

Mobile brings an array of benefits and opportunities to the 4.7 billion people around the world who are now connected. However, it also creates new challenges in how to keep those people safe and secure when using voice and data services, while also ensuring they 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 the potential risks associated with connectivity 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 work with governments, multilateral organisations and non-governmental organisations to address concerns related to consumer protection by:

- Defining and promoting global best practice.
- Building and participating in cross-sector coalitions.
- Leading technical initiatives.
- 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 are appropriately protected and informed as they enjoy the full range of benefits that mobile technology makes possible.

Children and Mobile Technology

Background

Young children and teenagers are enthusiastic users of mobile technology. The report Children's Use of Mobile Phones — An International Comparison 2015 reveals that 67 per cent of children aged 8-18 in the countries surveyed use a mobile phone, and 85 per cent of those children use their mobile phone to access the internet. Young people's knowledge of mobile applications and platforms often surpasses that of parents, guardians and teachers, and the international comparison report confirmed that children 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 and 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 and a safe, secure environment to benefit from mobile technologies.

The mobile industry has taken active steps in the area of child online protection. The GSMA has played a leading role in self-regulatory initiatives dealing with issues such as parental controls, education and awareness.

Debate

What potential harms are children exposed to in the online environment?

To what extent can technology protect young people from online threats, and what role does consumer awareness and education play?

We are grateful for the leadership shown by the GSMA Mobile Alliance members in tackling online child sexual abuse material. Their coordinated action helps set the standard and illustrates how proactive steps taken by industry can help protect children's rights in today's digital society.

— Eija Hietavuo, CSR Manager, UNICEF

Is industry doing enough to protect children when they are online, and what is the role of parents and teachers?

Should governments require mobile operators, through regulation, to take steps to protect children from online risks?

Are concerns about online risks preventing mobile learning and education opportunities from being fully realised?

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 child online protection is best approached through multi-stakeholder efforts. The GSMA takes part in international initiatives related to child online protection, including contributing to the ITU's Child Online Protection programme, and actively engages with governments and regulators looking to address this issue.

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), INHOPE and INTERPOL, hold national and regional multi-stakeholder workshops on the issue. These workshops bring together policy makers, 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. Furthermore, the GSMA leads several initiatives to promote the safe use of mobile services for young people, provides useful research on child online safety, and gathers evidence about how young people use their mobile devices in different parts of the world.

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.

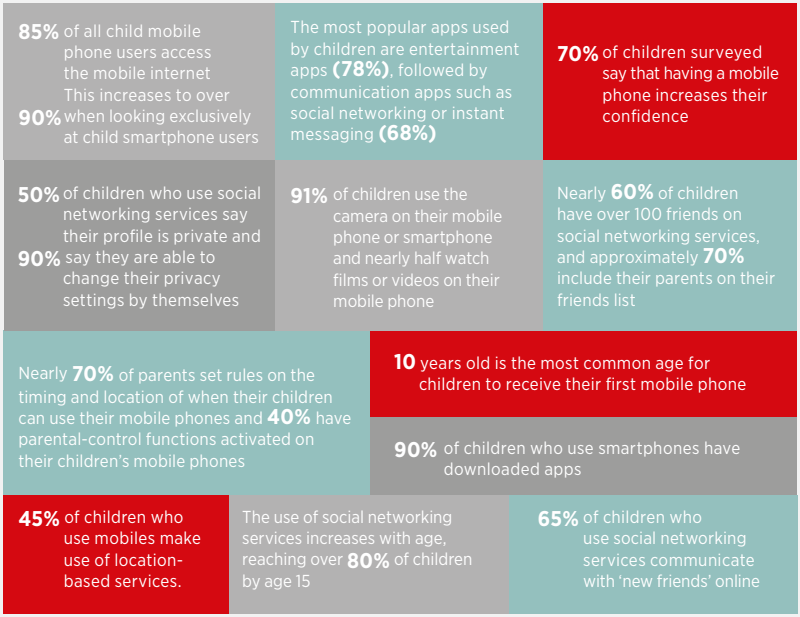
Resources:
UNICEF Guidelines for Industry on Child Online Protection website
UNICEF Tools for companies in the ICT sector website
ICT Coalition website
GSMA mYouth website
GSMA Report: Children's Use of Mobile Phones, An International Comparison 2015
GSMA Report: Children's Use of Mobile Phones, A Special Report 2014

Facts and Figures

Children's Use of Mobile Phones in Algeria, Egypt, Iraq and Saudi Arabia

Since 2008, the GSMA has been collaborating with NTT DOCOMO's Mobile Society Research Institute on a multiyear project to better understand how children aged eight to 18 use mobile phones around the world.

The research is comparative, typically covering four or five different countries. Some standard questions, posed to children and their parents since the beginning of the programme, enable broad year-on-year comparisons on areas such as age of first mobile ownership and the reasons for getting a phone, as well as parents' concerns about their children's use of mobile. New questions are added to account for the evolution of children's mobile lives — more recent research, for example, has asked children about accessing social media services from mobiles and how they manage their privacy settings. Countries taking part in the research are able to develop a targeted understanding of the real mobile habits of younger users and can therefore develop strategies for promoting safe and responsible use of mobile from a firmer foundation.



Source: GSMA and NTT DOCOMO

About the ICT Coalition

The ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU (www.ictcoalition.eu) is made up of 23 companies from across the information and communication technology (ICT) sector. Members of the ICT Coalition pledge to encourage the safe and responsible use of online services and internet devices among children and young people and to empower parents and carers to engage with and help protect their children in the digital world.

The principles are suitably high-level, enabling their application to evolve as technology and consumer propositions evolve, and to facilitate their adoption by a variety of companies and services. The ICT Coalition's members include leading internet and online service providers such as Google and Facebook, device manufacturers, and mobile operators including Deutsche Telekom, KPN, Orange, Portugal Telecom, TDC, Telecom Italia, Telefónica, Telenor, TeliaSonera and Vodafone.

Members of the ICT Coalition are required to specify how their organisation will deliver on six principles related to online content, parental controls, dealing with abuse and misuse, child abuse and illegal contact, privacy and control, and education and awareness.

Electromagnetic Fields and Device Safety

Background

According to the World Health Organization (WHO), there are no established health risks from the radio signals of mobile devices that comply with international safety recommendations.

However, research has shown a possible increased risk of brain tumours among long-term users of mobile phones. As a result, in May 2011, radio signals were classified as a possible human carcinogen by the International Agency for Research on Cancer. 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.

Mobile phone compliance is based on an assessment of the specific absorption rate (SAR), which is the amount of radio frequency (RF) energy absorbed by the body.

Mobile phones use adaptive power control to transmit at the minimum power required for call quality. When coverage is good, the RF output level may be similar to that of a home cordless phone.

Some parents are concerned about whether mobile phone use or the proximity of base stations to schools, day-care centres or homes could pose a risk to children. National authorities in some countries have recommended precautionary restrictions on phone use by younger children, while others, such as the US Food and Drug Administration (FDA), have concluded that current scientific evidence does not justify measures beyond international safety guidelines.

A comprehensive health risk assessment of radio signals, including those of mobile phones, is being conducted by the WHO. The conclusions are expected in 2017.

Debate

Is there a scientific justification for mobile phone users to limit their exposure?

Do radio signals from mobile phones present a risk to children?

Where can people turn to find the latest research and recommendations?

Industry Position

Governments should adopt the international limit for SAR recommended by the WHO and require compliance declarations from device makers based on international technical standards.

We encourage governments to provide information and voluntary practical guidance to consumers and parents, based on the position of the WHO.

The GSMA believes parents should have access to accurate information so they can make up their own mind about when and if their children should use wireless technologies.

Concerned individuals can choose to limit their exposure by making shorter calls, using text messaging or using hands-free devices that can be kept away from the head and body. Bluetooth earpieces use very low radio power and reduce exposure.

The SAR is determined by the highest certified power level in laboratory conditions. However, the actual SAR level of the phone during use can be well below this value. Differing SAR values do not mean differing levels of safety.

Resources:
World Health Organization International EMF Project website
International Agency for Research on Cancer Monograph on Radiofrequency Fields website
GSMA Mobile and Health — independent expert review website
Mobile Manufacturers 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

RF research is continuing in a number of areas, but data currently available provides no clear or persuasive evidence of any other effects. For this reason, the Committee and the Ministry of Health continue to support the use of exposure limits for RF fields set in the current New Zealand Standard, which is based on guidelines published by an international scientific body recognised by the WHO for its independence and expertise in this area. Those guidelines were first published in 1998 and endorsed, following a review of more recent research, in 2009.

— Ministry of Health (New Zealand), 2015

Altogether it provides no or at most little indications for a risk for up to approximately 15 years of mobile phone use. No empirical data are available for longer use; however, cancer rates in Sweden and other countries do not show any increase that might be attributed to the massive mobile phone use that started in the beginning of this century. There are no indications from the few studies with cultured cells, that RF fields are capable of initiating a tumour. Many animal studies have been performed using a large spectrum of tumour types and long term, often lifelong, exposure. With very few exceptions, no effect of RF exposure on tumour growth and development has been found.

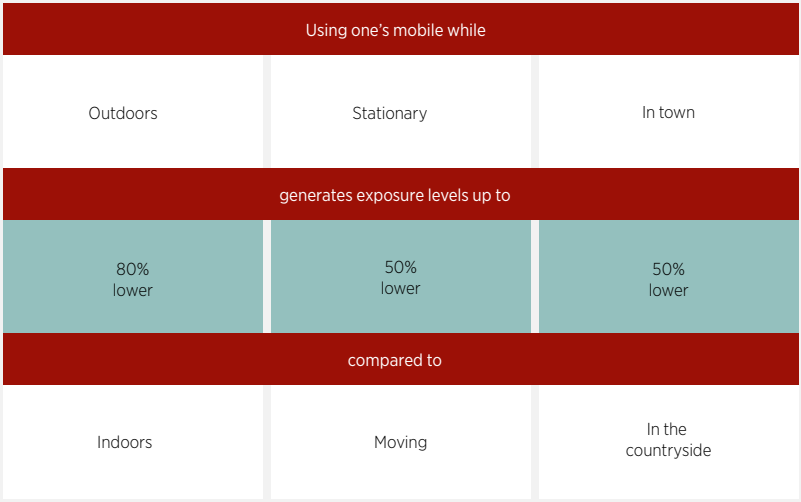
— Swedish Radiation Safety Authority, 2016

The Committee considers it unlikely that exposure to radiofrequency fields, which is associated with the use of mobile telephones, causes cancer. The animal data indicates a possibility of a promoting effect, but it is not clear whether this could explain the increased risk for tumours in the brain, head and neck that has been observed in some epidemiological studies. The Committee feels it more likely that a combination of bias, confounding and chance might be an explanation for the epidemiological observations.

— Health Council of the Netherlands, 2016

Personal Control Over Exposure

Mobile phone users who remain concerned about the possible risks of EMF can make small changes to reduce their exposure significantly. Mobile phones increase their transmission power when the signal is weak, when they are in motion and when they are in rural areas. To decrease exposure, callers may choose to use their mobile phone more when they are outside, in one spot and in urban areas.



Source: GSMA

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, including reduction factors that provide protection against all established health risks.

The World Health Organization (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 WHO reviews on going research and provides recommendations for research to support health-risk assessments.

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.

The 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).

The WHO is currently conducting a risk assessment for radio frequency signals. The results are expected in 2017, including policy recommendations for governments.

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?

What EMF exposure limits should be specified for base stations?

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.

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.

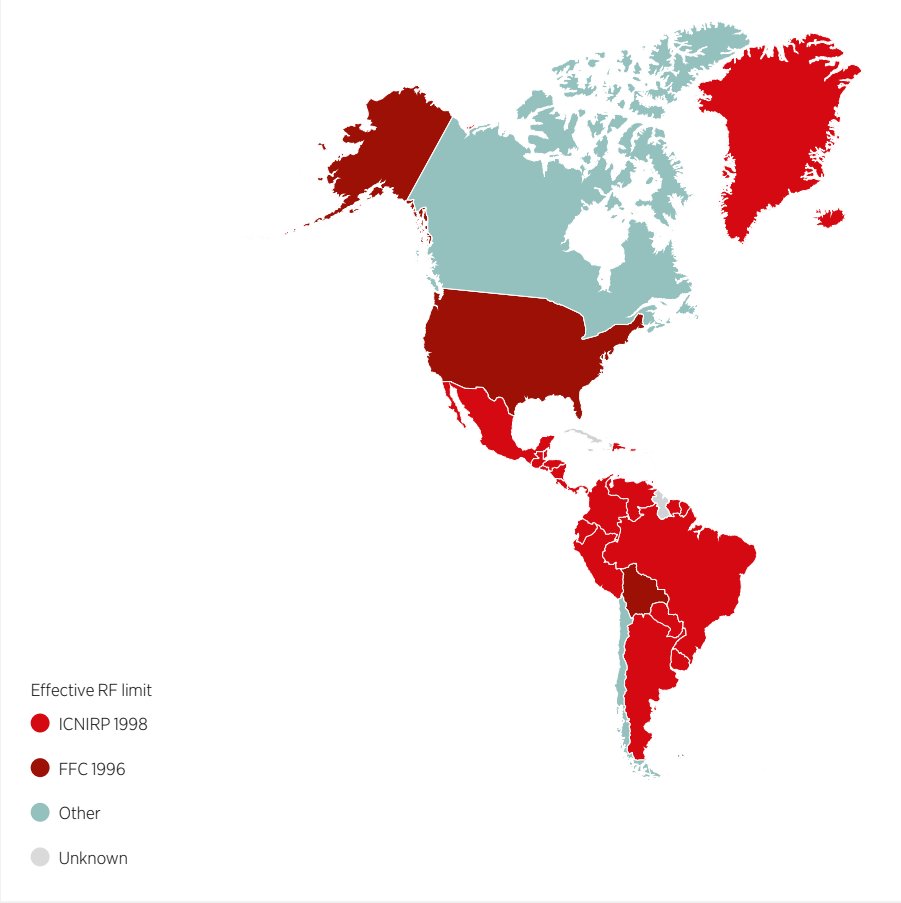
Resources:
WHO International EMF Project website
GSMA Report: Arbitrary Radio Frequency Exposure Limits — Impact on 4G Network Deployment
GSMA Report: LTE Technology and Health
ITU-T activities on human exposure to EMF website
ITU EMF Guide website

Deeper Dive

A Global Look at Mobile Network Exposure Limits

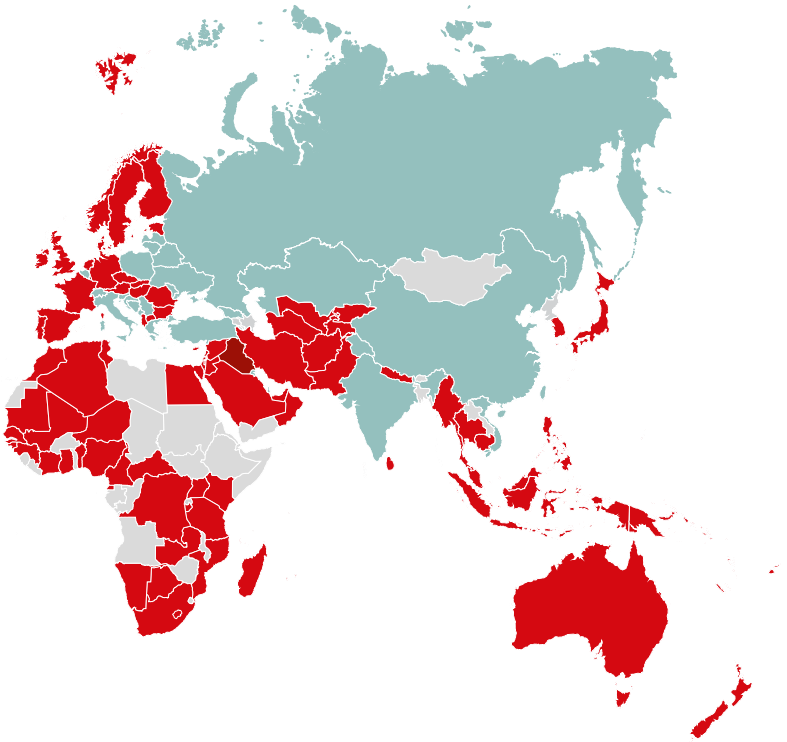
The World Health Organization (WHO) endorses the guidelines of the International Commission for Non-Ionizing Radiation Protection (ICNIRP) and encourages countries to adopt them. While many countries have adopted this recommendation, some have adopted other limits or additional measures regarding the 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, 124 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.

As part of the ICT sector, mobile operators generate e-waste during periods of technological renewal and also through the normal supply of products to customers (such as routers, mobile phones and tablets).

Mobile operators around the world have developed WEEE management programmes both as compliance measures to conform to current legislation, and also due to their desire to meet their own sustainability and corporate social responsibility goals.

However, in some regions, such as Latin American, there is a lack of 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 (due to 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 should be created by relevant environmental authorities and developed into legal frameworks for e-waste management that recognise the principle of EPR.

- 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

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) services, video or instant messaging services.

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 law-enforcement and security agencies can protect citizens, and the rights of 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 of communications providers 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

Case Study

National Regulatory Approaches to Government Access

Increasingly, as witnessed in the UK, France, Germany and Australia, laws are being proposed that would require service providers to capture and retain communications data and grant the government systematic access to this information.

In the UK, communications service providers are required to separately retain a range of account and communications data and must ensure the data can be disclosed in a timely manner to UK law enforcement agencies, the security services and a number of prescribed public authorities under the UK Regulation of Investigatory Powers Act (RIPA). Prescribed authorities can also seek a warrant from the Secretary of State to intercept communications.

The two main objectives of RIPA are to regulate the investigatory powers of the state and to set the legitimate expectations for citizens' privacy. As RIPA is subject to oversight by the Surveillance Commissioner and the Interception Commissioner, citizens can seek redress for alleged unlawful access to their data or communications, and service providers operating in the UK can raise concerns about the validity of requests.

In April 2014 the European Court of Justice ruled that the EU Data Retention Directive is 'invalid' as it violated two basic rights — respect for private life and protection of personal data. The European Commission has emphasised that the decision of whether or not to introduce national data-retention laws is a national decision and consequently, the UK and a number of other countries in the European Union are reviewing their data-retention laws, which required communications service providers to store communications data for up to two years.

Meanwhile, in May 2015, the German government outlined plans for a new data-retention law which would require telecoms companies to retain 'traffic data' relevant to communications and hand them over (under certain conditions) to Germany's law enforcement and security agencies. Germany's privacy campaigners questioned whether the plans were constitutional adding that, in their opinion, the German government had not sufficiently outlined why the retention of the data is necessary.

In July 2015, the French Parliament approved a bill that allows intelligence agencies to tap phones and emails without seeking permission from a judge. The new law requires communications providers and internet service providers to hand over customers' data upon request, if the relevant customers are linked to a 'terrorist' inquiry. Protesters from civil liberties groups claimed the bill would legalise intrusive surveillance methods without guarantees for individual freedom and privacy.

Australia's new Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 requires telecommunication service providers to retain for two years certain telecommunications metadata prescribed by regulations. This two-year retention period equals the maximum allowed under the EU's earlier Data Retention Directive which the EU's Court of Justice ruled as invalid.

Trending Towards Transparency

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 reports showing the types and/or volume of requests from governments for user information. Typically, these 'transparency reports' include how many of these requests resulted in the disclosure of customer information. These reports reveal not only the frequency of such requests, but some detail about the kind of information accessed — customer account information; metadata, which can reveal an individual's location, interests or relationships; and the interception of communications. Although mobile operators often have no option but to comply with such requests, they are increasingly pressing for greater transparency about the nature and scale of government access.

At a time of growing public awareness and debate over government surveillance and privacy in many countries, this trend towards reporting the demands of governments for communications data (where it is legal to do so) has revealed the degree to which government intelligence and law enforcement agencies rely on such information.

The political debate is heated on both sides — those who argue that law-enforcement agencies require broad access in order to fight crime, and those who rail against perceived overzealous snooping and strive to maintain citizens' right to privacy in the digital age.

Like the internet content providers, 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. Transparency reporting brings valid information to the public and policymakers, raising key questions about the balance between government access and privacy.

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 take-down' 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 take-down processes and reporting mechanisms to keep their services free of this content.

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?

INTERPOL is pleased to support the Mobile Alliance Against Child Sexual Abuse Content which sends a clear message from its members — that there is zero tolerance of child exploitation on their network. Alliances such as this, and its willingness to work with other stakeholders and society in general, are hugely important and will serve as an example of best practice.

— Mick Moran, Assistant Director Human Trafficking and Child Exploitation. INTERPOL

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

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.

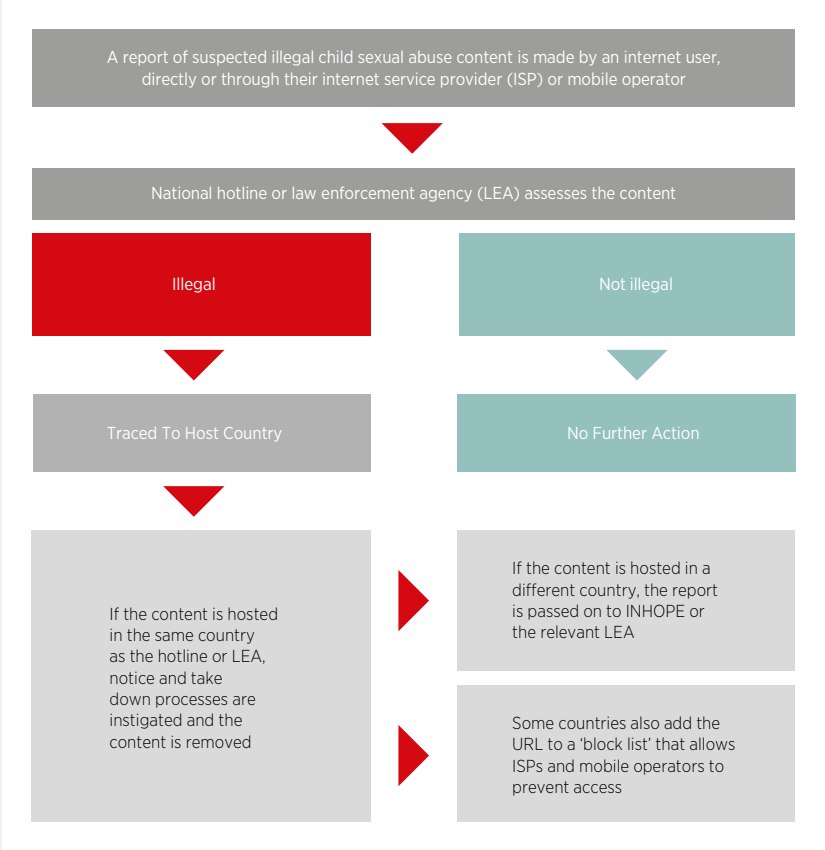
Alliance members have made the commitment to:

- Implement technical mechanisms to restrict access to 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, co-operation 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. It also collaborates with the European Financial Coalition and the Financial Coalition Against Child Pornography.

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 also is concerned with technical issues related to network management and standards, for example, 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 the inputs of 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?

Global internet governance must be transparent and inclusive, ensuring full participation of governments, civil society, private sector and international organisations, so that the potential of the Internet as a powerful tool for economic and social development can be fulfilled.

— Joint press release from the governments of the USA and Brazil, June 2015

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) and the Internet Architecture Board (IAB) and other fora.

Economic and transactional issues such as internet interconnection charges are best left to commercial negotiation, consistent with commercial law and regulatory regimes.

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

Mandatory Registration of Prepaid SIMs

Background

In many 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.

A number of governments, however, have mandated prepaid SIM registration as part of efforts to mitigate security concerns and address criminal and anti-social behaviour. To date, there has been no empirical evidence that mandatory SIM registration directly leads to a reduction in crime.

Some governments, including the United Kingdom and the Czech Republic, have decided against mandating registration of prepaid SIM users, concluding that the potential loopholes and implementation challenges outweigh the merits.

Nevertheless, SIM registration can allow many consumers to access value-added mobile and digital services that would otherwise be unavailable to them as unregistered users (such as mobile money and e-government services).

For SIM registration to lead to positive outcomes for consumers, it must be implemented in a pragmatic way that includes taking into account local market circumstances, such as the ability of mobile operators to verify customers' identity documents. Conversely, if the registration requirements are disproportionate to the specific market, mandating the policy may lead to implementation challenges and unforeseen consequences. For example, it could unintentionally exclude vulnerable and socially disadvantaged consumers who lack the required identity documents, or may 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 has the potential to offer valuable benefits to citizens, governments should not mandate it.

To date, there is no evidence that mandatory registration of prepaid SIM card users 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.

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 administratively 'light' registration processes.
- 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.

Resources:

GSMA report: Mandatory registration of prepaid SIM cards — Addressing challenges through best practice
GSMA White Paper: Mandatory Registration of Prepaid SIM Card Users
GSMA & World Bank Report: Digital Identity — Towards shared principles for public and private sector cooperation
London School of Economics Academic Paper: The Rise of African SIM Registration — Mobility, Identity, Surveillance & Resistance
Deutsches Institut für Wirtschaftsforschung Academic Paper: Implications of Mandatory Registration of Mobile Phone Users in Africa
GSMA Mobile Connect website
Simon Fraser University Academic Paper: Privacy Rights and Prepaid Communication Services
AllAfrica News: Assessing the Impact of SIM Registration on Network Quality (Nigeria)
Kosmopolitica News: Global Crackdown on Phone Anonymity

Mobile Device Theft

Background

Unfortunately, there are criminals who seek to gain from the trade of stolen mobile phones, feeding a black market in handsets obtained through mugging and street crime.

Policymakers in many countries are concerned about the incidence of mobile phone theft, particularly when organised crime becomes involved in the bulk export of stolen handsets to other markets.

In 1996, the GSMA launched an initiative to block stolen mobile phones, based on a shared database of the unique identifiers of handsets reported lost or stolen. Using the International Mobile Equipment Identifier (IMEI) of mobile phones, the GSMA maintains a central list — known as the IMEI Database — of all phones reported lost or stolen by mobile network operators' customers.

The efficient blocking of stolen devices on individual network Equipment Identity Registers (EIRs) depends on the secure implementation of the IMEI on all mobile handsets. The world's 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?

Should regulations be imposed on mobile device registration?

To what extent can device-based anti-theft features complement network blocking of stolen devices, and what capabilities should those features support?

Handset theft is a growing crime and law enforcement problem in some markets where measures have not been taken to comprehensively deal with the issue. Every stolen phone causes misery, possible violence and psychological consequences for mobile users.

— James Moran, Security Director, GSMA

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 handset theft is not of the industry's creation, the industry is part of the solution. When lost or stolen mobile phones are rendered useless, they have no value, removing all incentive for thieves.

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's IMEI Database to ensure devices stolen from their customers can be blocked on networks that use the database. These solutions have been in place on some networks and in some countries for many years and they continue to be improved and extended.

IMEI blocking has had a positive impact in many countries, but for a truly effective anti-theft campaign, a range of measures must be put in place, only some of which are within the control of the mobile industry.

The concept of a 'kill switch' — allowing mobile phone users to remotely disable their stolen device — has received much attention as mobile device theft has risen. The GSMA supports device-based anti-theft features and has defined feature requirements that could lead to a global solution for owners to locate or disable their lost or stolen device and to protect and deny access to personal data stored on the device. These high-level requirements have set a benchmark for anti-theft functionality, while allowing the industry to innovate.

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 distribution of stolen devices.

A coherent regional information sharing approach involving all relevant stakeholders would make national measures more effective.

Some national authorities have proposed national 'whitelists' to combat mobile terminal theft. The GSMA opposes this approach, which could impede the free movement of mobile devices around the world, introduces privacy issues for consumers and would be considered illegal in some countries.

Resources:
GSMA & OAS Briefing Paper: Theft of Mobile Terminal Equipment
GSMA IMEI Database website
GSMA & EICTA Report: Security Principles Related to Handset Theft
GSMA Reference Document: Anti-Theft Device Feature Requirements
GSMA & EICTA Report: IMEI Security Weakness Reporting and Correction Process
GSMA News: Mobile Phone Theft in Costa Rica
GSMA Mobile Device Theft website

Mobile Security

Background

Security attacks threaten all forms of ICT, including mobile technologies. Consumer devices such as mobile handsets 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.

The GSMA plays a key role in coordinating the industry response to security incidents. It cooperates with a range of stakeholders, including its operator members, device manufacturers and infrastructure suppliers, to ensure a timely and appropriate response to threats that could affect services, networks or devices. Specifically, GSMA's Fraud and Security Group acts as a centre of expertise to drive the industry's management of fraud and security matters related to mobile technology, networks and services. 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?

How significant is the threat of mobile malware, and what is being done to mitigate the risks?

Do emerging technologies and services create new opportunities for criminals to steal information, access user accounts or otherwise compromise the security and safety of mobile networks and those that use them?

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 very high and research into possible vulnerabilities has generally been of an academic nature.

While no security technology is guaranteed to be unbreakable, practical attacks on GSM-based services are extremely rare, as they would require considerable resources, including specialised equipment, computer processing power and a high level of technical expertise beyond the capability of most people.

Reports of GSM 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.

The GSMA supports global security standards for emerging services and acknowledges the role that SIM-based secure elements can play, as an alternative to embedding the security into the handset or an external digital card (microSD), because the SIM card has proven itself to be resilient to attack.

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 from the security improvements from one generation of mobile technology to the next.

Resources:
GSMA Statement: Media Reports Relating to the Breaking of GSM Encryption
GSMA Security Accreditation Scheme website
GSMA Security Advice for Mobile Phone Users 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, through the side-effects of blocked high-risk number ranges.

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 mobile 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:

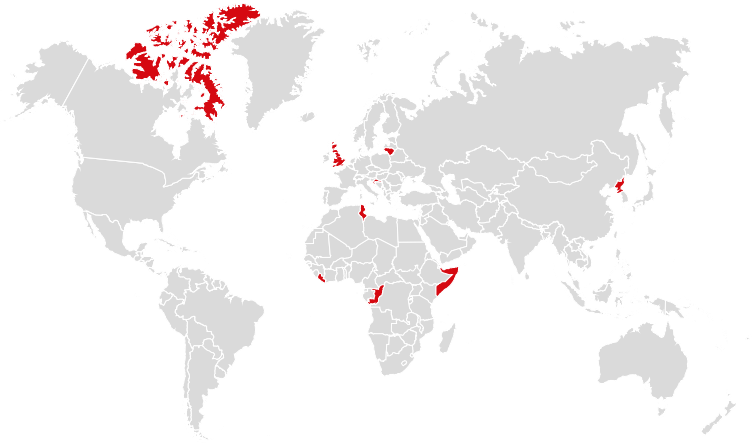
- Ensure national numbering plans are easily available, accurate and comprehensive.
- Implement stricter controls over the assignment of national number ranges to applicants and ensure the ranges are used for the purpose for which they have been assigned.
- Implement stricter controls over leasing of number ranges by number-range assignees to third parties.

The Fraud and Security Group shares abused number ranges used for fraud 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.

Resources:
ITU-T Misuse of an E.164 International Numbering Resource website
GSMA Number Resource Misuse and Fraud website

Facts and Figures

Top 10 Countries Whose Numbering Resources Are Being Abused



United Kingdom	Croatia	Republic of the Congo (Brazzaville)	Liberia	North Korea
Canada (Arctic Territories)	Tonga	Tunisia	Lithuania	Somalia

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 Report: Consumer Research Insights and Considerations for Policymakers
GSMA Mobile and Privacy website
GSMA Report: Mobile Privacy Principles — Promoting a user-centric privacy framework for the mobile ecosystem
GSMA Report: Privacy Design Guidelines for Mobile Application Development

Best Practice

Mobile Privacy Principles

The GSMA has published a set of universal Mobile Privacy Principles that 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 users' 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 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 compatible with national law.

Key areas of concern for privacy of mobile data

Data Capture	Data Security	Data Usage
What is my data used for? Is it used for commercial gain? For advertisements? Do I have a say in that?	Is my data safe? How is it being protected? What do I do if it gets compromised?	What happens to my personal data when I use my mobile? What data is collected? Who uses the data? For how long it is retained?
83% of respondents feel 3rd parties should seek permission before using their personal data	**88%** of respondents feel safe-guarding personal information is very important	**72%** of respondents are concerned about sharing the exact location of their mobile

Source: Futuresight, GSMA – User Perspectives on Mobile Privacy (2012)

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 so-called 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 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 will increasingly use the data they collect for Big Data initiatives. Therefore, 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 mobile network operators 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 Internet of Things (IoT). Rather, mobile network operators 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.

Mobile network operators 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.

Mobile network operators 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 their 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: Guidelines on the Protection of Privacy in the use of Mobile Phone Data for Responding to the Ebola Outbreak
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?

Service Restriction Orders

Background

From time to time, mobile network operators (MNOs) receive orders from government authorities to restrict services on their networks ('service restriction orders' or 'SROs'). These orders require operators to shut down or restrict access to their mobile network, a network service or an over-the-top 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 so that if they receive an SRO they can work swiftly and efficiently to determine the legitimacy of the SRO, whether it has been approved by a judicial authority, whether it is valid and binding and whether there is opportunity for appeal and they can work 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

Signal Inhibitors

Background

Signal inhibitors, also known as jammers, are devices that generate interference in order to 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' or '911', 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.

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 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 around the globe.

Global coverage

GSMA Intelligence publishes data and insights spanning 237 countries, more than 1,400 mobile network operators and over 1,200 mobile virtual network operators (MVNOs). Comprising approximately 26 million individual data points, GSMA Intelligence combines historical and forecast data from the beginnings of the industry in 1979 forward to a five-year outlook. 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 4,400 network deployments to date. White papers and reports from across the GSMA and weekly bulletins are also available as part of the service.

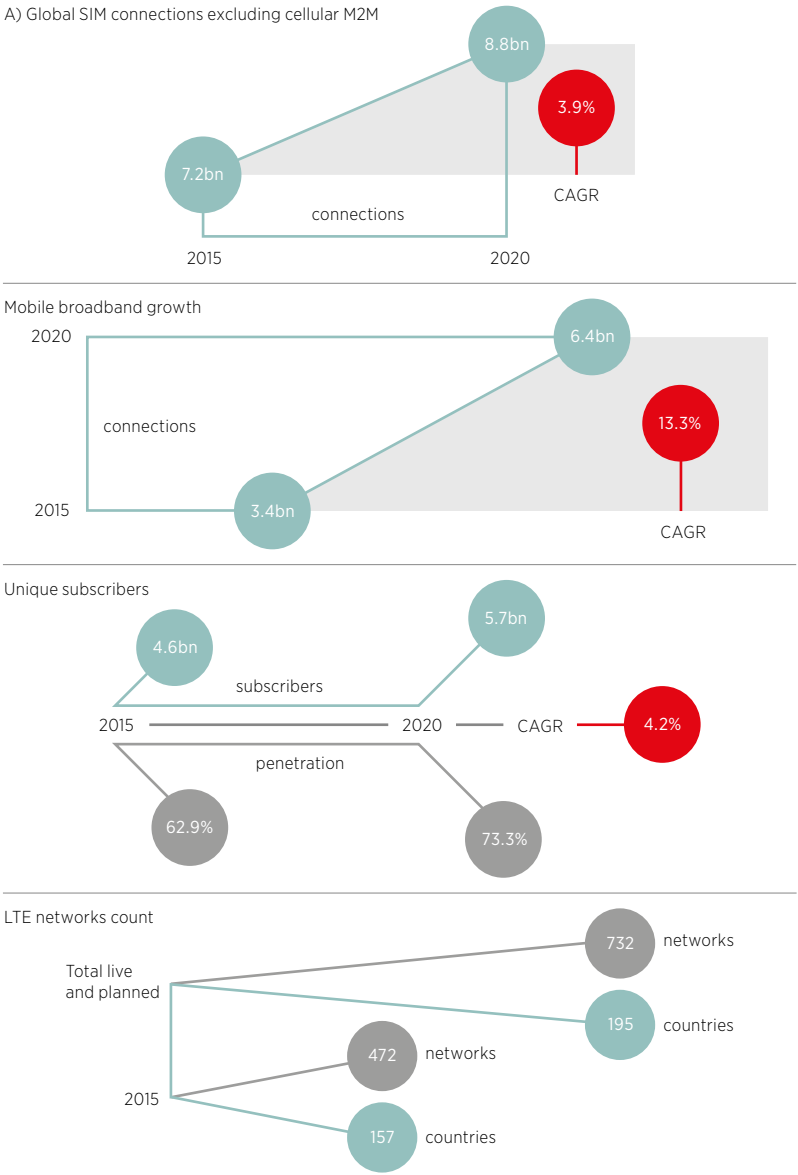
Powerful data tools

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, or graphs and charts into presentations.

https://gsmaintelligence.com
info@gsmaintelligence.com

Global Market

Source: GSMA



CAGR: compound annual growth rate

Unique subscriber penetration by region

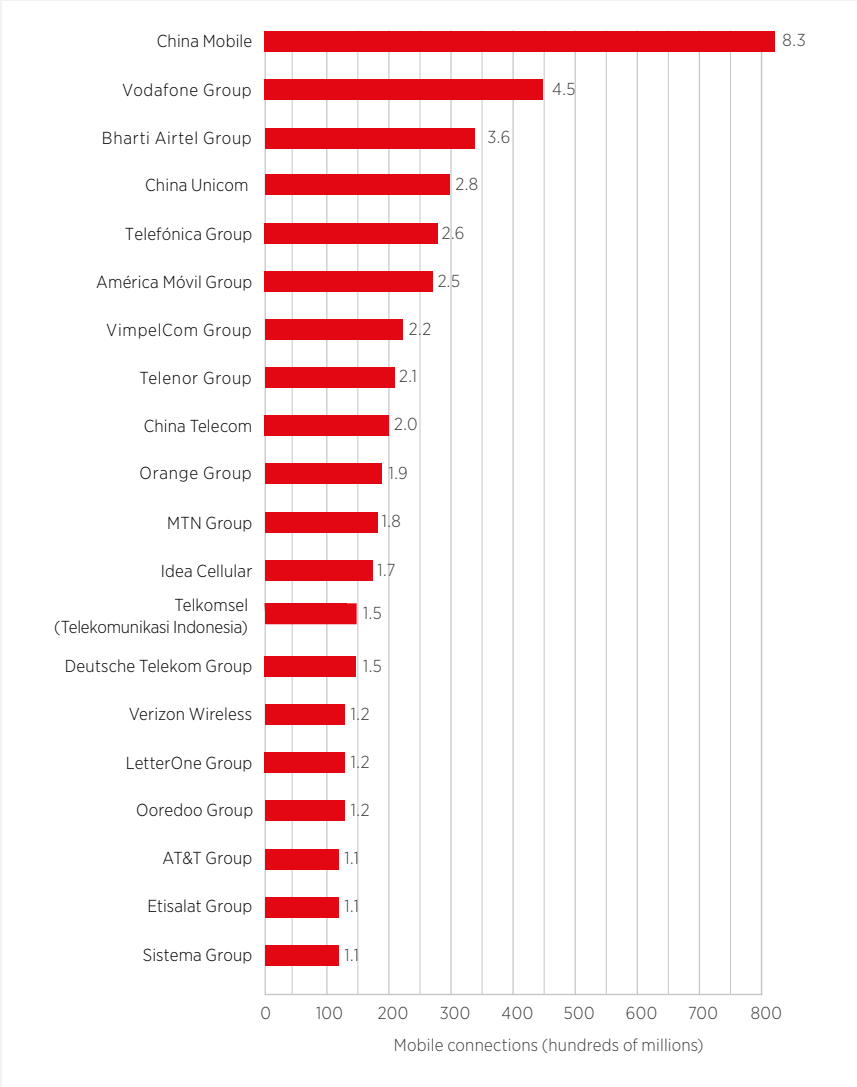
Source: GSMA Intelligence

The global unique subscriber base grew by 4.8 per cent during 2015: growth is forecast to continue, but at a slower rate of 4.2 per cent out to 2020. However, this growth is far from uniform across the regions of the world. Growth is now largely coming from developing markets, which are forecast to add nearly 980 million subscribers over the next six years, compared to only 85 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 at the end of 2015 at 43 per cent of the population, despite having seen the fastest subscriber growth of any region over the past decade.

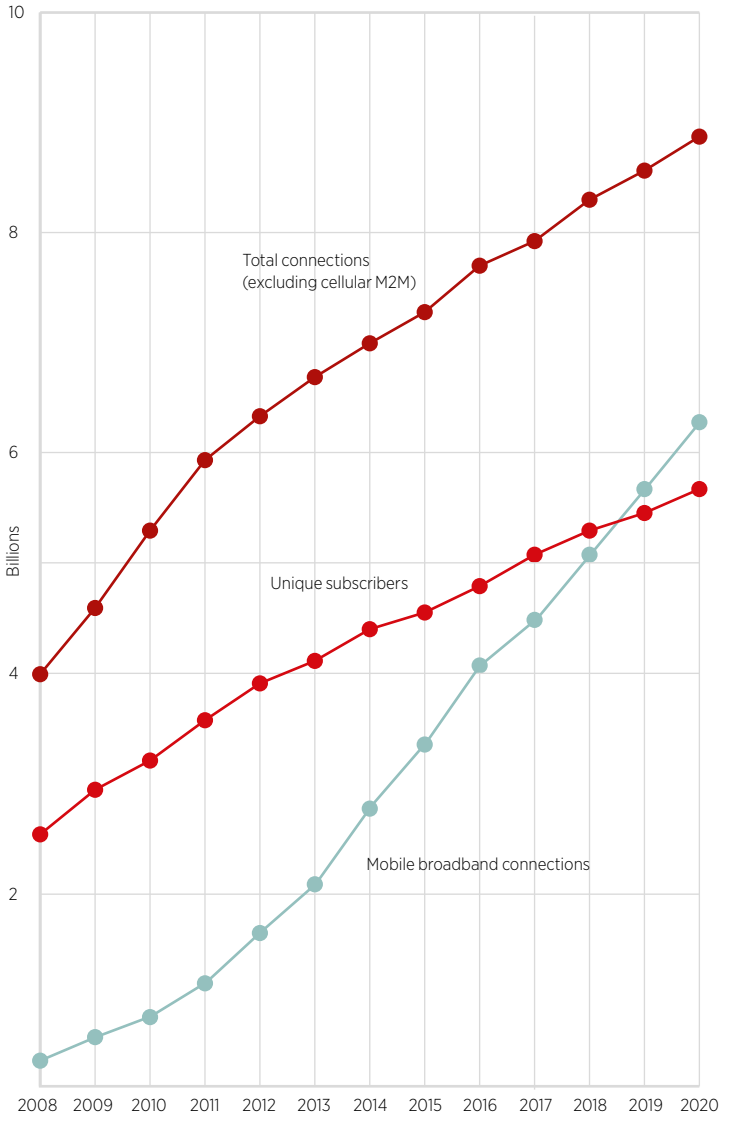
Mobile operator group global ranking by connections Q4 2015

Source: GSMA Intelligence, company reports



Global connection trends

Source: GSMA Intelligence

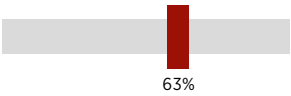


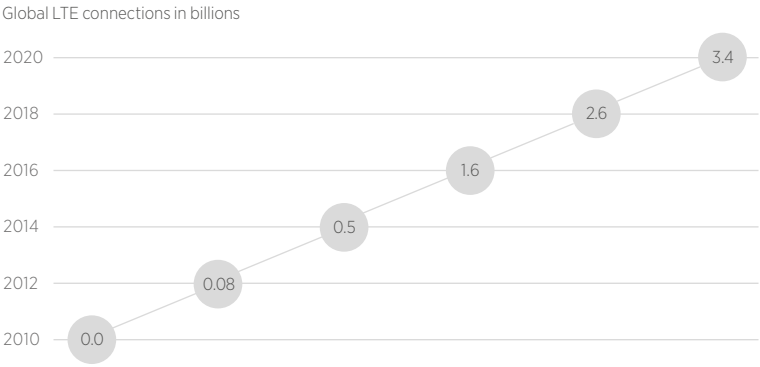
Global 4G-LTE connections forecast 2010-2020

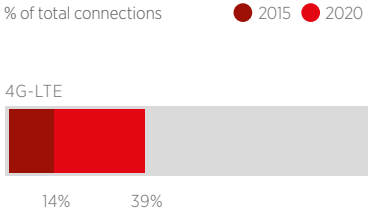
Source: GSMA Intelligence

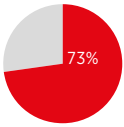
472 LTE networks commercially launched across 157 countries worldwide between December 2009 and December 2015, and at least a further 260 operators are expected to launch LTE over the coming years, leading to 3,500,000,000 4G-LTE (FDD/TDD) connections expected worldwide in 2020.

63% of global 4G-LTE connections will come from the developing world in 2020, up from less than a half in 2015, largely driven by TD-LTE growth in China.

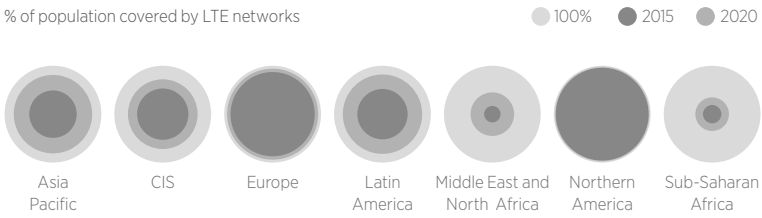




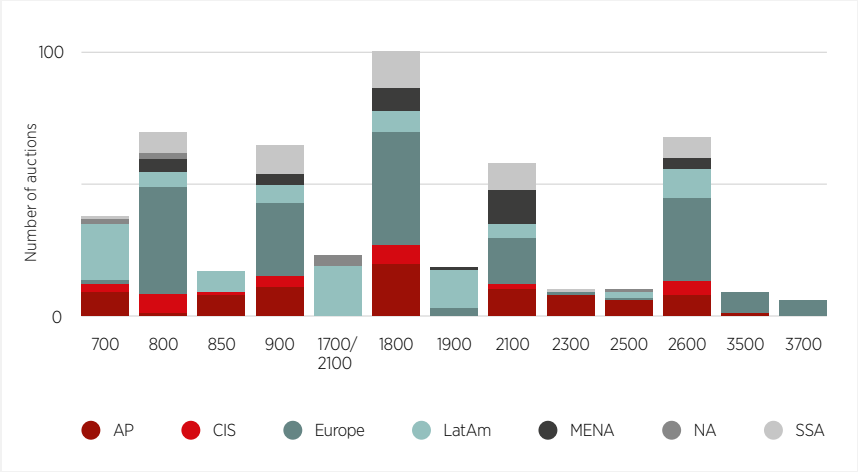




73% of the world's population will be covered by 4G-LTE networks by the end of 2020.

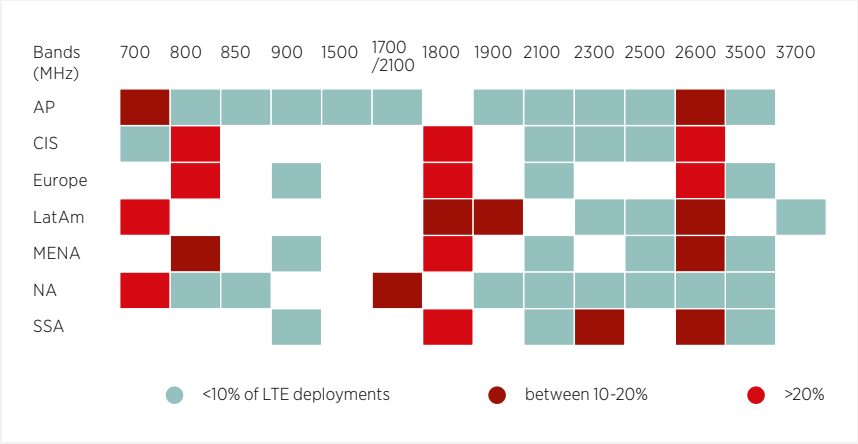


Spectrum auctioned across regions in 2012-2016 by bands



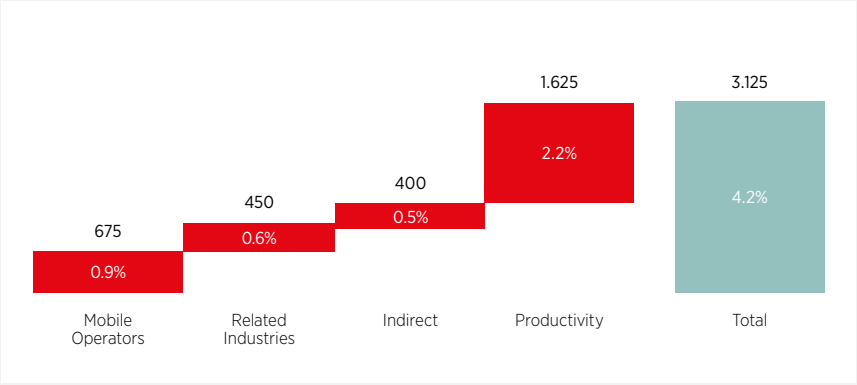
Share of LTE deployments by frequency band, by region (Oct 2016)

Source: GSMA Intelligence



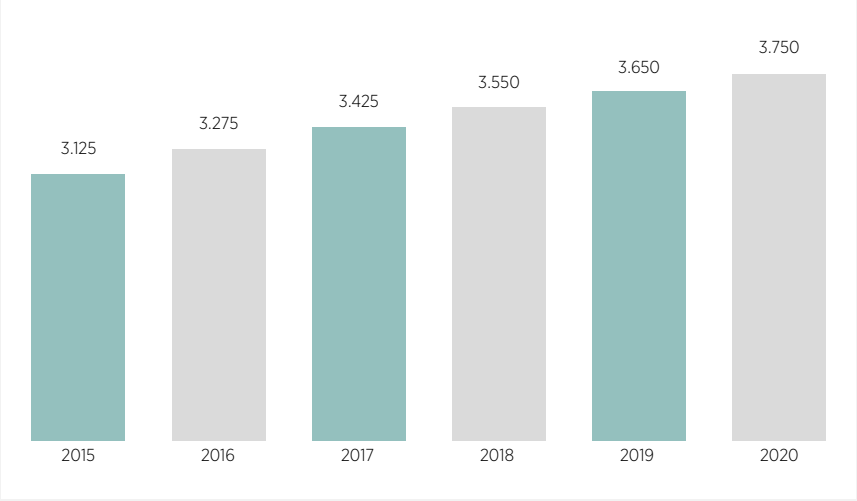
Total (direct and indirect) contribution to GDP

(2015 $bn)



Total mobile contribution to GDP out to 2020

Value added ($bn)



Financial Data