Mobile Policy Handbook

An insider's guide to the issues

October 2014

This handbook belongs to:

____

____

____

OCT | 2014

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. To this end, 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 a 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 is a practical guide to the issues, a window into industry perspectives, a signpost to regulatory best practice and a portal to more information.

As the global trade association of mobile operators, the GSMA conducts and commissions research on policy trends and challenges in the 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 third edition of the Mobile Policy Handbook, new policy topics and industry positions have been added for internet governance, single wholesale networks and passive infrastructure providers. The Mobile Initiatives section has been reorganised and updated to reflect the broad priority areas for the industry, namely, to be trusted guardians of consumer data, to connect the digital and physical worlds, to build and enable digital commerce ecosystems and to create the network for secure, smart and seamless services. All of the content has been updated and refreshed, with new resources, up-to-date statistics and real-world examples. And the appendix has been enhanced with more visual renderings of industry data from GSMA Intelligence.

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 heralds a new era, with the majority of the world's population not only making their first phone call using a mobile handset, but accessing the internet over mobile technology too. Equally profound is the revolution in machine-to-machine communications. We are at the very beginning of this development, but already billions of automated messages flow between widely connected devices, over the internet, driving forward productivity and making major improvements in health services, for example. Today about half of the world's population has access to a mobile phone; within a decade, the mobile internet will support over 50 billion machine-to-machine connections.

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.

The Role of Effective Policy

Never before has the role of the communications ministry and regulator been so critical to the success of governments' 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 is a compass that is referred to regularly on that voyage.

Mobile Initiatives

Business Environment

Spectrum Management and Licensing

Consumer Protection

Appendix

Mobile Initiatives

The mobile industry is among the most groundbreaking and dynamic economic sectors of our time, delivering connectivity, individual empowerment and an ever-growing range of mobile-powered services to people nearly everywhere on the planet. Continual innovation and investment by the industry is being driven by healthy competition, generating great benefits for consumers, 6 billion of whom will benefit from mobile broadband connections by 2020.

The GSMA leads several programmes that are shaping the continued growth and development of the sector. From new forms of mobile payment to innovations in transportation, these initiatives are laying the foundations of an increasingly connected, mobile world.

Each of the following initiatives has its own public policy considerations, and relate to one or more of the public policy topics presented in this handbook.

Agriculture
Automotive
Connect
Development
Employment
Energy
Health
Identity
Network 2020
NFC
Mobile Money
mLearning
Personal Data
Smart Cities
VoIP
Women

Connected Living: Mobilising the Internet of Things

The Internet of Things (IoT) holds tremendous promise for 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 the means to shrink healthcare costs, reduce carbon emissions, increase access to education, improve transportation safety and much more.

Still a nascent industry, by the end of 2014, there will be 250 million machine-to-machine (M2M) connections worldwide, according to GSMA Intelligence, including everyday objects such as consumer electronics, vehicles, monitors and sensors equipped to support M2M services.

For mobile network operators, IoT communications are very different from traditional 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 require global distribution coverage and managed platforms. Innovative services require mobile operators to adopt flexible commercial and technical solutions in the different geographies where their business customers operate.

To capture the benefits of the IoT, policymakers and regulators need to ensure that policy and regulatory frameworks enable large-scale deployments that encourage investment. Significant social and economic benefits through the growth of IoT services can be realised if policies and regulations are relevant, flexible, balanced and technology-neutral.

Although IoT services take many forms and are spreading across all economic sectors and geographies, they share a number of common regulatory issues:

- **Numbering and addressing resources.** IoT connected devices require numbering and addressing resources to function on mobile networks. Given the significant growth of IoT connections, numbering ranges may soon be short in supply.
- **Privacy and trust.** Consumer confidence can only be fully achieved when consumers can manage their personal data effectively and service providers respect privacy choices. Data protection and legal frameworks for privacy should be practical and proportionate, ensuring that privacy protections provide customers with transparency, notice, choice and control over the use of their personal information.
- **Security.** Robust security measures should be extended to the whole value chain of the IoT market, including device and chip manufacturers and software vendors. Reducing vulnerabilities in devices, applications and web services should be a priority for all parties, and this can be achieved through certification schemes that set global security requirements
- **Harmonised spectrum.** Both licensed and unlicensed spectrum are needed to support a wide variety of IoT applications, for connections appropriate to long and short distances, indoor and outdoor scenarios, as well as mobile and static situations. Service and technology restrictions should be removed from the terms of existing spectrum licences.

These regulatory enablers underlie all of the following 'connected living' technologies — in the automotive industry, healthcare, education and urban planning and management.

Mobile Automotive

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 (e.g., traffic jams, weather conditions, road works, parking availability), use convenience services (e.g., auto maintenance, event reservations, voice-enabled email) and enjoy car-appropriate infotainment (e.g., internet radio, social networking, passenger gaming and videos). Large-scale deployments of connected car solutions already exist in many parts of the world, and the variety of services is growing significantly as more connected navigation and infotainment options are offered.

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, fraud management) and sector-specific services such as telematics service provision, disaster recovery and datacentre hosting. To bring these innovations to the market on a wide scale, the automotive and mobile industries must work together to ensure scalable, secure, interoperable and intuitive connected experiences.

Programme Goals

The GSMA is engaging with automakers, mobile network operators and the wider ecosystem to create opportunities for connected automotive solutions and devices. A major focus of the programme is to foster the development of value-added services by mobile operators.

The primary platform for these activities is the Connected Car Forum (CCF), established by the GSMA, which accelerates the development and take-up of telematics and infotainment services through initiatives including:

- Identifying new service and data monetisation opportunities offered by 'big data' derived from connected cars and devices
- Enabling differential charging and billing for in-vehicle services using embedded technologies
- Remotely managing operator profiles with embedded SIM cards, to facilitate simple and scalable connections for vehicles
- Promoting an appropriate regulatory framework for mobile operators, as well as taking full advantage of the opportunities fostered by the regulation
- Creating cross-industry alignment on tethering technologies, such as Wi-Fi Direct and Near Field Communications (NFC)

Public Policy Considerations

A range of regulatory areas potentially affect mAutomotive service delivery. These include roaming, privacy regulations, spectrum regulation, network neutrality and internet service provider liability. The automotive sector has unique characteristics with different policy implications than consumer electronics or machine-to-machine (M2M) markets. These include, for example, a longer device lifetime, a shift away from traditional M2M services to more consumer-oriented in-vehicle services, and the need for services to operate regionally or globally.

In some regions, the uptake of mAutomotive solutions is being driven by public policy, which is mandating the fitment of embedded technologies:

- In Europe, eCall is an in-vehicle emergency call system that automatically triggers an emergency call in the event of a severe road accident. Even if passengers cannot speak, eCall creates a voice link to the closest Public Safety Answering Point (PSAP) and sends an emergency message containing essential information about the accident. The proposed legislation focuses on deployment for passenger vehicles beginning in 2015 through the 'type approval' process.
- In Russia, ERA GLONASS has similar goals to eCall and extends to insurance reconstruction and dangerous goods transport services. The first deployments are legislated for the end of 2014 for commercial vehicles.
- In Brazil, SIMRAV focuses on reducing vehicle theft and lowering vehicle insurance rates through mandatory fitment for stolen vehicle location services. Consumers have the opportunity to opt in for anti-theft services from any service provider. The first deployments are legislated for the end of 2014.

Resources
GSMA mAutomotive
Report: Connected Car Forecast Next Five Years
White paper: Split Charging and Revenue Management Capabilities for Connected Car Services
White paper: Connecting Cars — Tethering Challenges
Report: Connecting Cars — the Technology Roadmap
White paper: 2025 Every Car Connected
White paper: Connected Cars — Business Model Innovation
Interactive map: mAutomotive Deployment Tracker

Background

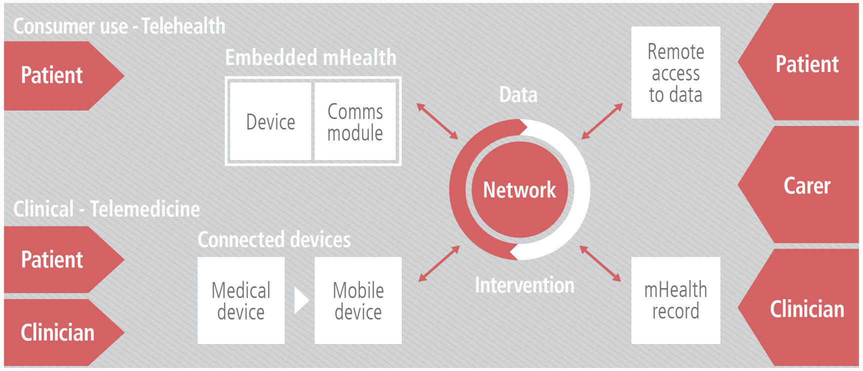
The pressures on healthcare systems have never been greater, due to factors including rising expectations, ageing populations and, particularly in emerging economies, the combined challenges of infectious disease and increasing incidence of chronic illness. Mobile health solutions provide an opportunity 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 2013 research by PWC, mHealth could help an additional 28.4 million people access the healthcare system in Brazil by 2017, and an additional 15.5 million people in Mexico benefit from healthcare without having to add a doctor. In the European Union, mHealth could save €99 billion in healthcare costs and add €93 billion to the region's GDP in 2017 if mHealth adoption is encouraged.

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. As such, there are a wide range of potential regulatory touch points.



Source: PA Consulting Group

Clear policy and regulation for mHealth is necessary 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 empowerment.** Developing policies that promote user autonomy, which will drive mHealth adoption
- **Reimbursement.** Moving towards reimbursement schemes that reward health outcomes and support innovation
- **Implementation.** Establishing government programmes that address market barriers, build evidence and lead to implementation

Regulatory themes include:

- **Medical devices.** Defining the processes for the approval of mobile medical devices and, in the case of high-risk devices, prescribing protocols and principles for product design, market implementation and tracking
- **Systems and interfaces.** Promoting interoperability and standards that enable scalability and a plug-and-play experience
- **Data protection.** Building trust through suitable data protection approaches

Resources
GSMA Response to European Commission Green Paper on mHealth
Europe: Joint Statement of the Healthcare Coalition on Data Protection
GSMA Position Paper: Medical Device Regulation
GSMA Report: Potential of Mobile Health Solutions to Address Chronic Disease Challenges
GSMA Video: Transforming Healthcare with Embedded Mobile
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

Mobile Learning

Background

Educators in many countries are using mobile technologies to support learning, not only in schools and universities, but for vocational training, continuing education, workplace training and virtually any learning situation — formal, non-formal or informal. This practice can make learning and assessment more personal, collaborative, convenient, attractive and engaging for learners, while improving their attendance and learning outcomes. Institutions benefit from better results, more flexible delivery of education, reduced costs, and better communication with students, teachers and parents.

For all of the known benefits, some educators and administrators are reluctant to introduce mobile technologies for teaching and learning, and many schools still have policies banning the use of mobile phones on their premises. However, there is now substantial evidence and insight that institutions and teaching staff can draw upon to mitigate the risks and maximise the benefits of mobile technologies in teaching and learning.

Through its Connected Living programme, the GSMA is working to build wider acceptance and adoption of mobile learning solutions, particularly mobile-enabled portable devices such as e-readers and tablets, to enhance formal education.

Public Policy Considerations

In addition to the efficacy of mobile education solutions to improve access to education and enhance learning outcomes, issues of interest to policymakers centre on the safety, privacy and health implications of mLearning.

- **Safety.** A key concern for educators, policymakers and parents is ensuring the safety of children who use the online services accessed through mobile education technologies. Safeguarding children involves the elimination or mitigation of various risks, such as access to illegal or inappropriate content and communication, mobile bullying, or undue financial burden that could affect students using the mobile service. The GSMA is actively engaged with a number of organisations that address these issues, including Teachtoday, the Family Online Safety Institute and the ITU's Child Online Protection initiative.
- **Privacy.** The GSMA and its members also address privacy issues related to all consumers' use of mobile technology, identifying mobile-friendly ways to help users make informed decisions about their information and privacy, and ensuring user privacy is respected and protected by those designing and building mobile applications.
- **Health.** Research about the potential health risks from mobile phones and networks is plentiful, and most governments and the World Health Organization have concluded that current guidance on electromagnetic field exposure limits are sufficient to protect all people, and that no specific measures are warranted for children.

Resources

GSMA mLearning Policy Handbook
GSMA and McKinsey Report: Transforming Learning Through mEducation
GSMA Report: Safeguarding, Security and Privacy in Mobile Education
UNESCO: ICT in Education

Smart Cities

Background

The world is urbanising, and municipalities realise that they need to make far better use of information and communication technology (ICT) to enable millions of people to live together successfully in small geographic areas. A 'smart city' makes extensive use of information and communication technology, including mobile networks, to improve the quality of life of its citizens through connected transport, sensors in public spaces, smart energy, mobile connectivity, contactless payments, mobile government and more. The strength of a smart city lies in its ability to harness 'big data', combining information captured by intelligently-connected infrastructure to generate insights that can improve the efficiency of a city.

Although many smart city or green city initiatives are well underway, the use of mobile technology in smart cities is still relatively new. Nevertheless, of the 150 smart cities the GSMA tracks globally, more than 100 have deployed services, beyond smartphone apps, that make use of mobile networks.

Mobile operators can play a role in four elements of smart city services:

- **Managed connectivity.** Connecting city infrastructure and individuals' handsets to central servers and databases
- **Data aggregation and analysis.** Combining data from multiple sources to produce new insights
- **Service delivery.** Delivering real-time information to people and machines that will enable them to adapt and respond to events in the city
- **Customer interface.** Providing customer support operations, such as call centres and web portals, as well as delivering messages to subscribers

Programme Goals

To ensure cities of the future are safe and healthy places to live and work, smart city initiatives are being established globally. The GSMA Connected Living programme is helping to overcome barriers to smart city advancement through industry collaboration, encouraging appropriate regulation, optimising networks as well as developing key enablers to support the growth of machine-to-machine connections in the immediate future and the Internet of Things in the longer term.

The GSMA is also working with the City of Barcelona and Generalitat de Catalunya to establish the Smart City Initiative as part of the Mobile World Capital.

The GSMA has also created the Smart Cities Index to demonstrate the value of using mobile technology for city infrastructure and services, and to measure the impact of smart city projects on municipal operations, the economy and communities.

Public Policy Considerations

Smart city projects and strategies can help city administrators achieve large-scale goals to increase the efficiency and effectiveness of city operations and achieve sustainable urban development.

Mobile smart city solutions relate to four broad areas of public policy: transportation (e.g., ticketing applications, intelligent transport systems and traffic information systems), environment and energy (e.g., smart metering, building efficiency and electric vehicle charging), municipal infrastructure (e.g., waste and water management and street lighting) and economic stimulus (e.g., the creation of mobile app developer clusters).

As all smart city strategies are inherently linked to data aggregation, integration and use, an area of potential regulatory interest relates to data collection and handling. Smart city projects must incorporate appropriate systems and practices to ensure the privacy of individual citizens is respected and their personal information protected.

Resources
GSMA Report: Guide to Smart Cities: The Opportunity for Mobile Operators
Mobile Smart City Benchmarking Report
Smart City Resilience: Learning from Emergency Response and Coordination in Japan
Article: Smart Home of the Future
Case Study: T-City Friedrichshafen, Germany

Digital Commerce

Mobile technologies are fundamentally changing how people manage their money and conduct financial transactions. Millions of people who have never had access to financial services or could not afford a bank account are now experiencing the practicality, security and convenience of mobile money services. Financial inclusion, driven by the ubiquity of the mobile phone, is creating economic opportunities for individuals and reducing the risks associated with a cash economy.

Meanwhile, mobile operators around the world are working with retailers, loyalty scheme providers and equipment vendors to roll out mobile services for digital commerce. For example, some mobile operators are offering a mobile wallet — a specialist application that can store digital versions of payment cards, loyalty cards, vouchers, tickets and other items normally found in a physical wallet. The GSMA is working with regulators to develop and support the ecosystems needed to roll out sophisticated digital commerce propositions around the world.

Mobile Money

Background

In developing countries, 2.5 billion people are 'unbanked' and have to rely on cash or informal financial services, which are typically unsafe, inconvenient and expensive. However, over 1 billion of these people have access to a mobile phone. This provides the basis for mobile money, whereby mobile technology is used to deliver convenient and affordable financial services to the underserved.

With mobile money, customers can convert cash to and from electronic value (i.e., e-money), and they can use mobile money to perform transfers or make payments. Banks that rely on traditional 'bricks and mortar' infrastructure struggle to serve low-income customers profitably, particularly in rural areas. However, mobile operators have large airtime distribution networks that can be used to provide customers with a network of mobile money agents who perform cash-in and cash-out transactions. Large mobile operators in developing countries typically have 100 to 500 times more airtime reseller outlets than all of the banks' branches put together.

Mobile money has already proven to be viable and sustainable. As of July 2014, there were 245 mobile money services in 88 countries serving more than 61 million active users. At least nine countries now have more mobile money accounts than bank accounts, and 44 countries have more mobile money outlets than bank branches.

Programme Goals

The GSMA Mobile Money programme helps mobile money services achieve scale by identifying and sharing benchmark data, operational best practices and approaches to cross-service interoperability, as well as cultivating positive regulatory environments.

Public Policy Considerations

There are many reasons for governments to encourage digital financial inclusion among their citizens. It contributes to economic growth, it offers convenience and consumer protection, and it reduces the vulnerability of a country's financial system by lowering the risks caused by the informal economy and widespread use of cash.

Mobile money services depend on a regulatory framework that embraces innovation, allowing a new class of financial services providers to sustainably provide digital payment and transfer services. Risks posed by licensed non-bank mobile money providers can be successfully mitigated by requirements that safeguard funds entering the system and ensure customers can cash out electronic value on demand. An open and level playing field is required, allowing banks as well as non-bank providers to offer mobile money services.

Mobile money reduces the risk of money laundering and terrorist financing, as electronic transactions can be monitored and traced more easily than cash.

Interoperability should not be mandated. In such a young industry, service providers and policymakers should work together to understand different models of mobile money interoperability, including the benefits, costs and risks. The role of the policymaker is to facilitate dialogue between providers, ensuring that interoperability brings value to the customer, makes commercial sense, is set up at the right time, and regulatory risks are minimised.

Resources
GSMA: Mobile Money for the Unbanked
GSMA: MMU Deployment Tracker
GSMA: 2013 State of the Industry report
GSMA: Mobile Money Regulatory Guide
GSMA: Mobile Money: Enabling Regulatory Solutions
GSMA: The Kenyan Journey to Digital Financial Inclusion
GSMA: Enabling Mobile Money Policies in Sri Lanka — The Rise of eZ Cash

Near Field Communications

Background

Businesses and consumers are looking to digital commerce to provide flexible and efficient transaction services across a range sectors, including retail, transport, financial services, online and advertising. Near Field Communications (NFC) is a wireless technology that can transfer information between two devices within a few centimetres of each other. NFC chips are now being embedded into mobile phones and SIM cards in mobile phones, enabling an array of new digital services, including:

- **Ticketing** — replacing paper tickets on public transport systems
- **Payments** — replacing cash and credit cards to purchase goods and services
- **Access control** — replacing traditional keys
- **Couponing** — replacing vouchers and coupons
- **Advertising** — using NFC tags that can be embedded on posters, on billboards or next to products in retail stores to give NFC users additional information such as maps, video and URLS

By the end of 2014, there will be more than 150 SIM-based NFC launches, of which nearly 60 operate as commercial services around the world. Mobile operators, as they seek to harness the potential of NFC, are engaging with the relevant actors in their markets, including local and national governments, transportation bodies, banks, retailers and other stakeholders. In some cases, mobile operators are forming joint ventures with other operators and banks. In others, they are engaged in partnerships based on business models that incentivise all the actors in the NFC value chain.

Programme Goals

The GSMA is focused on driving a standardised deployment of mobile NFC using the SIM as the secure element to provide authentication, security and portability across many different handsets. Adopting SIM-based NFC as a global standard will also create economies of scale and ensure interoperability. These factors will be critical to the widespread adoption of NFC, enabling people around the world to benefit from NFC services, regardless of their operator network or device type.

Public Policy Considerations

SIM-based NFC handsets can provide robust security features, such as PIN numbers to access services and strong authentication techniques (such as a digital signature or one-time password) to protect the mobile wallet. Moreover, the mobile operator can activate and deactivate services over the air if the phone is lost or stolen, and reinstall services once a new phone is provisioned. The SIM also complies with international security standards and is tamper resistant.

SIM-based NFC reduces the need for cash and plastic cards, leading to operational efficiencies and cost savings. In some cases, SIM-based NFC could also reduce fraud, increase the number of customers who can be served at one time, help track inventory and facilitate value-added services, such as automatic coupon redemption.

Mobile NFC services have the potential to lower barriers to entry for smaller service providers. This could lead to increased competition, more choice for consumers and reduce prices.

Resources

GSMA Report: Socio-Economic Benefits of SIM-Based NFC
GSMA Report: Mobile and Online Commerce, Opportunities provided by the SIM
GSMA Toolkit: Managing Risk in Mobile Money
GSMA White Paper: Mobile NFC in Retail
GSMA Report: The Value of Mobile NFC in Transport 2014

Network 2020

With the gradual shift in mobile telecommunications towards internet protocol (IP)-based content and services, mobile operators need a new model for delivering voice and messaging. In an all-IP world, mobile operators will deliver a broader set of communications options for their customers, including voice, data, video and other rich communication services.

Embracing this future is vital for mobile operators as they compete to win and retain customers. The GSMA is working with mobile operators to use inative IP communication services such as voice and video calling over LTE, rich communication services, and HD Voice to provide the same carrier-grade experience historically linked with voice services, initiated via a handset's green button. This is the industry's Green Button Promise — to provide reach, reliability and richness to customers, strengthened by the ability to interconnect all mobile phones and devices globally.

The mobile network of the future is also more energy efficient. Mobile network operators remain overly dependent on fossil fuels to power generators at off-grid mobile base stations. The GSMA is assisting mobile operators with energy assessments and recommendations for using renewable energy sources to reduce operating costs, shrink dependence on diesel fuel and reduce carbon emissions in the provision of mobile service.

IP Communication Services

Background

Using IP-based solutions opens up a world of innovative and enhanced communication services for customers. The GSMA's Network 2020 Programme covers a wide portfolio of IP-based services.

- **Rich Communication Services (RCS)** comprise not only voice and messaging, but also live video and file sharing between IP-enabled devices and across IP-enabled networks. RCS marks the transition of messaging and voice capabilities from circuit-switched technology to an all-IP world, leveraging the same IP multimedia subsystem (IMS) capabilities as Voice over Long Term Evolution (VoLTE) and video calls over LTE. The service can be natively integrated into the handset for a seamless user experience, and it is already supported by a wide range of mobile devices. It can also be implemented from downloadable apps. RCS is offered by nearly 40 mobile operators in over 30 countries.
- **VoLTE and video calling over LTE** using IMS technology are recognised as the industry-agreed progression of voice services. VoLTE can be deployed in parallel with video calls over LTE and RCS multimedia services. It also increases the service quality delivered to consumers by offering HD Voice. There are nearly 120 VoLTE services commercially available in 73 countries.
- **High-Definition Voice** provides a significant upgrade to the sound quality of communications, offering users greater clarity, reduced background noise and the feeling that the person they are speaking to is right next to them.

Programme Goals

The GSMA is working with leading operators and equipment vendors to accelerate the launch of IP-based VoLTE and RCS services around the world. The work of the programme covers the development of specifications, assisting operators with the tecnical and commercial preparations for service launches and speeding progress towards more interoperability. For consumers in some markets, the presence of these RCS services is through the joyn^{TM} brand, which acts as verification that devices and services carrying the logo have been accredited.

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 policy 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 standard.** RCS is currently specified by the GSMA and a cross-operator forum as an open industry standard for IP-based file and video sharing services, generically based on the IMS. RCS allows any mobile operator or service provider to interconnect without discrimination.
- **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, to retain a range of subscriber and usage data and to disclose this data to law enforcement agencies on demand. While RCS allows lawful intercept at both the service data layer and session data layer, any interference with mobile users' right to privacy must be in accordance with the law.
- **Security.** National data can stay secure and in country through local deployment of IMS infrastructure by operators and control of routing by the home network. The protection and privacy of customer communications is at the forefront of operators' concerns, and the mobile industry is committed to maintaining the integrity of its communications services.
- **Interconnect.** RCS allows interconnect to happen at the service layer, and termination of RCS traffic follows the same model as standard mobile voice and data services. Mobile termination rates (MTRs) are wholesale rates, regulated in many countries by establishing a schedule of annual rate changes that are factored into mobile network operators' business model.

Resources
Report: The Value of Reach in an IP World
Report: RCS and Joyn: Keeping Operators at the Center of Communications

Mobile Energy Efficiency

Background

Mobile network operators (MNOs) spend approximately $15 billion on their annual energy use. Therefore, it is no surprise that energy efficiency is a strategic priority for them globally. As mobile use continues to grow, so does the demand for energy, particularly by the network infrastructure. At the same time, mobile technology plays an important role in enabling energy efficiency in other sectors, and more generally across the global economy.

Mobile's Green Manifesto 2012, published by the GSMA, outlines the positive impact of mobile operator initiatives in energy and carbon management, as well as progress around mobile's efficiency-enabling role. Highlights from the report include the following:

- Mobile has the potential to enable much greater emissions savings of at least 900 million tonnes of CO_{2e} in 2020, which is 1.7% of the global 2020 greenhouse gas emissions forecast by the International Energy Agency in its 'business-as-usual' scenario.
- Analysis of 34 mobile networks worldwide shows total network energy consumption increased only slightly from 2009 to 2010, despite considerable growth in mobile connections and traffic.
- Total energy per unit traffic declined by approximately 20% and energy per connection declined by 5%, from 2009 to 2010.
- Currently, 26 million mobile machine-to-machine connections worldwide are reducing greenhouse gas emissions by an estimated 3 million tonnes of CO_{2e} annually.

Programme Goals

To help MNOs reduce their energy costs and greenhouse gas emissions, the GSMA's Mobile Energy Efficiency (MEE) programme offers two services to mobile network operators: MEE Benchmarking and MEE Optimisation.

MEE Benchmarking is a management tool that helps MNOs measure and monitor the relative efficiency of their radio access networks, identifying under-performing networks and quantifying the potential efficiency gains available, typically around 10% to 25% across a mobile network operator's portfolio.

MEE Optimisation is a follow-on service that uses the MEE Benchmarking results combined with site audits and equipment trials, first to analyse the costs and benefits of specific actions to reduce energy and emissions, and second to roll out the most attractive solutions. The service is run in partnership with a third-party vendor or systems integrator.

Resources
GSMA Mobile Energy Efficiency
Mobile's Green Manifesto 2012
GSMA Report: Mobile Energy Efficiency — An Overview
GSMA Mobile Energy Efficiency Case Studies

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 connected devices. Personal data and user authentication are requisite elements of being online — users must identify themselves to be able to access their accounts and subscriptions, to make purchases, and so on.

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. Meanwhile, identity theft is on the rise. Failure 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 digital identity management. With mobile operators' unique advantages such as the SIM card, strong registration processes, network authentication and fraud detection, mobile operators have the ability to provide sufficient 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 association is also working with industry standardisation bodies such as the Open ID Foundation to ensure support and interoperability for global standards.

Together, mobile operators will bring digital identity solutions to the market with scale, offering a seamless consumer experience, consistent technology and low barriers to entry across the digital identity ecosystem.

Advantages of mobile operators in providing a digital identity service

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
Flexibility to innovate	Ability to add consumer functionality such as 'add to bill' or 'click to call'

Mobile Connect

Background

At Mobile World Congress 2014, the GSMA unveiled the Mobile Connect initiative with the support of leading mobile operators. The GSMA Mobile Connect service will simplify consumers' lives, offering a single, trusted, mobile phone based authentication solution that fully respects their online privacy.

Digital identity services provide customers with the ability to authenticate and identify themselves remotely and securely via their mobile phone for digital services. This 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 will enhance user privacy, reduce the risk of identity theft and simplify the login experience for a range of services by leveraging the established data handling processes of the operators and inherent security of the SIM for authentication and identification. With a streamlined, secure log-in, consumers will have easier access to retail, government and banking services, among others, without the need to remember additional passwords.
- For service providers, Mobile Connect will offer 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.

The standards-based GSMA Mobile Connect service will utilise the OpenID Connect protocol, offering broad interoperability across mobile operators and service providers, further ensuring a seamless experience for consumers.

Programme Goals

Initially, the focus is on getting a consistent approach across the mobile industry to provide authentication services such as seamless login. This means that the consumer chooses to use Mobile Connect as their digital identity solution when they sign up for a new service with a provider (or add it later), and the provider then queries the mobile operator for the credentials of the consumer. As a result, the consumer can remain anonymous to the service provider, while the service provider gets a better way to manage credentials and give the consumer a more convenient user experience for its services.

Public Policy Considerations

Mobile identity services inevitably involve multiple devices, platforms and organisations that are subject to differing technical, privacy and security standards. Some governments are already using mobile technology as a key enabler to deliver digital identity services in their digital plans. However, 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 wide-scale mobile identity services and transactions
- Engage with MNOs and the wider ecosystem to facilitate interoperability and innovation

Governments should create a digital identity plan that acknowledges the central role of mobile in the digital landscape. 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 to protect mobile networks and their customers.

In summary, MNOs, 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 Identity Global Review
Mobile Identity: A Regulatory Overview
Case study: Norwegian Mobile Bank ID: Reaching scale through collaboration
Case study: Swisscom Mobile ID: Enabling an Ecosystem for Secure Mobile Authentication

Mobile for Development

The transformative power of mobile is particularly apparent in developing economies, where feature phones and smartphones span the digital divide to give billions of people access to communications, information and mobile-enabled services.

The economic benefit of mobile stems from the direct employment and economic activity generated by the sector, the wider mobile ecosystem that relies on mobile networks and technologies, and the increase in economic productivity that mobile provides by keeping people connected virtually wherever they are.

Access to the mobile internet and related services has been demonstrated to improve education, health and agricultural productivity, as well as create employment and entrepreneurial opportunities, leading to improved quality of life for individuals and their families.

These benefits of mobile technology have permeated society across much of the developing world, but there is more that the industry and government can do to maximise the potential of this technology for the added well-being and personal empowerment of all. Since the creation of its Mobile for Development programme, the GSMA has partnered with 50 mobile operators to roll out 104 initiatives that have impacted tens of millions of people in 49 countries. The following pages describe several of the areas where proven concepts are finding ways to scale.

Disaster Response

Background

In the 2005 World Disaster Report published by the International Committee of the Red Cross (ICRC), access to information was described as being as important as access to food, water, shelter and medication. In this way, mobile networks play a crucial role in disaster response efforts, and research highlights their extraordinary resilience and ability to facilitate critical communication between humanitarian agencies, affected populations and the international community.

The power of mobile was evident in the aftermath of the Haitian earthquake, which saw a proliferation of new coordination and response strategies that were built around this platform. Mobile's role in disaster response will only grow, and as the ecosystem becomes more complex, a better understanding of how the mobile industry can lend support is needed.

Programme Goals

The GSMA Mobile for Development Disaster Response Programme is working with mobile operators to determine how they can improve preparedness and network resilience in disasters, 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 mobile networks.

Resources
GSMA Disaster Response
Preparing for Disaster: An Analysis of Turkcell's Disaster Management System
OCHA Report: Humanitarianism in the Network Age
Philippines Case Study: Designing an Effective Disaster Preparedness and Response Programme
GSMA Report: Towards a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters

Green Power for Mobile

Background

Mobile networks in the developing regions of the world are challenged by the limited reach of the national electricity grid and lack of reliable power supply where there is grid. As a result, worldwide, there are about 640,000 off-grid mobile network sites, and these are primarily powered by diesel generators. Diesel-powered base stations in remote areas are costly to operate and maintain, and have a higher carbon footprint than on-grid base stations.

Programme Goals

With the support of the International Finance Corporation, the GSMA Green Power for Mobile Programme aims to extend mobile network coverage beyond the reach of national electricity grids, while reducing energy costs and minimizing the environmental impact.

The GSMA assists mobile operators in adopting renewable energy sources, such as solar, wind, biomass, fuel cell or sustainable biofuels and hybrid power systems, in order to power an estimated 118,000 new or existing off-grid base station sites in the developing regions of the world. Reaching this target will reduce annual diesel consumption by an estimated 2.5 billion litres, and reduce carbon emissions by up to 6.8 million tonnes annually.

By convening industry-wide working groups, disseminating market insights and offering direct technical assistance, the programme has prompted the adoption of green power at over 40,000 live and planned green sites, the details of which can be found on the Green Deployment Tracker.

Resources
GSMA Green Power for Mobile
GSMA GPM Bi-Annual Report, July 2013
GSMA Green Power Deployment Tracker

Mobile Agriculture

Background

Over 2.3 billion people in the world live in poverty, and the majority earn their primary livelihood from small farms in developing countries. In many of these countries, farmers get information such as planting techniques, crop management and pesticide use from agricultural extension workers. But in some countries, one extension worker may be expected to assist up to 4,000 farmers, resulting in long delays between each visit. Without access to timely information, farmers are vulnerable to factors such as weather, pests and disease, which can destroy their crops, harm their livestock, and keep them stuck in the cycle of poverty.

With mobile phone penetration in the developing world now exceeding 70% and continuing to grow rapidly, mobile technology provides a platform to bridge the information gap and connect smallholder farmers to timely, vital agricultural information that can help them make more informed decisions and boost their productivity. Commercially profitable mobile advisory services have taken hold in India, for example, and have boosted the productivity and income of smallholder farmers by up to 50%.

Programme Goals

The GSMA mAgri programme works with mobile operators, the development community and agricultural organisations to facilitate the creation of scalable, replicable and commercially sustainable agricultural information and advisory services. The initiative includes challenge fund grants, provision of digitised agricultural content via an online database, technical assistance, sharing of best practices and impact evaluation. Since its inception in 2009, the GSMA mAgri programme has supported pilot projects in India and Kenya, benefitting over 1.5 million farmers in the two countries. It has subsequently provided grants to four mobile operators under the mFarmer Initiative in partnership with the Bill & Melinda Gates Foundation and USAID to develop agricultural information and advisory services that will benefit over 2 million additional farmers.

With support from the UK Government's mNutrition Initiative, the GSMA mAgri Programme created a new challenge fund in February 2014. In order to reach 2 million users with life-changing mobile agriculture services, the fund provides risk capital to strong and innovative projects across South Asia and sub-Saharan Africa.

Public Policy Considerations

In some cases, the national Ministry of Agriculture has been important for the success of information-based mAgri services. One example is where organisations linked to the Ministry of Agriculture have provided validation for the content that mobile network operators (MNOs) send to farmers.

There are also some challenges that Ministries of Agriculture or other government bodies can help to overcome, such as these:

- **Kenya and Tanzania.** The Meteorological Departments have blocked MNOs from using private weather information, referencing the government's monopoly on this type of information. This kind of barrier hinders the uptake and value proposition of mobile agriculture solutions and needs to be addressed.
- **India.** Telecoms authority TRAI has hindered SMS outreach by increasing the charge for promotional and transactional SMS for operators. This was adopted as a measure against spamming consumers with marketing messages. They also brought in regulations that require customers to double-confirm their subscription to a service, the second confirmation through a third party. This consumer-protection measure curbs the practice of activating user accounts and charging them without their permission, and has been successful in decimating the number of consumer complaints related to this behaviour.

Resources
GSMA mAgri Website
Women in Agriculture: A Toolkit for Mobile Services Practitioners
GSMA Agri-VAS Toolkit
GSMA Infographics

Mobile for Employment

Background

Globally, according to the International Labour Organization, 74.5 million people aged 15–24 were unemployed in 2013, up nearly 1 million from the year before. With a global unemployment rate of 13.1 per cent, young people are three times as likely to be unemployed as adults.

As an extreme example, the Nigerian National Bureau of Statistics (NBS) reported that 54 per cent of young people in the country were unemployed in 2012. This staggering rate was surpassed by Spain at the beginning of 2014, when 56 per cent of those aged 16–24 were reportedly out of work. As the global economy rebounds from a lengthy and painful recession, there are few signs of recovery in youth employment.

Macro-economic forces impact the supply of jobs, clearly, but research shows a disproportionate impact of economic constriction on young people, due to the lack of appropriate skills and experience, communication barriers, lack of knowledge of jobs available, and inability to travel to work. Pioneering mobile services such as Stepping Stone, Souktel Job Connect and Ooredoo Najja7ni are providing much-needed job-related training, employment matching and career guidance.

Because of the prevalence of mobile phones among young people worldwide, the mobile industry can play a valuable, practical and sustainable role in filling young job-seekers' gaps in skills and knowledge.

Programme Goals

The GSMA Mobile for Employment programme fosters the launch of youth-focused mobile employment services such as learning and training, job connect platforms, salary payments, employee registrations, and secure helplines for employment advice.
The GSMA also conducts research to understand market opportunities, and brings together mobile operators, the development community and other key stakeholders to provide guidance in developing scalable solutions.

Public Policy Considerations

Governments should recognise the benefits of mobile as a low-cost means of serving and communicating with unemployed citizens. Mobile can be used as a means of gathering labour-market statistics, in order to design programmes that help formal and informal sector workers improve their social and economic status. Key actions:

- Develop programmes that train youth and funnel youth into mobile employment services
- Establish policies and programmes that support youth employment through mobile technology
- Drive collaboration among mobile network operators to promote access, outreach, and scale for mobile employment offerings
- Monitor the quality of mobile training programmes to ensure they offer the best advice and guidance

Resources
GSMA Mobile for Employment
BBC News Article: Future Costs of Youth Unemployment
Economist Article: Generation Jobless

Women and Mobile

Background

Mobile phones provide distinct benefits to women, including improved access to educational, health, business and employment opportunities. According to a 2010 study commissioned by the GSMA and the Cherie Blair Foundation for Women, across low and middle-income countries on three continents, women believe that a mobile phone helps them lead a more secure, connected and productive life.

However, a significant gender gap exists. Across all countries, women are 21% less likely to own a mobile phone than men. This figure increases to 23% if they live in sub-Saharan Africa, 24% if they live in the Middle East and 37% if they live in South Asia. The connectivity gap represents approximately 300 million women.

The reasons women cite for not owning a mobile phone include the cost of handsets and service, a lack of need for a mobile phone and fear of being able to master the technology. Cultural issues, such as the traditional roles of men and women, also factor into women's mobile phone ownership and can delay or even prevent a woman's acquisition of a mobile phone. Strategies that address these concerns are essential and, for mobile operators, spreading the benefits of mobile to unconnected women offers the incentive of an expanded customer base.

Women are also less present in many high-growth fields like science, technology and engineering, which are important to countries' innovation, connectedness and competitiveness in global markets. Women today compose 40% of the global workforce and account for more than half of university graduates, and yet we see only 3-5% of senior positions in technology being held by women. In Europe, organisations that have women in senior management positions generate a 35% higher return on equity, while female employment overall provides an annual economic boost of €9 billion, according to a 2013 European Commission survey on women in ICT.

Programme Goals

The GSMA Connected Women programme is focused on the socio-economic benefits of greater inclusion of women at all points in the mobile industry continuum, from consumer to employee to leader. It seeks to accelerate growth of the female digital economy by working with partners to bring significant socio-economic benefits to all women and to the global mobile ecosystem.

The programme is supporting stakeholders in increasing the number of women consumers and levels and variety of usage of mobile technology. Working alongside mobile operators and non-governmental organisations, the programme aims to equip mobile network operators and their partners with the knowledge needed to take action to reduce the global mobile gender gap, increase the availability of life-enhancing mobile services, and overcome barriers to women's use of mobile phones.

The programme is also educating mobile industry stakeholders on the value of driving gender equity in the industry, motivating industrywide action with the goal of closing the digital skills gap and increasing the proportion of female leaders in the industry. This includes raising global awareness of the issue while addressing the gaps in female participation and skills that have the potential to hold back innovation, productivity and commercial success.

Resources
GSMA mWomen
IFC Report: Investing in Women's Employment
Report: Women and Mobile — A Global Opportunity
GSMA Report: Striving and Surviving — Exploring the Lives of Women at the Base of the Pyramid
GSMA mWomen Deployment Tracker
GSMA calls for more women in the mobile communications industry

Business Environment

Governments are duty-bound to create a business environment in which industry can thrive and innovate for the good of all. For the mobile sector, flexible, light-touch regulation is essential. The market, inevitably, will shape the industry's evolution, and highly prescriptive regulatory policy cannot keep pace with the swift advance of mobile technologies, services and consumer demand.

One example of regulation falling behind is the current asymmetry 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. Internet players offering equivalent voice and messaging services are subject to none of these requirements. Asymmetric regulation has resulted in an uneven competitive landscape, and the mobile sector is bearing the cost of the market distortion created by outdated regulation.

Equitable rules for business create an environment that, through competition and innovation, leads to the best outcomes for citizens everywhere. Getting the business environment right is not only important for the mobile industry and the billions of consumers it serves, but also for the whole digital ecosystem.

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 levels, 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 planning permission 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?

Should EMF exposure limits be specified in mobile operator licences?

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

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. International standards provide the most appropriate basis for the management of EMF concerns.

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, collocations or certain site upgrades, 'one-stop shop' licensing procedures and tacit approval.

Base-station exposure guidelines should be aligned with international standards as recommended by the World Health Organisation (WHO) and International Commission on Non-Ionizing Radiation Protection (ICNIRP). International standards are based on sound scientific evidence and expert review, and should be respected. Additional 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.

> *In the large majority of countries, 36 services are now commercially available, at least in major urban areas. As networks are being upgraded and services accordingly offered in the market, mobile broadband subscriptions will continue to grow strongly.*
>
> — International Telecommunication Union, 'Measuring the Information Society 2013'

Resources

Report: Base Station Planning Permission in Europe
World Health Organization: Electromagnetic Fields
Federal Communications Commission (USA): Radio Frequency Safety
GSMA: Arbitrary Radio Frequency Exposure Limits – Impact on 4G Network Deployment
GSMA Infographic: Mobile Networks for a Better-Connected World
GSMA: LTE Technology and Health

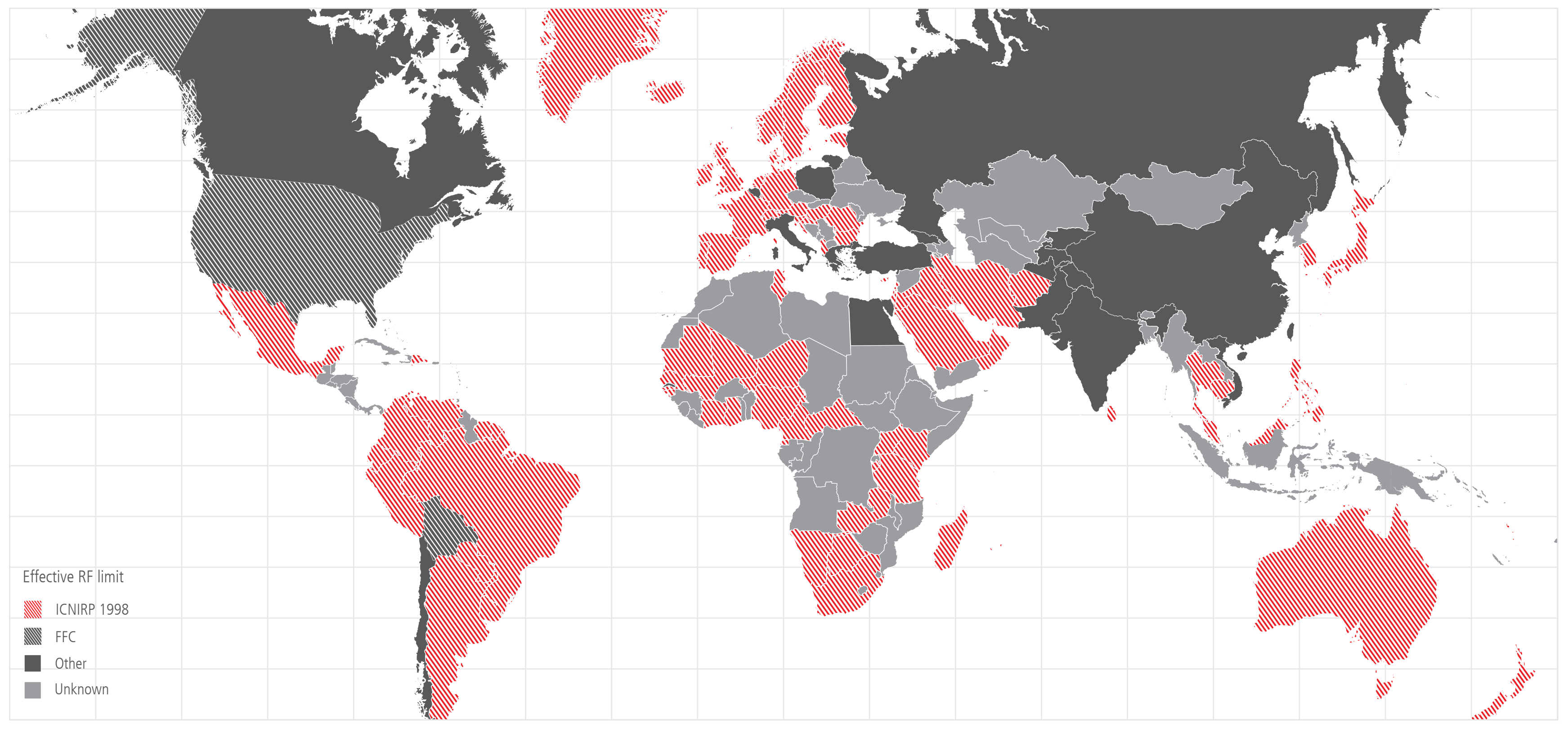
Facts and Figures

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.



Source: GSMA

Competition

Background

Mobile phones are the most widely adopted consumer technology in history. The success of mobile can be linked to a number of factors: rapid advances in technology, innovation in product and service design, and strong latent demand from the many billions who had yet to make a phone call.

A number of these factors were driven by innovation in core network design and technology, itself the result of a widespread policy of infrastructure competition. Now the innovation has moved to the edges — in the handset and in mobile applications. The internet has caused this shift, and indeed the mobile network is part of the internet.

Mobile industry competition occurs in two main areas: access and services. Access competition is typically based on infrastructure. Service competition used to be predominantly among the technology-enabled, traditional telecommunications companies, but movement towards digital and IP-based mobile networks has brought in new service competitors, whose focus is typically on user applications and software.

Early in the mobile licensing process, most countries decided to ensure competition in mobile communications by licensing at least two providers. Since then, as additional mobile bands have been identified and allocated, new infrastructure competitors have entered, increasing the level of competition.

Debate

What is the appropriate level of infrastructure competition in a given market?

What measures can governments take to achieve appropriate competition without stifling innovation?

Industry Position

Governments should facilitate the normal functioning of competition in the mobile sector rather than over-regulating it. Excessive regulation can stifle innovation, raise costs, limit investment and harm consumer welfare due to the inefficient allocation of resources, particularly spectrum.

Mobile markets should, in principle, be open to competitive entry, for example through the provision of spectrum licences. Governments should not discriminate in favour of, or against, new market entrants, but establish a level playing field.

Because the industry is capital-intensive, sufficient scale is needed for mobile operators to function profitably while keeping prices affordable for their customers. Allocating spectrum to organisations that don't have the ability to deploy or heavily invest in infrastructure may not, in fact, increase competition.

Market power, usually the result of commercial success, is only harmful when it is abused. Competition law should be sufficient to safeguard against market dominance that harms consumers.

Governments should be critical of any barriers to market consolidation and, instead, allow sustainable market structures to evolve naturally.

Whatever the institutional framework, there is always a choice between *ex ante* and *ex post* intervention. When markets are mature and competitive, *ex ante* regulation is less appropriate, and *ex post* regulation should be the primary remedy.

> *Competition has done wonders for the mobile voice market, and now I hope it will bring more prosperity by delivering mobile broadband, especially where there are no fixed networks.*
>
> — Martin Cave, Imperial College Business School

Resources

Report: Mobile Wireless Performance in the EU and US
Report: Competition and the Mobile Sector in Developed and Developing Countries
Report: Mobile Broadband, Competition and Spectrum Caps
Report: Licensing to Support the Broadband Revolution

Case Study

Comparing Mobile Sector Performance in the EU and US

There is broad agreement that the European Union mobile wireless market is underperforming relative to other advanced economies, including the United States. The EU is lagging in deployment of next generation wireless infrastructures and the advanced services they make possible, and EU consumers are worse off as a result.

The US market is outperforming the EU market:

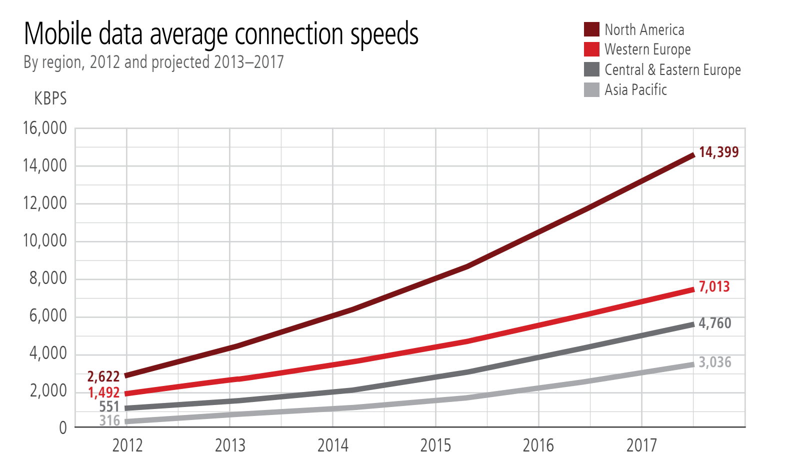
- EU consumers pay less per month than US consumers for mobile wireless services, but Americans use five times more voice minutes and twice as much data.
- Investment growth in the US is translating into faster data connection speeds: US speeds are now 75% faster than the EU average, and the gap is expected to grow.
- The US is deploying LTE at a much faster pace than the EU; by the end of 2013, 19% of US connections will be on LTE networks compared to less than 2% in the EU.

Part of the cause is the relatively inefficient structure of mobile wireless markets in the EU:

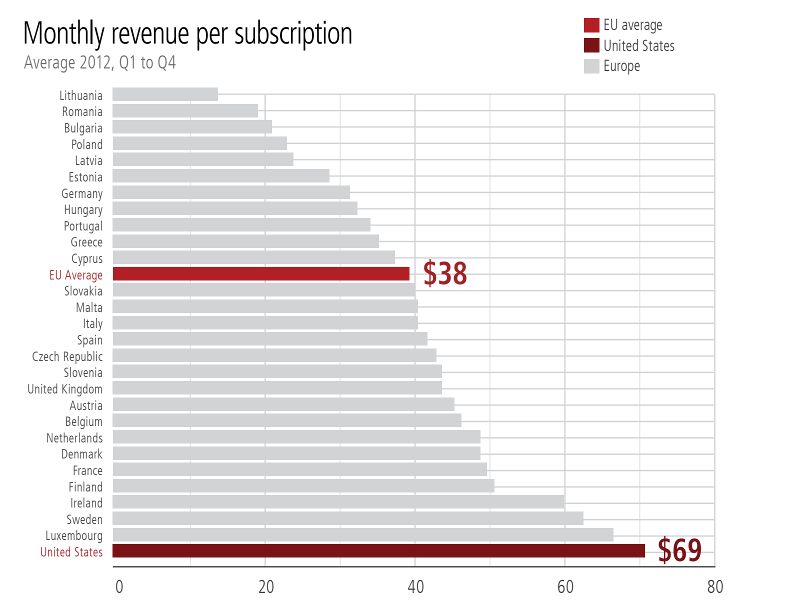
- Market fragmentation prevents EU carriers from capturing economies of scale and scope. America's two largest carriers are each larger than the three largest EU carriers combined.
- Market fragmentation limits consumer choice: it explains, at least in part, why Apple chose not to make the iPhone 5 compatible with some EU mobile networks.
- Efficient consolidation would provide incentives for investment, facilitate a more integrated mobile wireless ecosystem and improve consumer welfare.

The mobile wireless marketplace is extremely dynamic. While the current performance of the EU market is below par, sensible policy reforms could bring rapid improvement, creating substantial benefits for EU consumers and spurring accelerated economic growth.

Source: GSMA, 'Mobile Wireless Performance in the EU and the US', May 2013


Mobile data average connection speeds
By region, 2012 and projected 2013–2017

Source: Cisco VNI Mobile Forecast (2013)


Monthly revenue per subscription
Average 2012, Q1 to Q4

Source: GSMA Intelligence

Environment and Climate Change

Background

As mobile use expands, so does the demand for energy, particularly by the network infrastructure. The mobile industry is responsible for a small fraction, less than 0.5%, of global greenhouse gas (GHG) emissions, but energy is a significant cost for mobile operators, especially in emerging markets.

An analysis of 65 mobile networks showed that total network energy consumption increased only 4% from 2010 to 2011, despite considerable growth in mobile traffic and connections. Total energy per unit traffic declined by approximately 30%, and energy per connection declined by 3%.

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

The European Union, 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?

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?

Does mandated carbon accounting generate sufficient benefit, when there is no common, agreed methodology?

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 the 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, and 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 US$15 billion on energy use annually, energy efficiency and emission reduction are strategic priorities for them globally.

The GSMA's Mobile Energy Efficiency Benchmarking service enables network operators to evaluate the relative energy efficiency of their networks. Currently 35 mobile operators participate in the service, accounting for more than 200 networks and over half of global mobile subscribers.

The GSMA's Mobile Energy Efficiency Optimisation service uses the benchmarking results in conjunction with site audits and equipment trials to analyse the costs and benefits of energy- and emission-reduction actions, and roll out the most attractive solutions.

The GSMA is collaborating with the European Commission and the International Telecommunication Union (ITU) on standardisation, including methodologies to assess environmental impact. The Mobile Energy Efficiency methodology has been adopted in the ITU recommendation for environmental impact assessment of ICT networks and services.

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, promotes the use of renewable energies such as solar and wind at mobile network towers in remote, rural areas.

> *Creating a greener and more sustainable economy means transitioning from the resource-intensive physical infrastructure of the 20th century to the more efficient information infrastructure of the 21st century. Broadband has significant potential to help shift the world towards a low-carbon economy and address the challenge of climate change.*
>
> — The Broadband Commission for Digital Development, April 2012

Resources
Mobile Energy Efficiency on GSMA.com
Mobile's Green Manifesto 2009 and 2012 update
GSMA Green Power for Mobile
GeSI Smart2020 analysis
Broadband Commission: Leveraging Broadband for Sustainable Development
Broadband Commission: Linking ICT with Climate Action
ITU-T and Climate Change

Case Study

A Green Power Feasibility Study for Airtel Madagascar

Globally, a 16% increase of 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 power-source 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% 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% 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% reduction of 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.

Although most developed countries now have fully competitive international telecommunications markets, many in Asia Pacific, the Middle East, Africa and Latin America have yet to liberalise IGWs, and monopoly supply and pricing continue.

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 rollout.

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.

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 macro-economic benefits by lowering the cost of business and facilitating trade, 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% 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.

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
ZDnet: Could Tower-Sharing Be the Solution to Rural Networks' Problems?
ITU: Mobile Infrastructure Sharing
Article: Indus Towers — The India Way of Business

Deeper Dive

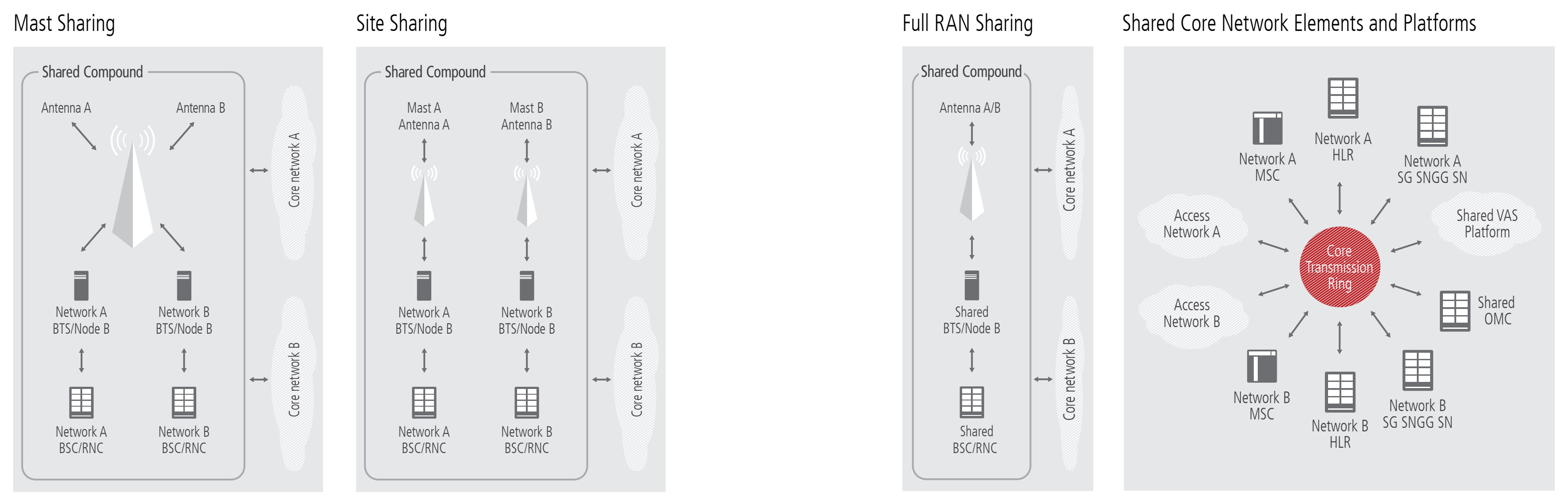
Types of Infrastructure Sharing

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



Mast Sharing

Site Sharing

Full RAN Sharing

Shared Core Network Elements and Platforms

Source: GSMA

Intellectual Property Rights — Copyright

Background

The emergence of the internet as a place for buying, sharing and downloading content has created challenges for policymakers and stakeholders, including combatting piracy, stimulating demand for legal content offers, reforming content licensing and clearly establishing consumer rights. Copyright is the basis for creative industries, collecting societies and artists to earn income from audio and visual work.

In the debate on piracy, mobile operators face the prospect of being liable for any illegal content transmitted over their networks, complying with burdensome monitoring obligations or disclosing user information without a court order. Several countries impose obligations on ISPs to cooperate with rights holders in fighting piracy. In Europe, most EU Member States have introduced copyright levies on devices such as MP3 players and mobile phones that could be used to copy and share protected content.

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 oppose content licensing reform and defend national licences.

In an attempt to modernise existing IPR rules in the EU, several legislative measures have been taken recently or are currently underway. In February 2014, the EU adopted a "Directive on collective rights management and multi-territorial licensing of rights in musical works for online uses" to be transposed into national law by April 2016. In December 2013, the European Commission launched a public consultation with a view to reviewing and modernising EU copyright rules. The response was overwhelming, but the release of a white paper on copyright was postponed. In July 2014, the newly elected President of the European Commission, Jean-Claude Juncker, outlined his political guidelines for the next Commission saying that he will "take ambitious legislative steps towards a connected digital single market" among others by "modernising copyright rules in the light of the digital revolution and changed consumer behavior."

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

We support multi-territorial licensing of audiovisual works and encourage effective competition of collecting societies by enabling choice for creators and users of intellectual property.

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. Current uncertainties over the direction of future licensing practices of collecting societies and the reciprocal agreements between them hold up the development of new business models and delay putting new content offers on the market.

Resources

Public Consultation on the review of the EU copyright rules

Directive on collective management of copyright

GSMA consultation response on EU Property Rights Enforcement Directive

Deeper Dive

The Economic Importance of Copyright

Copyright industries are defined by the World Intellectual Property Organisation (WIPO) as those industries in which copyright plays an identifiable role in creating tradable private economic (property) rights, and income from the use of these economic rights. This classification defines copyright industries in four groups:

- Core industries, which exist to create copyright materials
- Dependent industries, which manufacture equipment that facilitate copyright activity
- Partial industries, which don't create copyright but are dependent on it
- Support industries, which distribute copyrighted material

The original intention of copyright was to encourage the development of new creative work. It was a system put in place to stimulate incentives for artistic production. Copyright is still a critical foundation for the creative industries, and it is these industries that are most impacted by copyright infringement, in particular commercial-scale piracy, with counterfeiting having a greater impact on the partial copyright industries. Frontier Economics estimated the total value of all counterfeiting and piracy globally was between $455 billion and $650 billion in 2008, with digitally pirated goods estimated to be about 10% of the total value.

Classification	Example Industries
Core copyright industries	Literature, music, theatre, film, video, radio, photography
Copyright-dependent industries	TV sets, CD players, games equipment, photocopiers
Partial copyright industries	Household goods, footwear, apparel, museums, libraries
Non-dedicated support industries	Retailing, transportation, telecommunications

In the digital economy, copyright continues to perform the critical function of encouraging new works but also has a wider impact, playing a significant role in fostering innovation; the impact of copyright is therefore now much wider than the creative industry alone. Digital technologies, the companies that exploit them and the business models they facilitate are all potentially impacted by copyright.

Case Study

France's HADOPI Law Fails to Address Illegal File Sharing

In 2009, the French government passed a controversial law designed to curb illegal online file sharing and encourage its citizens to obtain copyrighted material legally. A government agency was created to administer the law, known as HADOPI, which imposed a 'three strikes' rule for copyright infringement.

The law required participation by internet service providers (ISPs), including mobile network operators. Once an offending internet subscriber was identified and an initial warning email sent, the ISP was required to monitor the internet connection. If a second and third offense were detected, the ISP would be required to suspend the connection for up to a year. Other ISPs would be required to refuse service to any internet user who was blacklisted in this way.

Despite its laudable goal of protecting the rights of content creators and publishers, HADOPI was fraught with controversy, largely due to concerns about government heavy-handedness and individuals' right to privacy. Shortly after the law was enacted, the French Constitutional Council ruled that access to online communications services is a basic human right, and an individual's internet access cannot be suspended without a judge's specific order. The council also raised concerns about HADOPI as a monitor of internet use. The law was revised and subsequently approved in October 2009.

In place for more than three years, HADOPI was ultimately judged in a government report to have had no effect on consumer behaviour, and had failed to benefit rights holders at all. Under the law, only one internet subscriber was ever barred from the internet — for 15 days — for failing to respond to the warning notices, while the financial costs of applying the HADOPI law amounted to €12 million.

The law was annulled by the government in June 2013, as its penalties were deemed disproportionate. More generally, legal protection of copyright under the French code of Intellectual Property is unaffected.

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 the European Union, roaming regulation has been in place since 2007. The latest regulation requires European mobile operators to provide wholesale roaming access services to alternative roaming providers, enabling them to offer competing retail roaming service within Europe. In regulating roaming access in this way, the EU seeks to increase competition, with the aim of removing the need for price cap regulation.

In December 2012, during the revision by the ITU of the International Telecoms 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.

Bill shock and certain high roaming prices have also attracted the attention of international institutions such as the OECD and the 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

International mobile roaming 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 Information Paper: Overview of International Mobile Roaming
Press Release: GSMA Launches Data Roaming Transparency Initiative
Roaming on GSMA.com

Case Study

Roaming Regulation in the EU

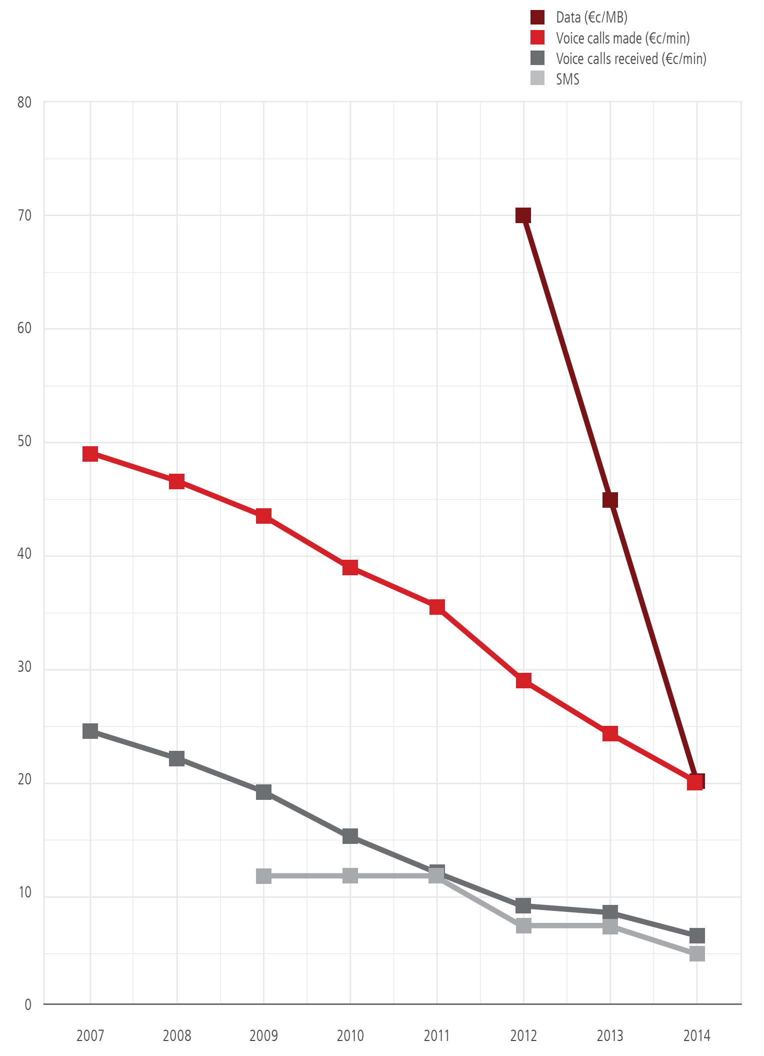
Following six years of information requests and public consultation, the first EU roaming regulation was proposed by the European Commission in 2006. The debate centred on the need for retail price controls and the legitimacy of the use of the EU legal framework for the Single Market. The regulation, which entered into force on 30 June 2007, obliged operators to introduce a Eurotariff for roaming within Europe as the default roaming plan. The regulation set Eurotariff and wholesale price ceilings following a downward glide path.

This intervention was followed by a second roaming regulation in 2009, which extended and lowered the existing caps on voice calls and extended them to also cover SMS (wholesale and retail) and data transfers (wholesale caps only). It also implemented a number of measures to increase the consistency and transparency of billing for these services, including per-second billing, the cut-off facility on roaming data charges at monthly €50 by default. Customers traveling to another Member State receive an automated message of the charges that apply for roaming services.

Although the third wave of regulation, which came into force in July 2012, continued the price cap regime for a transitory period with new retail price caps for data services, it also introduced structural measures, with the aim of steering away from indefinite retail price regulation and to progress to a sustainable, long-term, market-based approach. The competition-enhancing structural measures ensure that the market is open to different types of providers by mandatory wholesale access from 2012, and on the other hand they increase consumers' choice by allowing them to purchase roaming as a stand-alone service from 2014. Transparency and safeguard mechanisms were extended to EU customers roaming outside the region.

Evidence from innovative roaming offers suggest that market dynamics will deliver roaming prices close to domestic rates in a few years' time, driven in particular by the move from voice to more price elastic data usage. Nevertheless, in the Connected Continent proposals currently being debated by EU co-legislators, roaming prices are again on the agenda.

Regulated retail roaming prices within the EU (€c)



Source: GSMA

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?

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 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 model. Unsignaled, unanticipated alterations to these rates have a negative impact on investor confidence.

We believe 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.

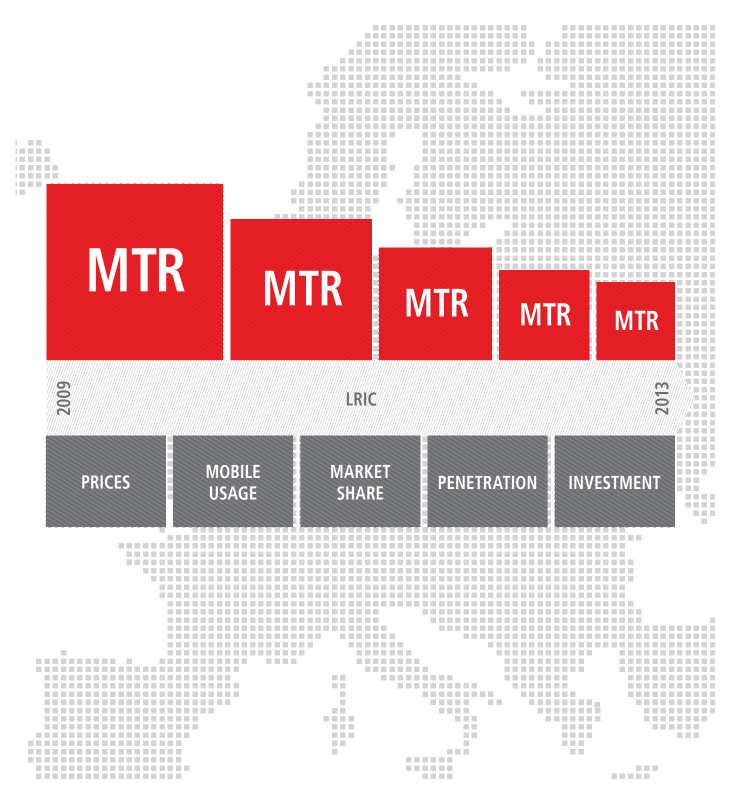
> *Intervening in a competitive market is far more complex and challenging than the traditional utility regulation of the kind normally applied to monopolies in gas, electricity and fixed-line telecommunications. With mobile, every action is more finely calibrated. The benefits of intervention are more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

Resources
Report: The Impact of Recent Cuts in Mobile Termination Rates Across Europe
Report: The Setting of Mobile Termination Rates
Report: Comparison of Fixed and Mobile Cost Structures
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 change, often unpredictably. The available bandwidth also can 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 bandwidths. 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 for 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. However, within the context of a single traffic type, operators should not discriminate in favour of any one content provider.

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

Net Neutrality on GSMA.com

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-appropriate 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

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 specific towers, strategic sharing alliances, formation of joint infrastructure companies between mobile operators or via independent companies that provide 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: The Rise of the Tower Business
Financial Times: 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 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, not all of which are under the control of operators. Defining specific quality targets is neither proportional nor practical.

Some of the factors affecting the quality of service are beyond the control of operators, such as the device type, application and propagation environment.

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 Latin America: QoS

GSMA Response to the EC Consultation on Traffic Management, Transparency and Switching

Deeper Dive

A Network of Interconnections

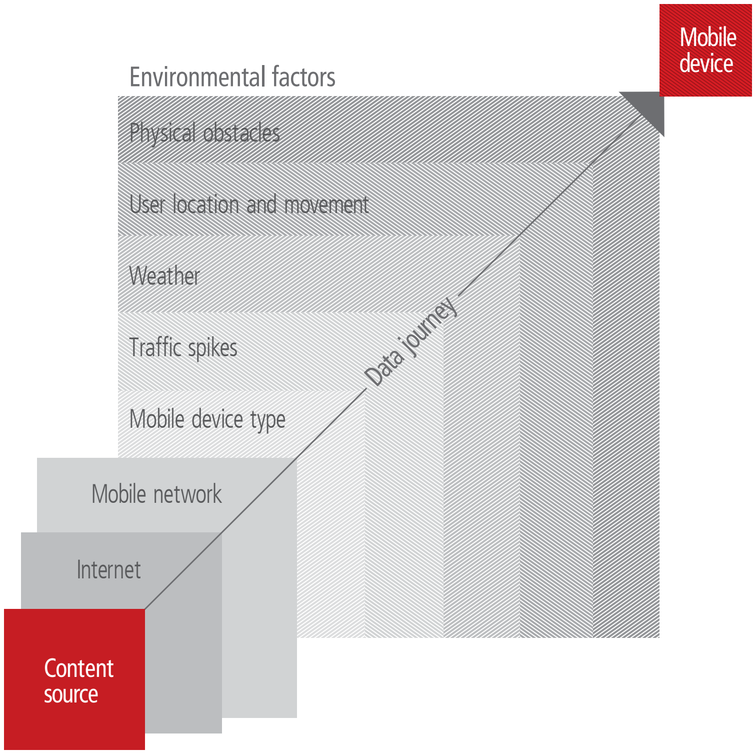
Offering a dependable quality of service is a priority for mobile network operators, as it allows them to differentiate the internet access service they provide from that of their competitors and meet customer expectations. However, mobile operators have little control over many of the parameters that 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 a number of countries are considering establishing a single wholesale network (SWN) instead of relying on competing mobile networks to deliver 4G 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.

No SWN has yet been implemented for mobile but, if it were, it 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 as many countries served by a single mobile network as by competing networks. Only 30 countries today, representing less than 3% 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.

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?

Resources
Report: Assessing the Case for Single Wholesale Networks in Mobile Communications, Frontier Economics, August 2014

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 fact that no SWN has yet been fully implemented is not a coincidence. 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 publically funded SWN could deliver coverage in areas where privately funded competing networks would not be willing to expand into, 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.

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

Debate

Do sector-specific taxes deliver short-term government income at the expense of a country's long-term additional tax revenues resulting from increased economic growth?

> *If we lower taxes, the market will no longer grow 130%, as in the past 15 months. It will grow 250% — it will explode.*
>
> — Paulo Bernardo, Brazilian Minister of Communications

Industry Position

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

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

- Taxes should be broad-based
- Taxes should account for sector and product externalities
- The tax and regulatory system should be simple, easily understandable and enforced
- Different taxes have different economic properties and, in general, broad-based consumption taxes are less distortionary than taxation on income or profits

Discriminatory, sector-specific taxes deter the take-up of mobile services and can slow the adoption of information and communication technology (ICT). Lowering such taxes benefits consumers, businesses and 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.

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

Resources

GSMA: Mobile Taxation Research and Resources
Report: Mobile Taxes and Fees — A Toolkit of Principles and Evidence
Report: Surtaxes on International Incoming Traffic in Africa
Report: Taxation and the Growth of Mobile Services in Sub-Saharan Africa
Report: The Impact of Taxation on the Development of the Mobile Broadband Sector
Report: Global Mobile Tax Review 2011

Facts and Figures

Taxes and Fees Burden on Mobile Services

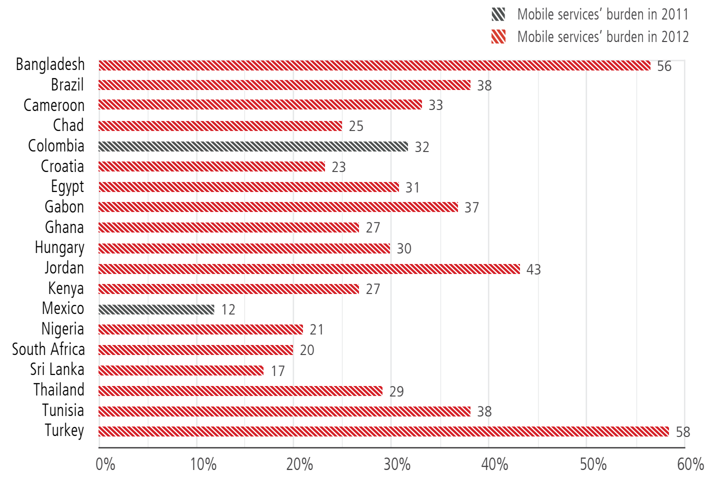
Mobile operators have repeatedly raised concerns that their customers are facing an undue burden from taxation, compared to other goods. The taxation and fees burden on the mobile sector consists of a wide range of charges. On the consumer side, this includes taxes on handset purchases and connection activation, as well as calls, messages and data access.

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. 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 consumers or a combination of the two.

Research by Deloitte for the GSMA revealed that, in 11 selected markets, mobile services saw an average annual increase in the tax and fees burden between 2008 and 2012. The average annual growth of the taxes and fees burden on mobile services across all markets is 2.1 per cent. Within these countries, the burden appears to have increased the most in Bangladesh, with an average annual rate of eight per cent, while Jordan has seen the second highest increase in the burden of around 7.7 per cent on average.

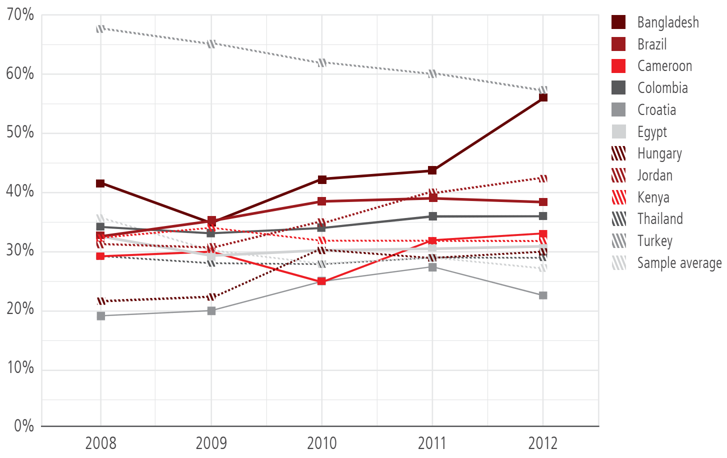
Moreover, the gap between telecoms and other sectors appears to be growing over the same period. The burden on mobile services has increased at an average of 2.1 per cent per year, yet the overall tax burden in the countries considered as a percentage of gross domestic product (GDP) has on average declined at an annual rate of -0.2 per cent.

Average burden on mobile service, selected markets



Source: Deloitte 2014

Tax burden on mobile services over time, selected markets



Source: Deloitte 2014

Universal Service Funds

Background

Universal service — characterised by 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, fewer 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 universal service funds 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 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.

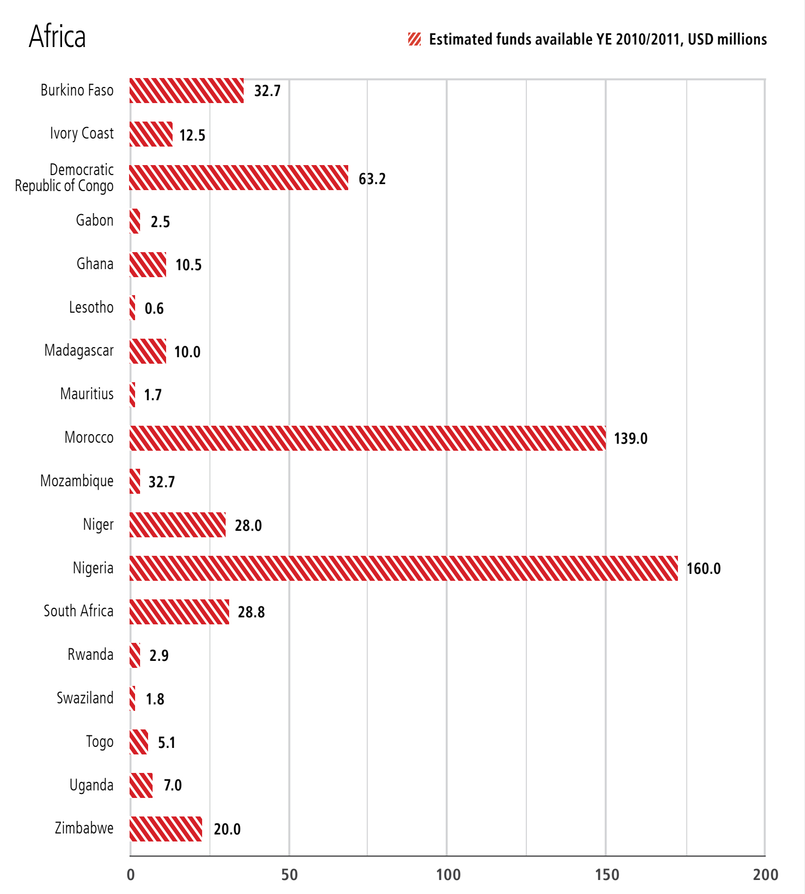
Resources

Report: Survey of Universal Service Funds, Key Findings

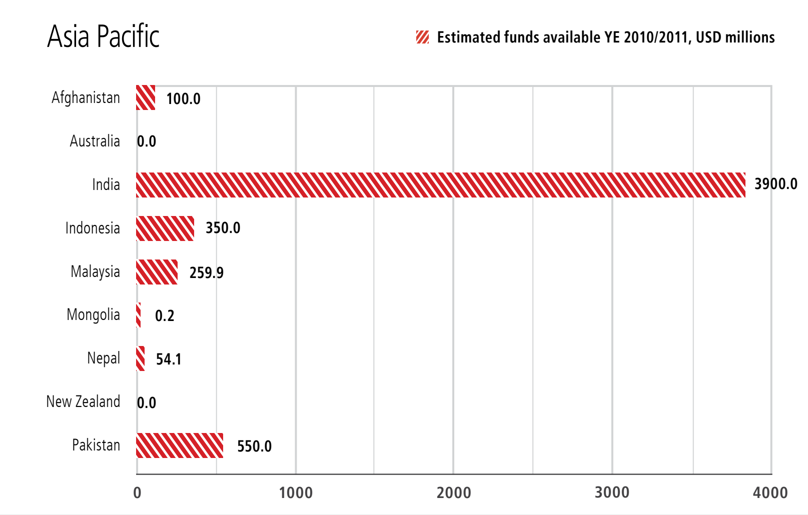
Facts and Figures

Estimated USF Funds Available

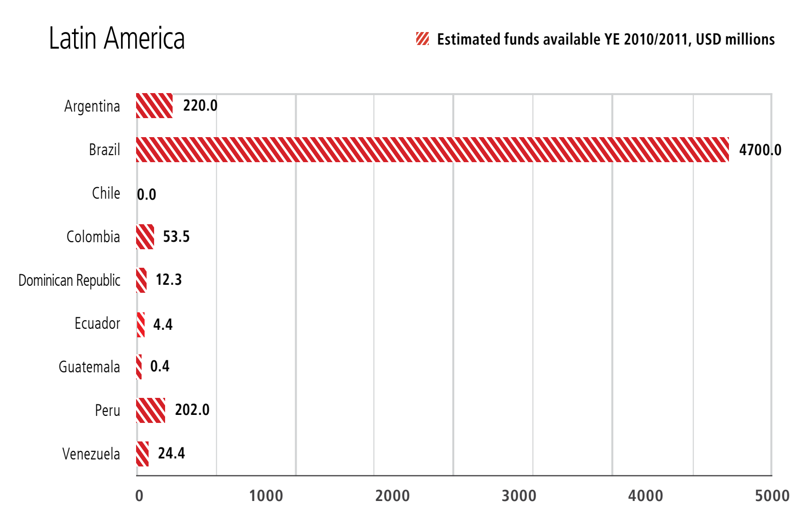
Despite the admirable goals that led to the creation of USFs during the early stages of telecoms liberalisation, there is now considerable doubt about their practicality and efficacy. A large proportion of USF monies collected remain undisbursed, and the structure of many USFs is too rigid to respond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



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



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



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

Spectrum Management and Licensing

Modern life is increasingly mobile, shaped by devices and services made possible by mobile broadband — email and entertainment, mapping and messaging, browsing and banking, social networking and sharing. People are consuming more and more rich content over mobile networks.

To meet this explosion in demand, mobile operators need more spectrum. Sufficient, internationally harmonised spectrum is essential to ensuring the quality of service that consumers and businesses have come to expect, and rely on, from mobile networks.

The GSMA is very active at the national, regional and global levels to advocate for the timely identification and release of more spectrum for mobile broadband. In this regard, we work with national governments and regulators, with regional organisations and the International Telecommunication Union (ITU).

International spectrum allocations are made only through the treaty negotiations that take place as part of the ITU's World Radiocommunication Conference (WRC) process, which happens every three to four years. It can take more than a decade from the start of the ITU process until we see national, commercial deployment of new spectrum bands. Therefore, any spectrum identified as a result of decisions at the WRC 2015 will not come into commercial use until 2025.

The GSMA also serves as a clearinghouse for sector research and market data. Because spectrum management has many facets — including issues such as interference, spectrum auctions and licence processes — the GSMA contributes on behalf of mobile operators to the work of regulators with market projections, analysis, regulatory guidance and policy recommendations based on objective data and recognised best practice. Many of these reports are referenced in this handbook.

2.1GHz Frequency Band

Background

Paired spectrum refers to mobile frequency bands, such as the 2.1GHz band, with separate allocations for uplink and downlink.

The 2.1GHz band, referring to 1.7/2.1GHz (3GPP band 4: 1710–1755MHz paired with 2110–2155MHz) in most countries in the Americas, and 1.9/2.1GHz (3GPP band 1: 1920–1980MHz paired with 2110–2170MHz) elsewhere, has been licensed for 3G mobile services in most markets. However, several countries are yet to release this spectrum for mobile.

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.

Debate

Is there any reason regulators should not have already licensed the entire 2.1GHz band to mobile operators?

How should the licences be awarded to maximise value to society?

Industry Position

The 2.1GHz frequency band should be released in all markets for mobile broadband services, preferably in blocks larger than 2x10MHz per operator.

Releasing the 2.1GHz band for mobile is critical for governments to enable the digital economy and to prevent a growing digital divide.

In certain markets, due to political instability or regulatory uncertainty, investors (including mobile network operators) may not advocate immediate licence allocation; in these cases the optimal timing of spectrum allocation depends on local factors.

Governments should not look to generate excessive fees from the licensing of 2.1GHz spectrum, as this will artificially limit demand, negatively impact network deployment, increase consumer prices and limit the economic benefits. Excessive fees also can result in unsold spectrum, further impeding policy goals of delivering mobile broadband access to everyone.

Resources

Report: Licensing to Support the Broadband Revolution

GSMA Europe response to the public consultation on the introduction of harmonised technical conditions for the terrestrial 2GHz band

Report: Momentum Building in the AWS Band (GVP)

2.6GHz Frequency Band

Background

The International Telecommunication Union (ITU) has identified the 2.6GHz band (2500–2690MHz) as a global allocation for mobile telecommunications.

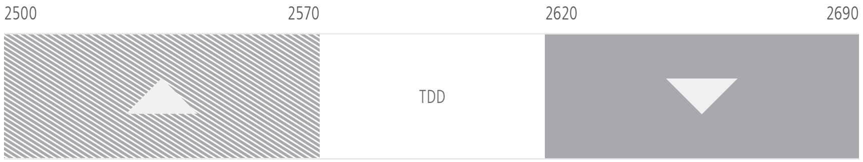
The 2.6GHz radio spectrum band is a 'capacity band' for mobile broadband, well-suited for the next generation of mobile technologies that respond to the soaring demand for data-heavy content, such as video.

The band is identified for mobile in all regions and 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, Chile, Qatar, UAE and the UK recently assigning 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 (e.g., LTE and Wi-MAX).

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 areas.

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 also can impede policy goals of delivering mobile broadband access to everyone.

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

Deeper Dive

Band Characteristics — Capacity vs Coverage

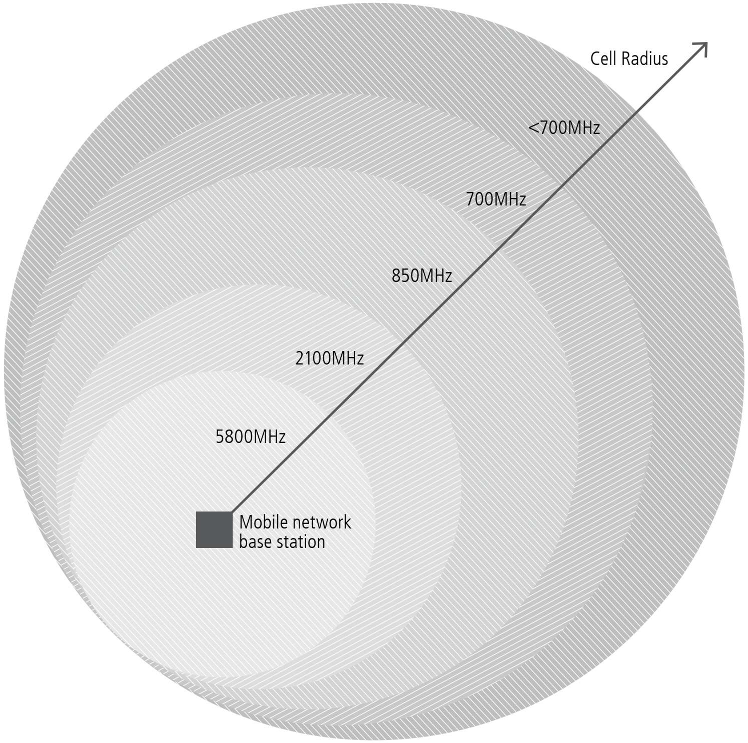
Not all radio frequencies are equal, and mobile network operators require access to a range of frequency bands to cost-effectively offer a high-quality service for different locations with different population densities and different demands on the network.

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.

Effect 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.

Digital Dividend

Background

The Digital Dividend is the spectrum made available for alternative uses following the switch-over from analogue to digital terrestrial television, which is more spectrum-efficient.

For mobile, the freed-up spectrum has made two potential bands available, 790–862MHz (aka the 800 band) used in ITU-R Region 1 (including Europe, Africa and the Middle East) and 698–806MHz (aka the 700 band) used in ITU-R Region 2 (Americas) and Region 3 (Asia Pacific).

Frequencies below 1GHz are ideal for mobile, offering good geographic coverage, improved in-building coverage, reasonable capacity and availability in large blocks for efficient delivery of mobile broadband.

The Digital Dividend is a key enabler for universal broadband access, bringing socio-economic benefits to people in cities as well as rural and remote areas.

Debate

Which services should Digital Dividend spectrum be licensed for, following the switch-over to digital terrestrial television?

What goals should governments try to achieve when relicensing the band?

> *Governments need to raise broadband to the top of the development agenda, so that rollout is accelerated and the benefits are brought to as many people as possible.*
>
> — Dr Hamadoun Touré, ITU Secretary-General, 2006–2014

Industry Position

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

The switch-over to digital television gives terrestrial broadcasters significantly more capacity for additional channels or high-definition television, even when the Digital Dividend is allocated to mobile.

The economic benefits of licensing the Digital Dividend to mobile are far greater than allocating it to any other service.

Regional harmonisation of the band will permit economies of scale (keeping handset costs low) and mitigate interference along national borders.

Governments should not look to generate excessive fees from the licensing of Digital Dividend spectrum, as this will artificially limit demand, negatively impact network deployment, increase consumer prices and limit the potential economic benefits. Excessive fees also can impede policy goals of delivering broadband access to everyone.

It is reasonable for coverage obligations to be employed to ensure efficient use of this spectrum.

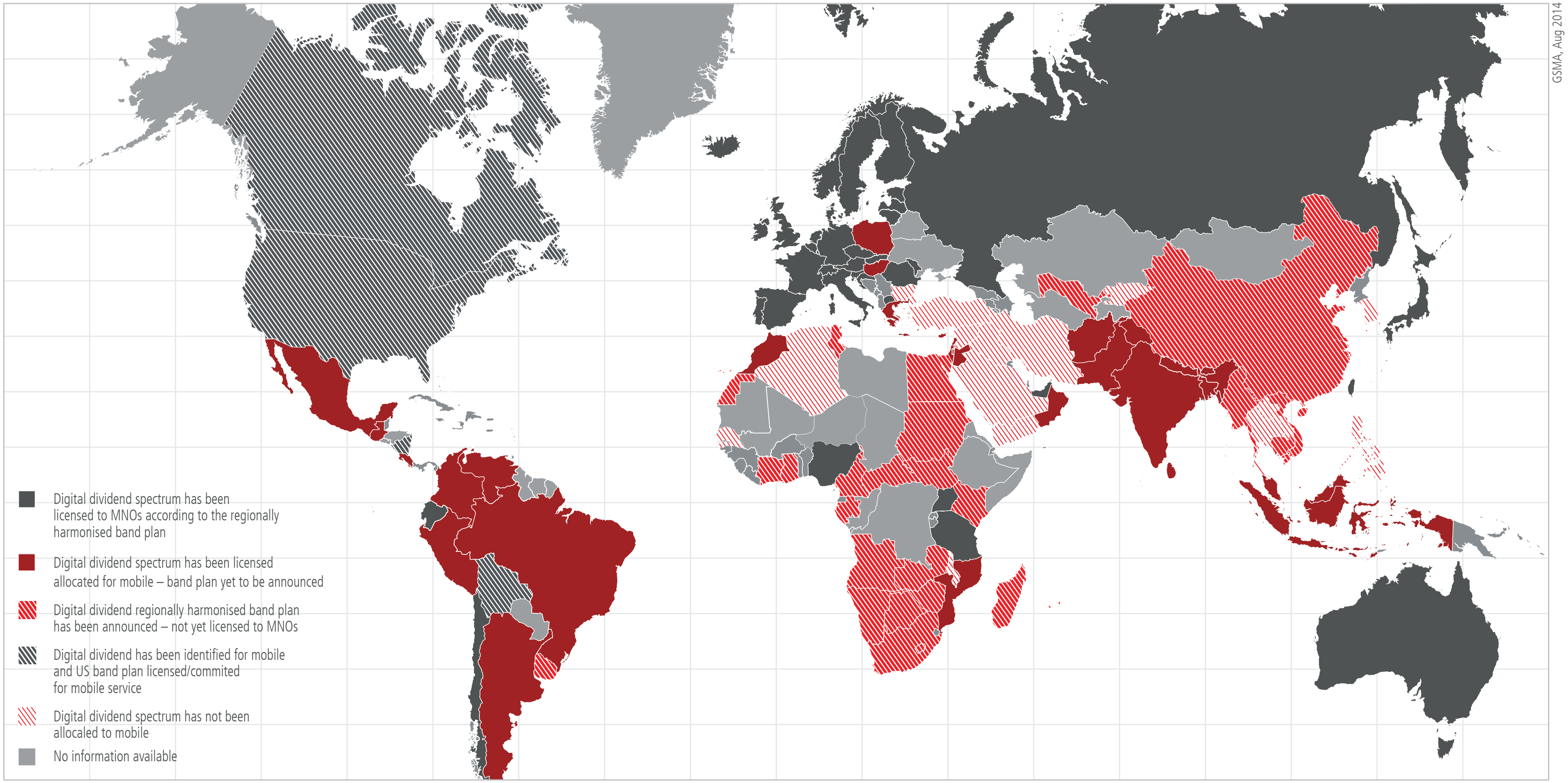
Resources

GSMA Position Paper: Digital Dividend
GSMA Position Paper: Asia Pacific Digital Dividend/UHF Band Plans
Report: Economic Benefits of the Digital Dividend for Latin America
Report: The Economic Benefits of Early Harmonisation of the Digital Dividend Spectrum and the Cost of Fragmentation in Asia
GSMA Digital Dividend Toolkit
Report: Licensing to Support the Broadband Revolution

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.


■ Digital dividend spectrum has been licensed to MNOs according to the regionally harmonised band plan
■ Digital dividend spectrum has been licensed allocated for mobile – band plan yet to be announced
▨ Digital dividend regionally harmonised band plan has been announced – not yet licensed to MNOs
▨ Digital dividend has been identified for mobile and US band plan licensed/commited for mobile service
▨ Digital dividend spectrum has not been allocaled to mobile
■ No information available
GSMA, Aug 2014

* The Digital Dividend on this map refers to the 800MHz band for Europe, the Middle East and Africa, and the 700MHz band for other regions.

Source: GSMA

Digital Dividend 2 Band Plan (EMEA)

Background

The World Radiocommunication Conference (WRC-12) agreed in February 2012 to allocate the 694–790MHz frequency band (aka the 700MHz band) to mobile services after WRC-15. This allocation applies to Europe, including Russia, the Middle East and Africa, known as International Telecommunication Union (ITU) Region 1.

The outcome of the WRC-12 was based on a commitment of most parties to seek harmonisation of that band and the 800MHz band (3GPP Band 20) in Region 1. The allocation does not come into force until WRC-15, giving time for technical studies and for countries to rearrange existing frequency usage.

There are currently several options/approaches for the 700MHz band plan for ITU Region 1.

Debate

Because of overlap between the 800MHz band and the Asia Pacific Telecommunity APT 700MHz band plan, what should the preferred band plan for the region be?

What is the benefit of region-wide harmonisation in Region 1?

Should ITU Region 1 adopt a second Digital Dividend band, which would extend the Digital Dividend band down to 694MHz?

Industry Position

Mobile operators support the proposed 2x30MHz band plan that consists of 703–733MHz (uplink) paired with 758–788MHz (downlink) as the preferred 700MHz band plan for Africa, Middle East and Europe.

This baseline band plan is based on the reuse of the lower duplexer of the APT band plan (i.e., 2 x 30MHz from the APT 2 x 45MHz).

Harmonising the regulatory and technical conditions for the 700MHz band plan in EMEA with the Asia Pacific band plan would maximise economies of scale (keeping handset costs low), mitigate interference along national borders and enable roaming.

Governments should also aim to support the use of the duplex gap for public commercial mobile networks (i.e., supplemental downlink).

However, the mobile industry recognises that some governments may want to consider another option — use of the duplex gap for Public Protection/Disaster Relief (PPDR) mobile broadband applications.

Although governments have options for dedicated PPDR networks outside the 700MHz band, for those that do wish to deploy PPDR within this range, the GSMA recommends that such governmental networks operate outside of the 2x30MHz aligned with the lower duplexer of the harmonised APT band plan.

Resources

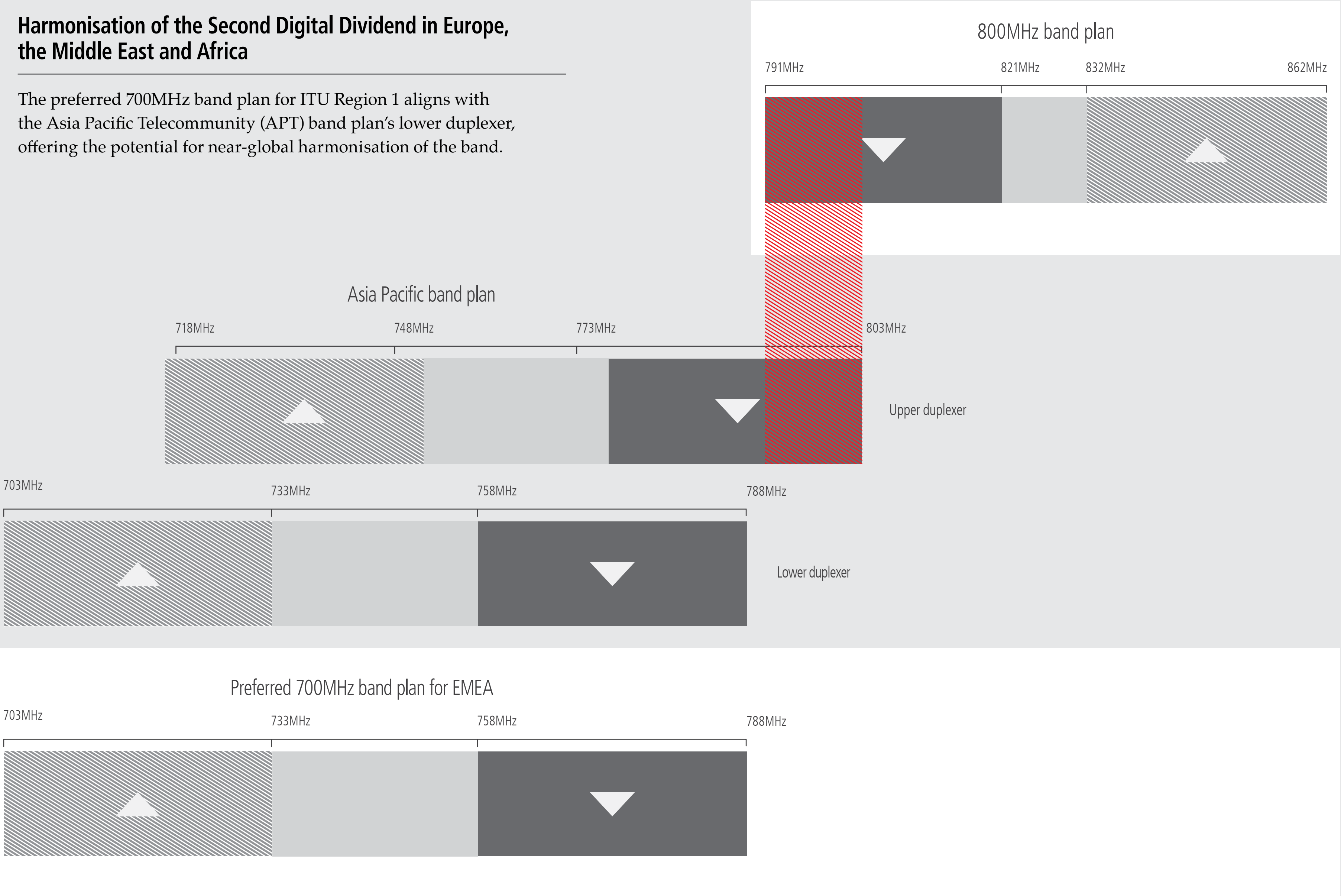
GSMA Public Policy Position on the Preferred Band Plan for Digital Dividend 2 in ITU Region 1

GSMA Welcomes UAE's Decisive Step to Lead Regional Surge in Mobile Broadband

Deeper Dive

Harmonisation of the Second Digital Dividend in Europe, the Middle East and Africa

The preferred 700MHz band plan for ITU Region 1 aligns with the Asia Pacific Telecommunity (APT) band plan's lower duplexer, offering the potential for near-global harmonisation of the band.



Source: GSMA

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.

Licensed shared access 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?

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.

> *The over-eager pursuit of unlicensed sharing models cannot turn a blind eye on the model proven to deliver investment, innovation and jobs — exclusive licensing.*
>
> — Joan Marsh, Vice President of Federal Regulatory, AT&T

Resources
The impact of Licensed Shared Use of Spectrum
GSMA Public Policy Position on Licensed Shared Access (LSA) and Authorised Shared Access (ASA)
Qualcomm: The 1000x Data Challenge
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 offer 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?*

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 transmitter and receiver RF performance are necessary.

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

> ***The increasingly congested skies above our heads require careful management and monitoring, on a global basis, with intensive cooperation and discussion to avoid the risk of interference. That is one of the most important parts of ITU's work, as the sole global agency charged with managing the world's shared radio spectrum and orbital resources.***
>
> – Dr Hamadoun Touré, Secretary-General, ITU

Resources
Technical paper: Managing Radio Interference
GSMA briefing paper on WRC Agenda Item 1.17 — broadcast interference
Fact sheet: 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 service using the 800MHz Digital Dividend band does not interfere with television broadcasting. Nevertheless, concerns continue to be aired in most markets until the actual roll-out of the mobile service. Now that mobile network operators in several countries have begun to deploy LTE networks using Digital Dividend spectrum, these concerns can be largely 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 was 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

at800 is the joint venture that was set up in 2012 by mobile operator licensees in the UK 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 £30m per 5MHz lot acquired. at800 was then responsible for collecting information about each operator's LTE800 rollout 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 30 January 2014, at800 had handled more than 175,000 calls from viewers, received over 15,000 web enquiries, and responded 2,700 people on social media. For viewers experiencing disruption that is not related to LTE at 800MHz, at800 directs viewers to organisations that may be able to help.

Planning for Future Spectrum

Background

The volume of data moving through mobile networks is rising rapidly — between 2008 and 2013, global mobile data traffic grew 45-fold.

This data demand is being driven by the growing number of mobile subscribers who are connecting to faster networks and consuming higher-bandwidth content such as video. The ITU's official spectrum demand model assumes that mobile traffic will increase between 44 and 80 times between 2010 and 2020.

In response, mobile operators are investing heavily in new technologies (e.g., LTE and LTE-Advanced) and new network architectures (e.g., small cells). However, such is the speed of data growth that operators will require access to significant additional spectrum in the future to efficiently meet demand. On average, around 1000 MHz of spectrum has been identified for potential mobile broadband use under the ITU's Radio Regulations, which are reviewed every three to four years at the World Radiocommunication Conference (WRC). The ITU predicts that the rate of data growth means an average total of 1340–1960 MHz will be required for mobile broadband by 2020.

The next opportunity to make additional spectrum available for mobile broadband is at WRC-15, where it is set to be the top agenda item.

Debate

How much spectrum will be required by the mobile sector, looking ahead to 2020 or 2025?

What will happen if significant additional spectrum is not made available for mobile broadband at WRC-15?

What frequency ranges are most suitable to meet mobile data demands?

> ***Based on the growth observed between 2008 and 2010, Analysys Mason expects more aggressive growth in total mobile traffic during the period to 2015 than has been observed in previous years… On the basis of recent forecasts, we estimate that mobile traffic will grow at a compound annual growth rate of 42%, to reach 28,000 PB per year in 2015.***
>
> — Analysys Mason, June 2011

Industry Position

The mobile industry will continue to need more harmonised spectrum to deliver the economic and social benefits of broadband.

The outcome of WRC-15 will be the single most important factor determining the future availability of affordable, ubiquitous, high-speed mobile broadband services. The decisions made will impact the wealth, well-being and future prospects of all countries and their citizens.

For example, the mobile industry (both directly and indirectly) created 3.6% of global GDP (equivalent to $2.4 trillion) and directly supported 10.5 million jobs in 2013. This is expected to rise to 5.1% of GDP and 15.4 million jobs by 2020.

By allocating sufficient additional spectrum for mobile at WRC-15, governments will be able to continue supporting existing radio services for as long as necessary, while ensuring they have the flexibility to gradually increase the amount available for mobile broadband when required.

In the absence of new allocations, governments will be constrained in their ability to make new mobile spectrum available as data traffic rises, resulting in a poorer user experience and potentially more expensive mobile services. As it takes about eight to ten years to re-allocate, re-assign and re-license spectrum, it is essential that administrations act now rather than reacting when it is too late to meet growing consumer demand.

GSMA research shows an additional 600–800 MHz should be made available for potential future mobile use by 2020 — these findings are in line with the ITU's own predictions. This spectrum should comprise a mixture of coverage (i.e., lower frequency) and capacity (i.e., higher frequency) bands to ensure networks can provide high-speed, cost-effective services in rural and metropolitan areas, as well as deep inside buildings.

The spectrum must also be harmonised globally, or at least regionally, to drive the economies of scale required for low-cost consumer devices and to enable roaming and minimise cross-border interference.

Resources

GSMA: Mobile Spectrum Requirements and Target Bands for WRC-15

GSMA: Data Demand Explained

Facts and Figures

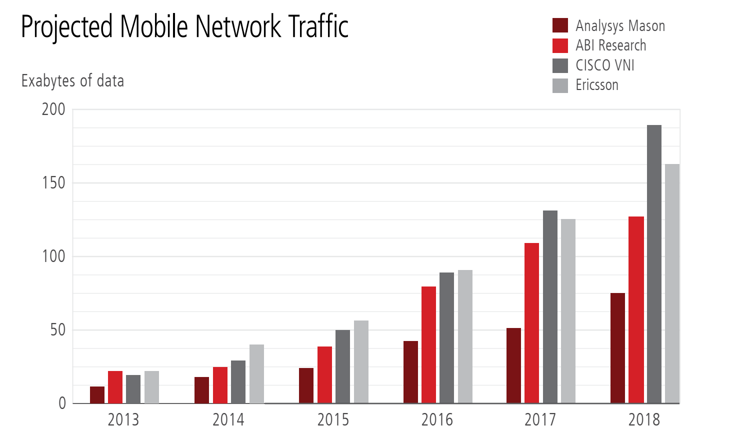
Global Data Traffic Forecasts from Multiple Sources

The growing volume of data traffic running over mobile broadband networks poses a significant challenge for the industry. Although mobile data traffic has grown dramatically in the past five years, there are plenty of reasons to believe there is far more growth still to come.

In the next ten years, billions more people and machines will use mobile networks to access online services and connect with each other. At the same time, smartphones will become increasingly ubiquitous and each new smartphone user will send and receive far more data than they did with their previous handset.

The growing popularity of high definition video and other rich multimedia content is going to fuel a further surge in mobile data traffic. While market forecasts vary significantly, there is a consensus that the traffic on mobile networks is going to grow dramatically for the rest of this decade.

By 2020, there are expected to be 2.5 billion 4G-LTE connections worldwide, up from 400 million at the end of 2013. As 4G users generate far more data than 3G users that implies a massive increase in traffic over the next six years. Cisco VNI forecast for Japan states mobile traffic will reach 15GB per month per unique subscriber by 2018.



Sources: Analysys Mason, Global Mobile Network Traffic, Nov 2013
ABI Research, Mobile Data Traffic & Usage, July 2013; Note: ABI Research data for 2014–2016 has been estimated
Cisco VNI Mobile Forecast, Feb 2014; Ericsson Mobility Report, June 2014

Deeper Dive

Potential Sources of New Mobile Spectrum

To meet rising data demand, the mobile industry is targeting new spectrum allocations for the mobile service in a portion of the following frequency bands at WRC-15:

	Band attributes	Existing uses	How to accommodate mobile
Sub 700MHz 470–694/8MHz	Extremely important for delivering high speed mobile broadband everywhere	Mostly broadcasting	Broadcasters use more spectrum-efficient technology, while IPTV, satellite, cable and LTE will complement.
L Band 1300–1400MHz 1427–1518MHz	Good general-purpose band for coverage and capacity	Aircraft control systems (i.e., telemetry); military and civilian radar; fixed links (e.g., for business); satellite phones; earth observation satellites	1452–1492MHz is largely unused and ideal for global harmonisation; radar and aeronautical mobile telemetry services could use spectrum more efficiently.
2.7–2.9GHz	Excellent capacity band; could use existing 2.6GHz base stations	Air traffic control; military radar	The band is underused and could support mobile, in part. Large exclusion zones are not needed.
C Band 3.4–3.8GHz 3.8–4.2GHz	Excellent capacity band; supports the fastest services; suitable for urban areas or small cells	Fixed satellite services (e.g., satellite TV and broadband)	Satellite providers can use a smaller portion, as they use other bands in the tropics with new technology. Large exclusion zones are not needed.

Source: GSMA

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 alternative 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?

> ***The countries that get their spectrum policy right will achieve widespread access to affordable and innovative mobile broadband services. Strong communications infrastructure, in turn, brings significant wider economic benefits including in boosting productivity and living standards.***
>
> — Competition Economists Group, 2012

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. Auctions should not be designed to maximise short-term revenue for governments.

Auctions are not the only option available to governments to manage spectrum allocation and should only be used in appropriate circumstances.

Resources

Report: Licensing to Support the Broadband Revolution
GSMA Position Paper: Spectrum Auctions
GSMA Position Paper: Spectrum Licensing

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.

Rather than focusing on revenue maximisation, governments would be wiser to focus on the positive social and economic outcomes generated by widespread mobile service, while assuring an appropriate level of industry competition. Lower, realistic reserve prices for spectrum auctions allow the market to determine the value of the spectrum being released. Following are two auctions where reserve prices played a critical role:

India: Hooked on high reserve prices

In March 2013, Indian telecommunications regulator TRAI conducted an auction of 1800MHz spectrum in four of its national 'circles' as well as 900MHz spectrum in three circles and 850MHz spectrum as a pan-Indian licence. Industry response to the offering was poor, as the reserve prices were deemed to be very high given the nature of the market, with its low consumer tariffs. Reserve prices for the 900MHz lots were set at twice the reserve prices of the 1800MHz spectrum in the same circles, for example. In the end, the auction attracted only one bidder, MTS, which secured 850MHz spectrum for just eight of the 22 service areas.

Australia: The first Digital Dividend spectrum to be left unsold

In May 2013, Australia's auction of Digital Dividend spectrum concluded, leaving one-third of the 700MHz band unsold. The auction, which also included lots of 2.6GHz spectrum, generated AUD$1 billion ($780 million) less than the government had predicted. It was reportedly the first occurrence of any Digital Dividend spectrum being left unsold. The Australian government has since come under fire for setting the reserve price unrealistically high at $1.43/MHz/population. Of the country's three incumbent mobile operators, Telstra and Optus bought less of the 700MHz spectrum than they were allowed to under the auction rules, and Vodafone Hutchison Australia chose not to bid at all.

In the words of GSMA Director General Anne Bouverot, "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 by any mobile operator. They are used by governments and regulators to manage the allocation of spectrum during auctions. The intention is to ensure effective competition and to prevent existing operators from using their economic strength to secure large spectrum assets, which could give them a competitive advantage in the future.

Spectrum caps are increasingly used by regulators in auction rules to encourage spectrum reallocation and to balance operator portfolios.

New entrants and players with fewer spectrum assets 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?

Are spectrum caps an appropriate way to address market dominance?

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.

Spectrum caps, when applied without discrimination among the operators, distribute spectrum among market players and, potentially, new entrants. If imposed, they 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.

Market dominance should not be addressed through spectrum caps, but through antitrust measures.

Resources

Report: Licensing to Support the Broadband Revolution
Report: Mobile Broadband, Competition and Spectrum Caps
Article: Forbes.com, 'Sending the Wrong Signals to the Wireless Marketplace'

Case Study

Assessing the Impact of Spectrum Caps in Chile

In September 2009, Chilean regulator Subtel licensed 90MHz of the AWS (1.7–2.1GHz) spectrum band, divided into three blocks, for national mobile service.
In doing so, Chile became the first Latin American country to license this band.

The Chilean Supreme Court authorised Subtel to impose a spectrum cap of 60MHz, effectively excluding the three incumbent mobile network operators — Movistar (Telefónica), Entel and Claro (América Móvil) — all of which were at or near the 60MHz threshold with their existing spectrum portfolios.

Cable television company VTR won block A of the AWS spectrum with an offer of US$3.02 million, and Nextel won blocks B and C, paying US$14.7 million. Both operators were required to deploy services within one year.

"The entry of two new companies will increase competition in the mobile phone and internet business, which is good news for 15 million Chileans," transport and telecommunications minister René Cortázar told reporters at the time.

With the benefit of hindsight, was the spectrum cap an effective strategy to increase competition and benefit citizens? Not entirely. Despite the requirement of a swift roll-out of services, the new entrants were unable to launch their 3G mobile service until May 2012, one and a half years after the October 2010 deadline.

Nor has the competitive landscape been dramatically altered, as VTR and Nextel together control only 1.3% of the market share, nearly three years after the AWS spectrum licences were awarded. The government is now considering allowing secondary market for spectrum, as some companies are not using all of the spectrum in their hands.

Company	Subscribers		Market Share*		Spectrum Holdings	
	Q3 2009	Q2 2013	Q3 2009	Q2 2013	Before	After
Enter	6,126,037	10,141,135	36.64%	37.36%	60MHz (35.0%)	60MHz (23%)
Claro	3,302,000	6,275,000	19.75%	23.12%	55MHz (32.5%)	55MHz (21%)
Movistar	7,255,400	10,377,100	43.39%	38.23%	55MHz (32.5%)	55MHz (21%)
Nextel	38,000	208,100	0.23%	0.77%	–	60MHz (23%)
VTR	–	140,100	–	0.52%	–	30MHz (12%)

*The 2.6GHz band was licensed in June 2012 (40MHz for Entel, 40MHz for Claro and 40MHz for Movistar).

Source: GSMA Intelligence, August 2013

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. This process culminates at the World Radiocommunication Conference, which takes place every two to three years and makes binding decisions regarding the use of the spectrum around the world.

> *A lot more harmonised spectrum is required if mobile broadband in sub-Saharan Africa is to provide sufficient capacity to users at affordable prices. Currently, mobile operators in a typical sub-Saharan African country have access to around 360 MHz of spectrum between them for mobile services. In contrast, operators in many high-income countries have access to 550 MHz of suitable spectrum.*
>
> — Plum Consulting, 2011

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 to going it alone.

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

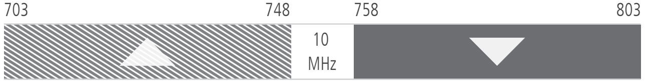
Resources

Report: The Economic Benefits of Early Harmonisation of the Digital Dividend Spectrum and the Cost of Fragmentation in Asia
Report: The Benefits of Releasing Spectrum for Mobile Broadband in Sub-Saharan Africa
Report: Economic Benefits of the Digital Dividend for Latin America

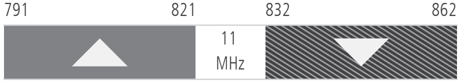
Deeper Dive

Internationally Identified Mobile Spectrum

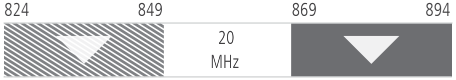
Coverage bands (<1 GHz)



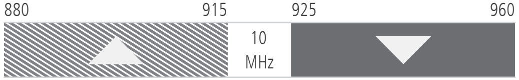
The 700 band: 2x45 MHz



The 800 band: 2x30 MHz

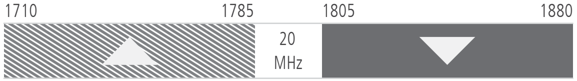


The 850 band: 2x25 MHz

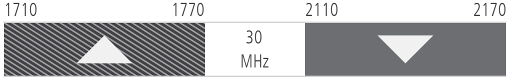


The 900 band: 2x35 MHz

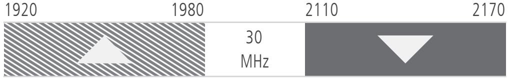
Capacity bands (>1 GHz)



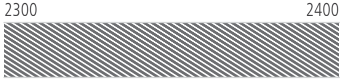
The 1800 band: 2x75 MHz



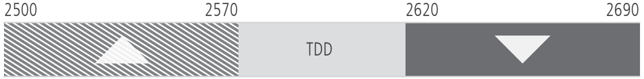
The AWS band: 2x60 MHz (including extension)



The 2100 band: 2x60 MHz



The 2300 band: 100 MHz



The 2600 band: 2x70 MHz with 50 MHz unpaired TDD

Identified Mobile Spectrum by Region

Region 1 – EMEA	800		900	1800		2100	2300	2600
Region 2 – Americas	700	850	900	AWS	1800	2100		2600
Region 3 – Asia Pacific	700	850	900	1800		2100	2300	2600

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
Position Paper: Renewal of Spectrum Usage Rights
Report: Licensing to Support the Mobile Broadband Revolution

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 policy — when supported by a stable, predictable and transparent regulatory regime — can dramatically raise the attractiveness of markets to investers.

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 5- to 10-year view and include a comprehensive and reasonably detailed inventory of current use.

Restrictive licence conditions limit operators' ability 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
Report: Licensing to Support the Broadband Revolution
GSMA Position Paper: Spectrum Licensing

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 mobile network 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 WWbe 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
Position Paper: Spectrum Trading
GSM Europe consultation response: Secondary trading of rights to use spectrum
CEPT/CEE Report: Description of Practices Relative to Trading of Spectrum Rights of Use

Deeper Dive

Spectrum Trading in Guatemala

Guatemala is one of the few countries that permits spectrum trading and where the practice is widespread. In 1996, the Guatemalan government chose to allow spectrum trading in specific liberalised frequency bands. This did not apply to bands that were allocated nationally for government or private amateur radio use, to protect spectrum for vital public services and individuals.

However, the bands allocated to commercial applications such as broadcasting and mobile services were liberalised, allowing licences lasting for 15 years to be leased, sold, subdivided or aggregated at the owner's discretion — and renewed for a longer period on request.

This kind of licence, known as a Título de Usufructo de Frecuencia (TUF), permits use over a specific frequency range in a certain geographical area at certain times, and is subject to power restrictions to prevent interference, especially close to national borders.

As such, the role of the regulator is restricted to adjudicating over interference disputes where mediation has failed, as well as managing non-liberalised government spectrum.

The TUF allocation process:

Interested parties submit formal requests, to which the government must publicly respond within three days.

Third parties have five days to oppose the request.

The only reasons requests may be denied are for violation of an international treaty (surrounding use of the frequency band) or if the existing right to flat frequency range is already held by another.

Assuming the requests meet these criteria, an auction must be announced within 15 days and must take place within 20 days after that.

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 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?

Industry Position

We support a licensing approach that allows any compatible, noninterfering 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 co-exist 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.

> ***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

Resources
Position Paper: Change of Use of Spectrum
Report: Licensing to Support the Broadband Revolution

Deeper Dive

The 1800MHz band: a global refarming success story for LTE

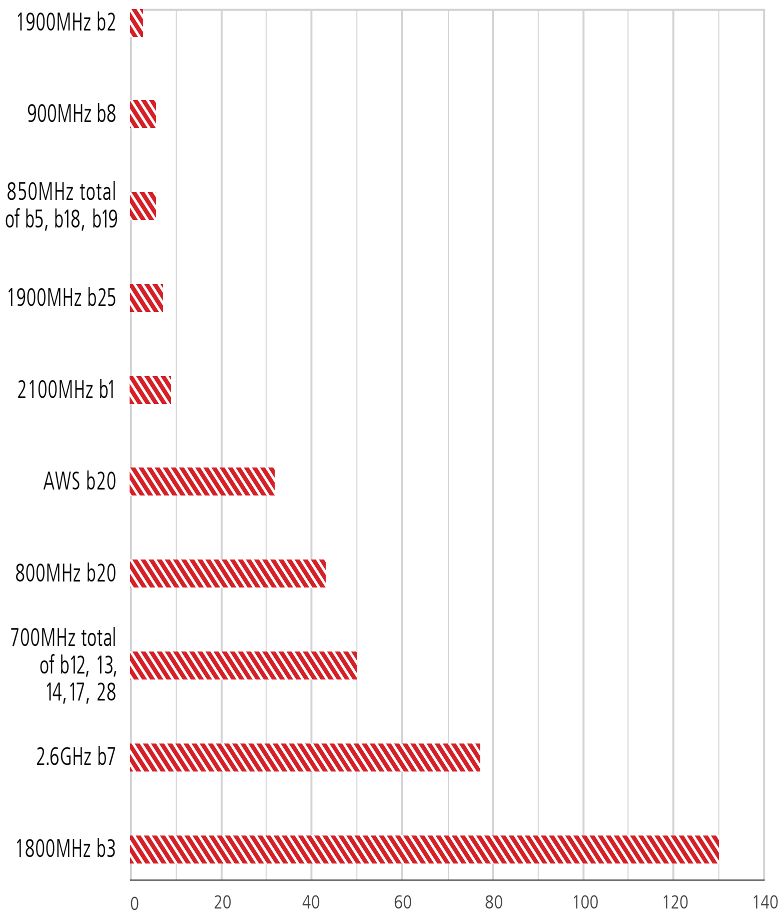
The lack of truly global LTE frequency bands made it difficult to establish a wide range of low-cost devices for the first phase of 4G services. It also prevented widespread international roaming.

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 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), 43% of LTE networks use the 1800MHz band, and over 589 compatible user devices have been announced as of April 2014.

Frequency bands used for global commercially launched LTE deployments



Source: GSMA

TV White Space

Background

The expression 'white space' is used to define the parts of the spectrum that are not used at a given time and geographical location.

Typically, TV white space consists of unused spectrum in the television broadcasting bands (e.g., 470–790MHz in Europe and 470–698MHz in the United States).

There is unused spectrum in these bands mainly because of the necessary geographical separation between television stations of the same channel, as well as parts of the spectrum dedicated to regional television stations that remain unused in certain areas.

Some internet players are advocating globally for use of TV white space for licence-exempt services such as Wi-Fi. 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 kinds of applications can take advantage of TV white space?

In reality, how much TV white space is available?

What licensing regime is most appropriate to get the maximum benefit from spectrum resources for mobile broadband?

Industry Position

Use of TV white space must not jeopardise the future of the UHF band, especially in the case of reallocation for exclusive mobile use.

The use of TV white space must not distort the market through inappropriate regulation. Eliminating the cost of acquiring licensed spectrum to provide cellular-type mobile services could create an unfair advantage.

The TV white space approach is made possible by a spectrum-use database including geo-location data, which cannot offer a predictable quality of service or spectrum availability. For TV white space, there is no *a priori* determination of the spectrum to be eventually accessed.

Interference management remains a top priority. The use of TV white space, on a secondary unlicensed basis, requires careful avoidance of interference with primary users such as existing TV broadcasters, as well as services in adjacent bands.

It is important to consider how to use the Digital Dividend spectrum most effectively to benefit citizens and businesses, and discussions about TV white space should not derail this process.

> *I think that white spaces probably won't prove to be very good, available mobile spectrum to use, so it's likely that people will have to resort to the other unlicensed bands that are already available, such as 900MHz, 2.4GHz and 5GHz.*
>
> — Bill McFarland, Vice President, Technology for Qualcomm (Mobile Europe, 1 July 2013)

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 devices have become indispensable in the digital age. For a vast number of people, mobile phones serve as a personal portal to the friends, family, services and resources they rely on every day. It is essential for the mobile industry, therefore, to deliver safe and secure technologies — complemented by safe and secure mobile apps — that inspire trust and confidence. At the same time, consumers need to be aware of their role in avoiding risks.

Mobile technologies are not immune to the issues faced offline and by other forms of information and communication technology. For example, criminal activities such as online exploitation of children, spamming and device or identity theft existed before the proliferation of mobile technologies. These threats have merely evolved to take advantage of the ubiquity of mobile phones and other mobile devices.

The mobile industry takes consumer protection seriously. The GSMA and its members work with governments, multilateral organisations and non-governmental organisations to address mobile-related threats to citizens by:

- Commissioning research that offers real-world insight and evidence
- Building and participating in cross-sector coalitions
- Defining and promoting global best practice
- Leading technical initiatives

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 2013 report Children's Use of Mobile Phones — An International Comparison reveals that 81% of children aged 8–18 in the countries surveyed use a mobile phone, and 55% 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.

Use of mobile technology offers children new ways to learn, exposes them to people from different segments of society and encourages creativity. Benefits can include:

- Skills for employment
- Enhanced formal and informal education and learning
- Information and services to aid in health and well-being
- Improved social engagement
- Opportunities 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?

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 the ITU's Child Online Protection programme, and actively engages with governments and regulators looking to address this issue.

Through its mYouth programme, 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 generations 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.

> ***I always point to mobile as an exemplary illustration of how self-regulation can achieve results.***
>
> — John Carr OBE, eNacso

Resources
UNICEF: Guidelines for Industry on Child Online Protection
European Framework for Safer Mobile Use
ICT Coalition
GSMA: mYouth
GSMA Report: Children's Use of Mobile Phones, An International Comparison 2013
GSMA Report: Children's Use of Mobile Phones, An International Comparison 2012

Deeper Dive

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 (http://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.

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.

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, Telefónica, Telenor, TeliaSonera and Vodafone.

Facts and Figures

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

Part of a growing body of research into the use of mobile devices by children around the world, Children's Use of Mobile Phones: An International Comparison 2013 focuses on four countries in the Middle East. This research was funded by mobile operators in Algeria, Egypt, Iraq and Saudi Arabia, in addition to a small contribution from the GSMA and continued support from the Mobile Society Research Institute. The report data was obtained through a series of surveys conducted in each country in 2012 and 2013.

55% of all child mobile phone users access the mobile internet This increases to **93%** when looking exclusively at child smartphone users

Children use social networking services more than their parents across all four continents

40% of children on social networking sites have public profiles, though girls are more likely than boys to have private profiles

63% of all children who use the internet through their mobile phone access it between one and five times a day, with **21%** accessing it more than six times a day and only **16%** accessing it less than once a day

57% of parents who have access to parental control solutions used them; content filters are the most popular control method at **56%**

Over **60%** of parents have concerns about children's mobile phone use, with viewing inappropriate sites the highest percentage at **85%**

55% More than half of all child mobile phone users surveyed make use of location based services

72% of children who use social networking services communicate with 'new friends' online

Of those children who access the internet via their smartphones… **85%** of them download or use apps

75% of parents believe that an adult in the family should educate their children about mobile phone use; this is a consistent preference across all countries

87% of children surveyed say that having a mobile phone increases their confidence; this is particularly the case in Saudi Arabia where this figure rises to **98%**

91% of function use is camera features, **88%** music players and **78%** movie players

73% of parents surveyed expressed concern about their children's privacy when using mobile phones, with equal concern expressed for girls and boys

Source: GSMA and NTT DOCOMO

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 classed as a possible human carcinogen by the International Agency for Research on Cancer. Health authorities have advised that this classification means more research is needed, and they have 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 radiofrequency (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, 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 2015.

> *Scientific assessments of risk and science-based exposure limits should not be undermined by the adoption of arbitrary cautionary approaches.*
>
> — World Health Organization

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 RF 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 mobile communication 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 while operating can be well below this value. Differing SAR values do not mean differing levels of safety.

Resources

World Health Organization EMF Project
International Agency for Research on Cancer Monograph on Radiofrequency Fields
GSMA — Mobile Communications and Health
SAR Tick Programme
Article: Dutch Health Authority Finds No Clear Evidence Mobiles Increase Brain Tumour Risk

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, June 2011*

The overall data on brain tumour and mobile telephony do not indicate an effect of mobile phone use on tumour risk, especially not when taken together with national cancer incidence statistics from different countries. There is still only limited data regarding risks of long term use of mobile phones, but compared to the previous report, the evaluated exposure duration has increased to approximately 13-15 years of use. Thus, current scientific uncertainty remains for regular mobile phone use for more than 13-15 years. It is also too early to draw firm conclusions about risk for brain tumours for children and adolescents, but the available literature to date does not indicate an increased risk.
— *Swedish Radiation Safety Authority, 2013*

There are still limitations to the published research that preclude a definitive judgement, but the evidence considered overall has not demonstrated any adverse health effects of RF field exposure below internationally accepted guideline levels.
— *Health Protection Agency (UK), 2012*

Personal Control Over Exposure

Mobile phone users who remain concerned about the effects 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.

using one's mobile while…		
Outdoors	Stationary	In town
generates exposure levels up to…		
68% lower	45% lower	10% lower
compared to…		
Indoors	Travelling	In the countryside

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 safety 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 is currently conducting a risk assessment for radio frequency signals. The results are expected in 2015, including policy recommendations for governments.

> *Current evidence does not confirm the existence of any health consequences from exposure to low-level electromagnetic fields.*
>
> — World Health Organization

Debate

Does using a mobile phone regularly, or living near a base station, have any health implications?

Are there benefits in adopting electromagnetic field (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.

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).

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 health authorities and expert scientists
- Set a national policy covering the siting of masts, balancing effective network rollout with consideration of public concerns
- Verify that mobile operators are compliant with international radio frequency levels using technical standards from organisations such as the International Electrotechnical Commission (IEC)
- 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

EMF-Portal research database
GSMA: Arbitrary Radio Frequency Exposure Limits — Impact on 4G Network Deployment
GSMA: Mobile and Health — independent expert reviews
GSMA: LTE Technology and Health
ITU-T activities on EMF
World Health Organization International EMF Project

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	No
Italy	1/0.1	Approval	Small antennas	Lower limits[g]	Yes
Japan	6	Approval	Small antennas	None	Local
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
Kindgom of Saudi Arabia	4.5	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

Source: GSMA 2014

[a] 50m around hospitals schools and homes for old people
[b] Proposal under public consultation, 2014
[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] WWAdopted 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

Government Access

Background

Mobile network operators are subject to a range of laws and 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 with respect to the privacy of its customers' information.

Legislation often lags behind technological developments; for example, in many cases they apply to established telecommunications operators but not to more recent market entrants, such as those providing internet-based services, such as Voice-over-IP (VoIP) services, video or instant messaging services.

In response to public debate concerning the extent of government access to consumer data, a number of major internet companies publish 'transparency reports' which provide statistics relating to government requests for disclosure of such data.

Debate

What is the right legal framework to achieve a balance between governments' 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 goverments. 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

Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework

Malone v. The United Kingdom, Application No. 8691/79, Judgment of 2 August 1984 of the ECJ

Google Transparency report

Case Study

National Regulatory Approaches to Government Access

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

In the UK, communications service providers must ensure 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). Certain agencies 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. Consequently, the UK and a number of other countries in the European Union are having to review their data retention laws, which required communications service providers to store communications data for up to two years.

Australia's Telecoms Act permits law enforcement agencies to demand communications data without a warrant. The Australian government conducted a review of access to communications data by law enforcement agencies in 2005, but no major changes materialised. In June 2013, Australia's Federal Attorney-General rejected the need for warrants and argued that Australian law enforcement "would grind to a halt" if agents were forced to apply for a warrant every time they wanted to access AustraliansW telecommunications data. Meanwhile, there are voices in Australian government and law enforcement seeking to require communications service providers to retain communications data and give law enforcement agencies systematic access to it.

Deeper Dive

Trending Towards Transparency

Many of the largest internet content providers — including Google, Yahoo!, Microsoft, Twitter, Apple, Dropbox and LinkedIn — publish periodic reports showing the 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.

Recently, some mobile network operators have followed suit. Verizon published its first global transparency report in January 2014, and AT&T, Vodafone and Deutsche Telekom released their first statistics within the next several months. 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 even live voice calls through phone tapping. Although mobile operators often have no option but to comply with such requests, they are increasingly vocal about the 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 images of child sexual abuse (child pornography).

Laws regarding illegal content vary considerably. Some content, such as images of child sexual abuse, are considered illegal around the world, while other content, such as dialogue that calls for political reform, is illegal in some countries while 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.

> *The Mobile Alliance is a prime example of the proactive action industry can take and, together with government and law enforcement support, we can make significant progress in the global fight against child sexual abuse content online.*
>
> — Hamadoun Touré, Secretary General, International Telecommunication Union

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 MNOs?

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 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. (Refer to Intellectual Property Rights — Copyright.)

Resources

GSMA Report: Hotlines — Responding to reports of illegal online content
Mobile Alliance against Child Sexual Abuse Content
INHOPE Website

Deeper Dive

Mobile Alliance Against Child Sexual Abuse Content

The GSMA's Mobile Alliance Against Child Sexual Abuse Content is a voluntary mobile industry initiative to prevent anyone from hosting, accessing or profiting from child sexual abuse content using mobile networks or services. Currently, 15 mobile operator groups and four independents are alliance members, covering approximately 1.2 billion mobile subscribers in 67 countries.

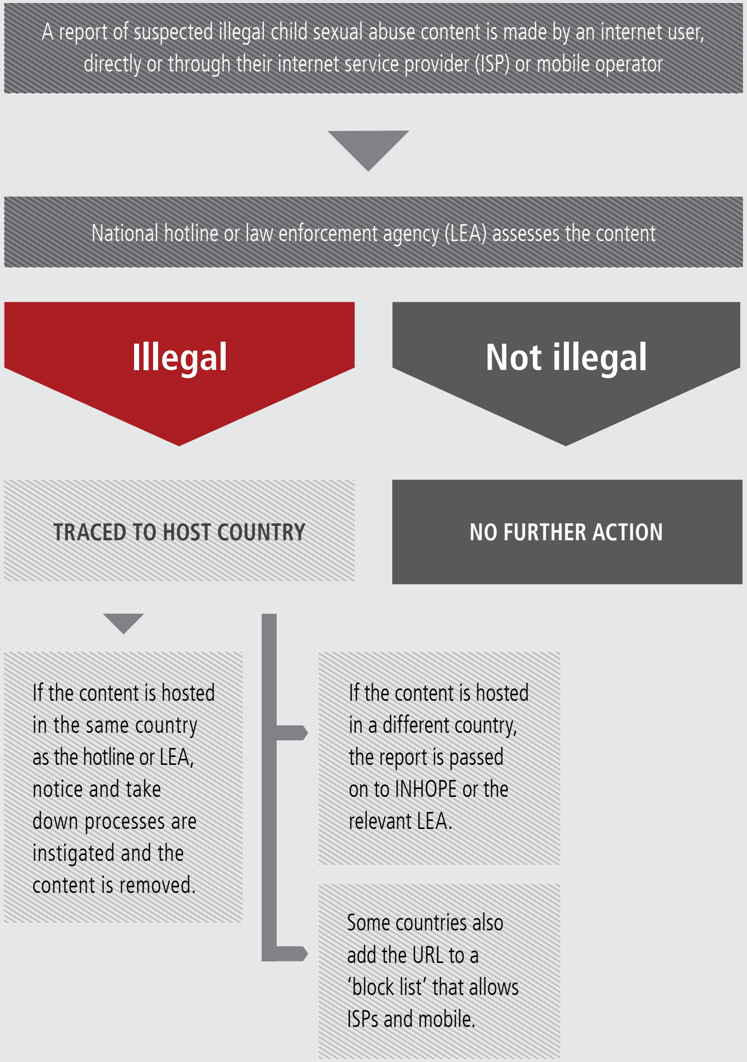
Through a combination of technical measures, co-operation and information sharing, the Mobile Alliance is working to stem, and ultimately reverse, the growth of online child sexual abuse content around the world.

Alliance members have made the commitment to:

- Implement technical mechanisms to prevent 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

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. It also collaborates with the European Financial Coalition and the Financial Coalition Against Child Pornography.

How Reports of Child Sexual Abuse Content Are Typically Assessed



A report of suspected illegal child sexual abuse content is made by an internet user, directly or through their internet service provider (ISP) or mobile operator

National hotline or law enforcement agency (LEA) assesses the content

Illegal

Not illegal

TRACED TO HOST COUNTRY

NO FURTHER ACTION

If the content is hosted in the same country as the hotline or LEA, notice and take down processes are instigated and the content is removed.

If the content is hosted in a different country, the report is passed on to INHOPE or the relevant LEA.

Some countries also add the URL to a 'block list' that allows ISPs and mobile.

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?

> ***We must strengthen the multi-stakeholder model to preserve the internet as a fast engine for innovation.***
>
> — Neelie Kroes, Vice President of the European Commission

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.

Globalisation of key internet functions should be promoted — in a transparent way — to preserve the resiliency, security and stability of the internet.

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 that should be addressed through standards bodies, the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB) and other fora.

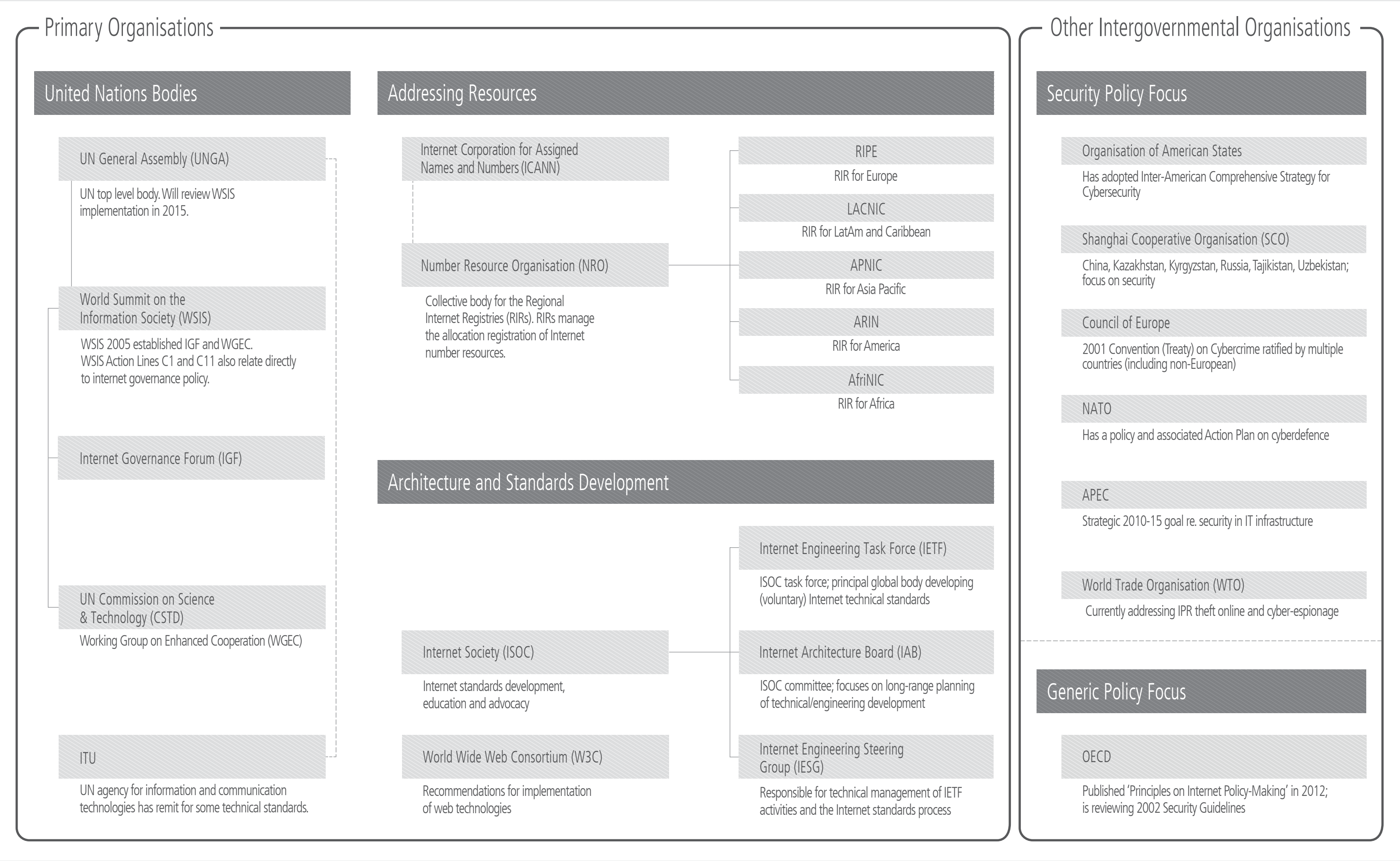
Economic and transactional issues such as internet interconnection charges are best left to commercial negotiation, consistent with commercial law and regulatory regimes.

Resources

Internet Society: Internet Governance
OECD Resources on Internet Governance
Centre for International Governance Innovation
Internet Governance Forum

Deeper Dive

Key Players in Internet Governance



Primary Organisations

United Nations Bodies

UN General Assembly (UNGA)
UN top level body. Will review WSIS implementation in 2015.

World Summit on the Information Society (WSIS)
WSIS 2005 established IGF and WGEC. WSIS Action Lines C1 and C11 also relate directly to internet governance policy.

Internet Governance Forum (IGF)

UN Commission on Science & Technology (CSTD)
Working Group on Enhanced Cooperation (WGEC)

ITU
UN agency for information and communication technologies has remit for some technical standards.

Addressing Resources

Internet Corporation for Assigned Names and Numbers (ICANN)

Number Resource Organisation (NRO)
Collective body for the Regional Internet Registries (RIRs). RIRs manage the allocation registration of Internet number resources.

RIPE
RIR for Europe

LACNIC
RIR for LatAm and Caribbean

APNIC
RIR for Asia Pacific

ARIN
RIR for America

AfriNIC
RIR for Africa

Architecture and Standards Development

Internet Society (ISOC)
Internet standards development, education and advocacy

World Wide Web Consortium (W3C)
Recommendations for implementation of web technologies

Internet Engineering Task Force (IETF)
ISOC task force; principal global body developing (voluntary) Internet technical standards

Internet Architecture Board (IAB)
ISOC committee; focuses on long-range planning of technical/engineering development

Internet Engineering Steering Group (IESG)
Responsible for technical management of IETF activities and the Internet standards process

Other Intergovernmental Organisations

Security Policy Focus

Organisation of American States
Has adopted Inter-American Comprehensive Strategy for Cybersecurity

Shanghai Cooperative Organisation (SCO)
China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Uzbekistan; focus on security

Council of Europe
2001 Convention (Treaty) on Cybercrime ratified by multiple countries (including non-European)

NATO
Has a policy and associated Action Plan on cyberdefence

APEC
Strategic 2010-15 goal re. security in IT infrastructure

World Trade Organisation (WTO)
Currently addressing IPR theft online and cyber-espionage

Generic Policy Focus

OECD
Published 'Principles on Internet Policy-Making' in 2012; is reviewing 2002 Security Guidelines

Source: GSMA

Mandatory Registration of Prepaid SIMs

Background

In many countries, pay-monthly or post-paid mobile phone contracts are common. These require customers to provide proof of identification and evidence of sufficient funds before they enter into a billing arrangement with their mobile network operator.

In the case of prepaid or pay-as-you-go services, customers must purchase credit to activate their subscriber identity module (SIM) card. This can be done anonymously, as registration is not typically required.

An increasing number of governments, however, have recently introduced mandatory registration of prepaid SIM card users, primarily as a tool to counter terrorism and improve law enforcement.

The take-up of mobile-commerce and e-government services can be boosted by the registration of all SIM card users, as it enables them to verify their identity and log in to such services using their mobile device. Nevertheless, mandatory registration often leads to implementation challenges and unforeseen consequences, particularly in developing countries, where the majority of mobile users have prepaid SIM cards.

These challenges include:

- Failure by some mobile users to understand that their SIM cards could be deactivated, sometimes without warning, if they do not register by a certain deadline
- Barriers that prevent some mobile users from physically registering, e.g., the distance to a registration centre
- Limitations to prepaid SIM card distribution channels due to the registration requirement
- The cost of implementation, which can be significant and may impact operators' ability to invest in new, innovative services and network infrastructure, particularly in remote and rural areas
- 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
- Mobile user concerns related to the access, security, use and retention of their personal data, particularly in the absence of national laws on privacy and freedom of expression

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

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 prepaid registration of prepaid SIM card users could offer valuable benefits to citizens and consumers, 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.

The effectiveness of prepaid SIM user registration depends on local market conditions, for example, whether citizen access to national identity documents is widespread throughout the country and whether the government maintains robust citizen identity records.

Where prepaid SIM user registration can create value and positive outcomes for consumers, mobile operators and governments will have an incentive to offer services that encourage consumers to register voluntarily.

We urge governments that are considering such a policy to examine the local market conditions, engage with industry and conduct impact assessments before introducing regulation.

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.

Resources

GSMA white paper: Mandatory Registration of Prepaid SIM Card Users
Academic paper: The Rise of African SIM Registration: Mobility, Identity, Surveillance & Resistance, London School of Economics, November 2012
Academic Paper: Implications of Mandatory Registration of Mobile Phone Users in Africa, Deutsches Institut für Wirtschaftsforschung, 2012
Academic Paper: Privacy Rights and Prepaid Communication Services, Simon Fraser University, March 2006
Article: Assessing the Impact of SIM Registration on Network Quality (Nigeria), July 2013
Article: Global Crackdown on Phone Anonymity, Kosmopolitica, May 2013

Best Practice

Impact Assessment Factors

The pros and cons of prepaid SIM registration will be different for each market. Governments considering a mandatory prepaid SIM registration policy should fully investigate a number of factors, including:

Whether there is evidence that the registration exercise would improve the reliability of data available to law enforcement agencies and contribute to crime reduction, and whether a criminal could easily obtain a SIM card — locally or abroad — to avoid registration

The share of population holding a valid ID document

Whether the government keeps an up-to-date and robust record of citizen identity documents (which consumers are required to use when registering their SIM)

Whether any geographic, demographic or cultural characteristic would affect how easily consumers could physically register a SIM in their name (e.g., those living in remote areas or informal housing, or those who are disabled)

The ability to make all consumers aware that their existing prepaid SIM cards may be deactivated if they fail to register them by a certain deadline

The impact of any data protection and privacy laws on how consumers' personal details are collected, stored and potentially shared with government agencies and third parties

Whether the registration exercise will impose a disproportionate burden on mobile operators

Implementation Factors

Where a decision to mandate prepaid SIM registration has been made, governments should take into account global best practices and consider the following:

Consumer-related issues

Identity verification and registration channels (How can prepaid SIM users verify their identity, and can the various registration channels cater to all consumer groups, such as those living in remote or rural areas?)

Effective public awareness campaigns (Are consumers aware that they need to register their SIMs and understand how to do this?)

Industry-related issues

Timescales for mobile operators to implement registration processes (Are they practical and realistic?)

The use, sharing and retention of SIM users' registration details (Are data retention and disclosure requirements proportionate, and do they preserve mobile users' privacy?)

Broader regulatory compliance

Regulatory enforcement and consequences of noncompliance for mobile operators (What are the regulator's enforcement powers after the registration deadline has passed?)

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?

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 is defining requirements that could lead to a global solution for owners to locate or disable their lost or stolen device. This will 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 and would be considered illegal in some countries.

> ***Handset theft has increased significantly in recent years, and handsets are becoming more attractive to thieves. Every stolen phone causes misery, possible violence and psychological consequences for mobile users.***
>
> — James Moran, Security Director, GSMA

Resources

OAS briefing paper on the theft of mobile terminal equipment
IMEI Database
Security Principles Related to Handset Theft
IMEI Security Weakness Reporting and Correction Process
Case Study: Mobile Phone Theft in Costa Rica
Q&A: Consumer precautions against mobile phone theft
News Release: Latin American Mobile Operators Commit to Combat Mobile Device Theft

Deeper Dive

Safeguards in Mobile Handset Manufacturing

Since 1996, the GSMA has promoted the use of Equipment Identity Registers (EIRs) among mobile network operators to ensure stolen handsets can be barred from networks by using the handsets' IMEI numbers. EIR effectiveness, however, is largely dependent on a secure implementation of the IMEI, and EIR deployment should be complemented by the efforts of the handset manufacturing community to ensure all handsets delivered to market incorporate appropriate security features. The following security principles help handset manufacturers protect the platform on which the IMEI mechanism is stored.

Principle 1

Implement safeguards for uploading, downloading and storing executable code and sensitive data related to the IMEI implementation

Principle 2

Protect components' executable code and sensitive data related to the IMEI implementation

Principle 3

Protect against exchange of data and software between devices

Principle 4

Protect IMEI executable code and sensitive data from external attacks

Principle 5

Prevent the download of previous software versions

Principle 6

Detect and respond to unauthorised tampering

Principle 7

Apply software quality measures for all sensitive functions

Principle 8

Prevent hidden areas from accessing or modifying executable code or sensitive data related to IMEI implementation

Principle 9

Prevent the substitution of hardware components

Source: GSMA and EICTA, Security Principles Related to Handset Theft, July 2005

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 emerging area of Near Field Communications (NFC) has raised the concept of electronic pickpocketing, or hacking into someone's NFC-enabled account from close proximity. This potential threat continues to receive more attention as NFC applications gain market traction and the role of the SIM as a secure platform for the hosting and execution of sensitive services becomes key.

The GSMA plays a key role in coordinating the industry response to security incidents, and 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 are service, network or device affecting.

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 there are no known cases of eavesdropping on UMTS or LTE networks.

Although mobile malware has not reached predicted epidemic levels, the GSMA is aware of the potential risks and its Mobile Malware Group coordinates the operator response to identified threats. The group facilitates the prompt exchange of information between industry stakeholders and encourages best practice to manage and handle malware by producing comprehensive guidelines for its members.

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 smart 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 on mobile technology to the next.

Resources

GSMA Statement on Media Reports Relating to the Breaking of GSM Encryption
The European Mobile Manifesto
GSMA Security Accreditation Scheme
GSMA Security Advice for Mobile Phone Users

Deeper Dive

Industry Vigilance to Protect Mobile Customers

The GSMA manages numerous working groups composed of subject-matter experts from GSMA member companies. Each working group focuses on an issue that requires cross-industry cooperation, and mobile security is one of these. The GSMA Security Group is responsible for technical security matters, maintenance and development of security algorithms, refinement of technical solutions to combat fraud and dissemination of security warnings and advice to GSMA members.

Security Group Activities

Identify and analyse security risks to which network operators are exposed

Advise network operators of the latest best practice being adopted in terms of technical security

Submit operator requirements to international standards bodies

Advise on technical solutions to combat fraud

Maintain and enhance mobile security levels

Meet changing threats

With its wide remit and the ever-changing nature of security in information and communication technology (ICT), the Security Group is highly responsive to security events and new potential risks. For example, when security researcher Karsten Nohl recently alerted the GSMA to a potential weakness in SIM encryption, the GSMA was able to investigate the assertion, issue a range of briefings to its members and provide guidance on the countermeasures operators could take. In that instance, only a minority of SIMs produced against older standards were found to be vulnerable. The swift and comprehensive response was the work of the GSMA Security Group, was widely recognised and commended.

Security Group Subgroups

CEIR Technical User Group

Responsible for the development and promotion of GSMA's Central Equipment Identity Register database to facilitate sharing of stolen handset data between networks

Mobile Malware Group

Responsible for coordinating the operator response to emerging threats posed by mobile malware and mobile device vulnerabilities

Device Security Steering Group

Responsible for device-related security threats that capture the attention and concern of regulators, the media and concerned users

Signalling Security Group

Responsible for raising awareness of signalling protocol risks and to reduce the potential for known weaknesses by investigating and recommending countermeasures and mitigation strategies

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, but 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 parts of the settlement.

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.

Number resource misuse is one of the topics currently being addressed by the GSMA Fraud Forum, a global conduit for best practice with respect to fraud management for mobile network operators. The Fraud Forum's main focus is to identify and analyse techniques used to perpetrate fraud against member networks and to recommend practical, cost-effective solutions.

The Fraud Forum supports a European Union initiative under which national regulators can instruct communications providers to withhold payment to downstream traffic partners in cases of suspected fraud and misuse. The group also advises Europol in its work to combat number resource misuse.

The Fraud Forum believes 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 Forum shares abused number ranges used for fraud among its members and with other fraud management industry bodies.

The Fraud Forum 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
GSMAs fraud management resources are available only to members.

Facts and Figures

Top 10 Countries or Services Whose Numbering Resources Are Being Abused

1. France
2. United Kingdom
3. Latvia
4. Maldives
5. Algeria
6. Globalstar mobile satellite service
7. Cuba
8. Zimbabwe
9. Austria
10. Haiti

Source: Operator reports to the GSMA, 2014

Best Practice

Recommended Operator Controls to Reduce Exposure to Fraud from Number Resource Misuse

Implement controls at the point of subscriber acquisition and controls to prevent account takeover

Remove the conference or multi-call facility from a mobile connection unless specifically requested, as fraudsters can use this feature to establish up to six simultaneous calls

Remove the ability to call forward to international destinations, particularly to countries whose numbering plans are commonly misused

Utilise the GSMA high risk ranges list, so that unusual call patterns to known fraudulent destinations can raise alarms or be blocked

Ensure roaming usage reports received from other networks are monitored 24x7, preferably through an automated system

Ensure that up-to-date tariffs, particularly for premium numbers, are applied within roaming agreements

Implement the Barring of International Calls Except to Home Country (BOIEXH) function for new or high-risk subscriptions

Privacy

Background

The growth of the mobile internet, led by the success of smartphones and mobile broadband technology, continues to bring widespread benefits and opportunities to people around the world. However, it is also creating new challenges regarding the security and privacy of mobile users' personal information.

Research shows that mobile customers are concerned about their privacy and want simple and clear choices for the control over their information, and they 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. In addition, important categories of data such as location or traffic data are often only subject to privacy rules when processed by a mobile operator and not an internet content provider.

This misalignment between national or market-sector privacy laws and global data flows makes a consistent user experience impossible. Equally, the misalignment distorts the market on data, causing legal uncertainty for operators, which can deter investment and innovation.

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.

> ***We believe that privacy matters. Through its Mobile Privacy Initiative (MPI) the GSMA published a set of universal Mobile Privacy Principles in 2011 that describe how mobile consumers' privacy should be respected and protected. The GSMA has also published and members are implementing a set of Privacy Design Guidelines for Mobile Application Development.***
>
> — Pat Walshe, Director of Privacy, GSMA

Resources
GSMA: Consumer Research Insights and Considerations for Policymakers
Mobile and Privacy on GSMA.com
Mobile Privacy Principles
Privacy Design Guidelines for Mobile Application Development

Best Practice

In January 2011, the GSMA 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.

Source: GSMA

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 is it 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 condernned about sharing the exact location of their mobile

Source: Futuresight, GSMA – "User perspectives on mobile privacy" (2012)

Spam

Background

'Spam' refers to bulk unsolicited messages. Most spam is intended to defraud or scam the recipient.

Attack techniques constantly change, as spammers identify new opportunities in the ever-changing technological, social, political and economic environment. Spammers are not inclined to obey local or international laws.

Spam detection and prevention techniques must continually evolve to stay ahead of spammers. The only effective way to prevent spam is to stop the messages from being delivered.

Spam is being discussed at many international law enforcement conferences and by multi-stakeholder organisations, including the Internet Engineering Task Force and the Internet Governance Forum.

Downloadable smartphone apps have opened another avenue for spammers to propagate unwanted messages and fraudulent content.

Debate

How can spam-related threats be addressed in the context of mobile services?

Are industry-led solutions the most effective approach?

Industry Position

The GSMA and its members are committed to combatting mobile spam by improving industry intelligence and collaborating with local law enforcement whenever possible.

Technology allows spammers to easily cross borders and evade local laws and law enforcement. Effectively addressing the problem requires global collaboration in law enforcement and technology.

Mobile spam damages the industry by increasing operator costs and reducing consumer trust. Mobile network operators should defend against these threats and continually protect the quality of the mobile service while reinforcing subscriber trust.

The GSMA offers a Mobile Spam Code of Practice, a coordinated effort among mobile operators to prevent SMS spam on mobile networks.

The GSMA also offers the Spam Reporting Service (SRS) which enables consumers to easily report spam via the universal short code '7726', which spells 'spam' on most device keyboards. These reports help participating operators take appropriate action to terminate spam attacks and improve their spam defence tactics. National, industry-coordinated efforts are encouraged to maximize the impact of prevention activities.

We believe that an international telecoms treaty is not the correct instrument for combating spam, as this could potentially raise sensitive issues regarding commercial or political free speech.

Formal regulatory measures to address spam should be introduced as a last resort, focused at the national level and only implemented after detailed impact assessments have been conducted.

> *The GSMA Spam Reporting Service will not only help defend against today's attacks, but proactively help protect our customers and our network from new and emerging mobile threats.*
>
> — Ed Amoroso, Chief Security Officer, AT&T

Resources
GSMA spam reporting services
Cloudmark spam-reporting clearing house
GSMA Mobile Spam Code of Practice

Best Practice

Mobile Spam Code of Practice

The Mobile Spam Code of Practice has been devised to protect the secure and trusted environment of mobile services to ensure customers receive minimal amounts of spam sent via SMS and MMS. The code takes a firm stance on how to deal with mobile spam messages that are either fraudulent or unsolicited commercial messages.

Participation by mobile operators is voluntary and applies specifically to three types of unsolicited SMS and MMS messages:

- Commercial messages sent to customers without their consent
- Commercial messages sent to customers encouraging them directly or indirectly to call or send a message to a premium rate number
- Bulk unlawful or fraudulent messages sent to customers (e.g., faking, spoofing or scam messages)

Under the code, the mobile operators that are signatories commit to:

- Include anti-spam conditions in all new contracts with third-party suppliers
- Provide a mechanism that ensures appropriate customer consent and effective customer control with respect to mobile operators' own marketing communications
- Work co-operatively with other mobile operators, including those who are not signatories to the code
- Provide customers with information and resources to help them minimise the levels and impact of mobile spam
- Undertake other anti-spam activities, such as ensuring that an anti-spam policy is in place, prohibiting the use of the mobile network for initiating or sending mobile spam, and adopting GSMA-recommended techniques for detecting and dealing with the international transmission of fraudulent mobile spam
- Encourage governments and regulators to support this industry initiative

Appendix

GSMA Contacts

Through direct engagement with governments, the GSMA's advocacy team strives to shape the regulatory agenda in ways that benefit the mobile ecosystem, as well as mobile-using citizens and businesses. The team comprises the association's government and regulatory affairs organisation, whose policy experts are distributed around the globe, as well as Mobile for Development, which provides technical assistance through a number of programmes to maximise the socio-economic benefits of mobile in developing countries.

Please e-mail **handbook@gsma.com** with any questions or comments about the Mobile Policy Handbook.

Tom Phillips
Chief Regulatory Officer
tphillips@gsma.com

John Giusti
Head of Policy
jgiusti@gsma.com

Matthew Bloxham
Head of Policy Research
mbloxham@gsma.com

Belinda Exelby
Head of Institutional Relations
bexelby@gsma.com

Zouhair Khaliq
Managing Director, Mobile for Development
zkhaliq@gsma.com

Lawrence Yanovitch
President, GSMA Foundation
lyanovitch@gsma.com

Sebastian Cabello
Director, GSMA Latin America
scabello@gsma.com

Francis Hook
Director, GSMA Africa
fhook@gsma.com

Peter Lyons
Director, GSMA Middle East and North Africa
plyons@gsma.com

Isabelle Mauro
Head of GSMA Africa and Middle East
imauro@gsma.com

Irene Ng
Director, GSMA Asia
ing@gsma.com

Martin Whitehead
Director, GSMA Europe
mwhitehead@gsma.com

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 236 countries, more than 800 mobile network operators and over 1,000 mobile virtual network operators (MVNOs). Comprising approximately 15 million data points covering 520 different metrics, 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 3,500 network deployments and more than 450 spectrum auctions to date. White papers and reports from across the GSMA and weekly bulletins are also available as part of the service.

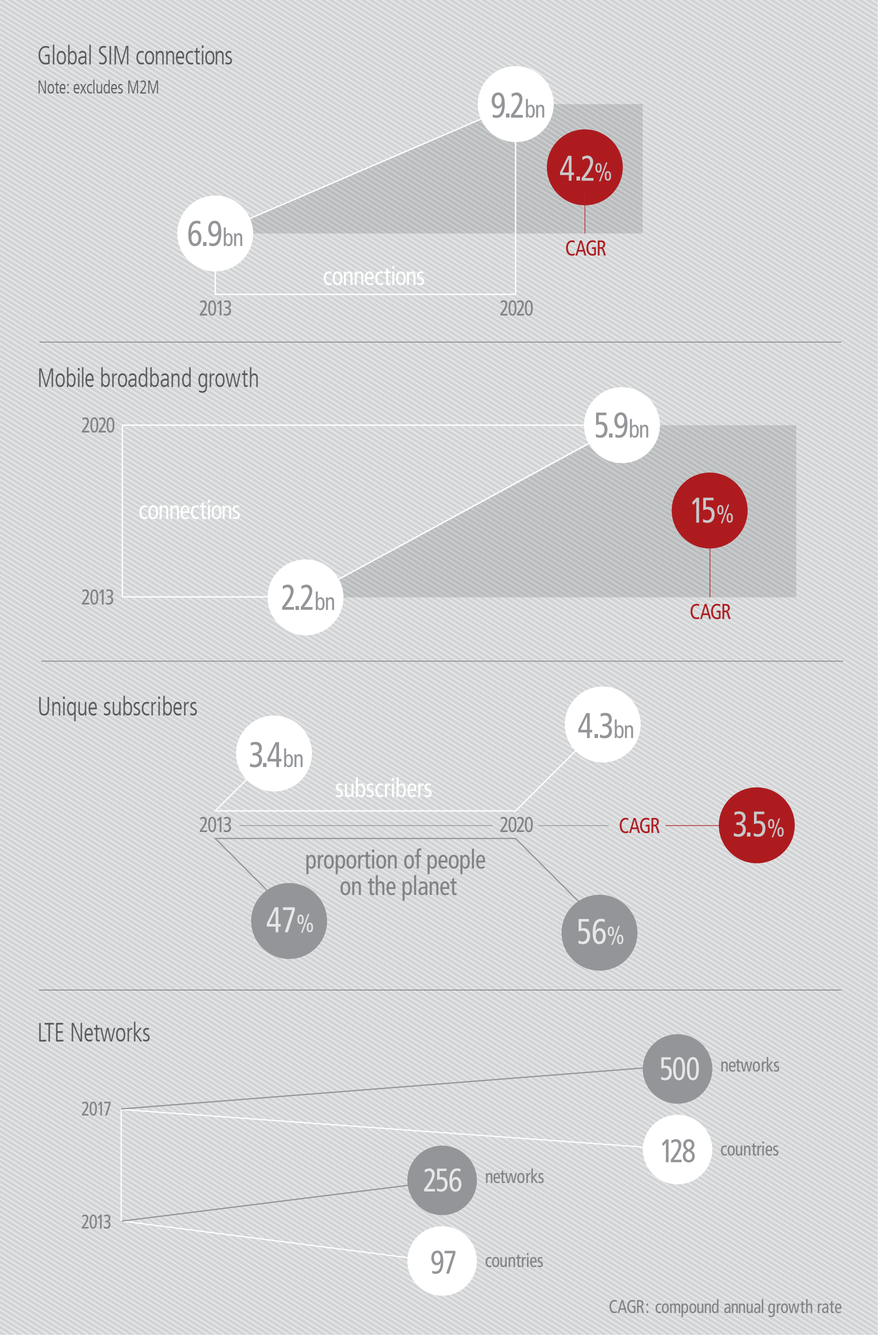
Powerful data tools

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 Intelligence

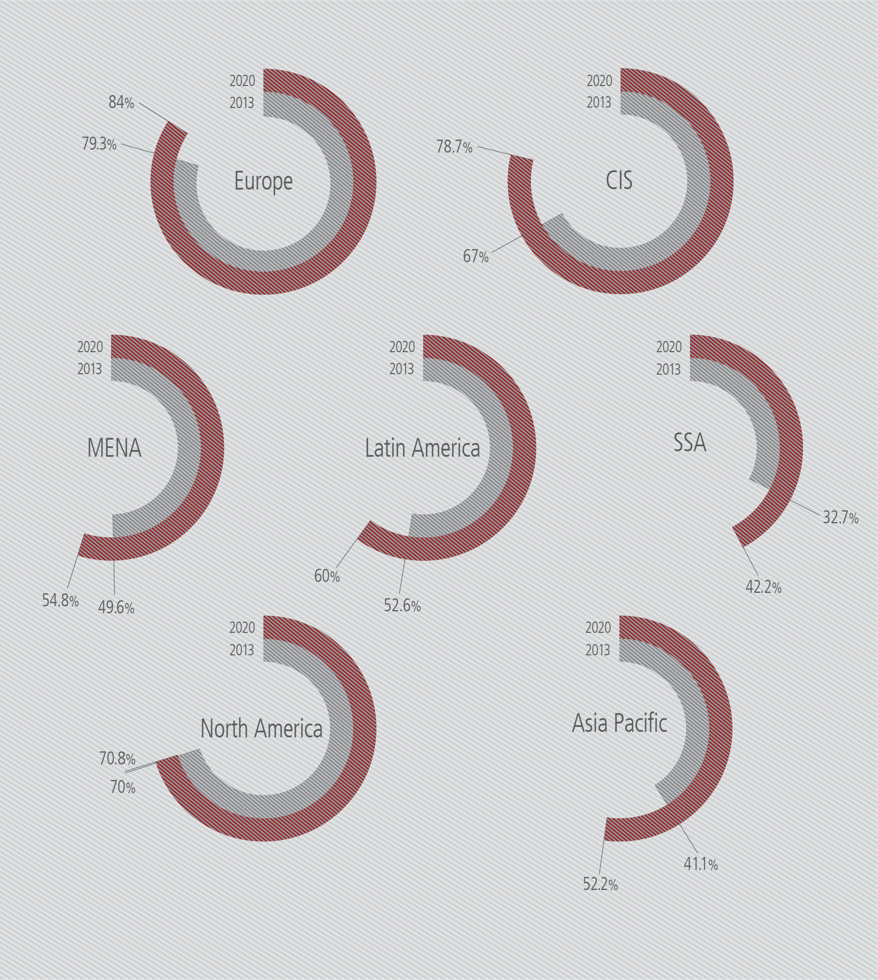


Unique subscriber penetration by region

Source: GSMA Intelligence

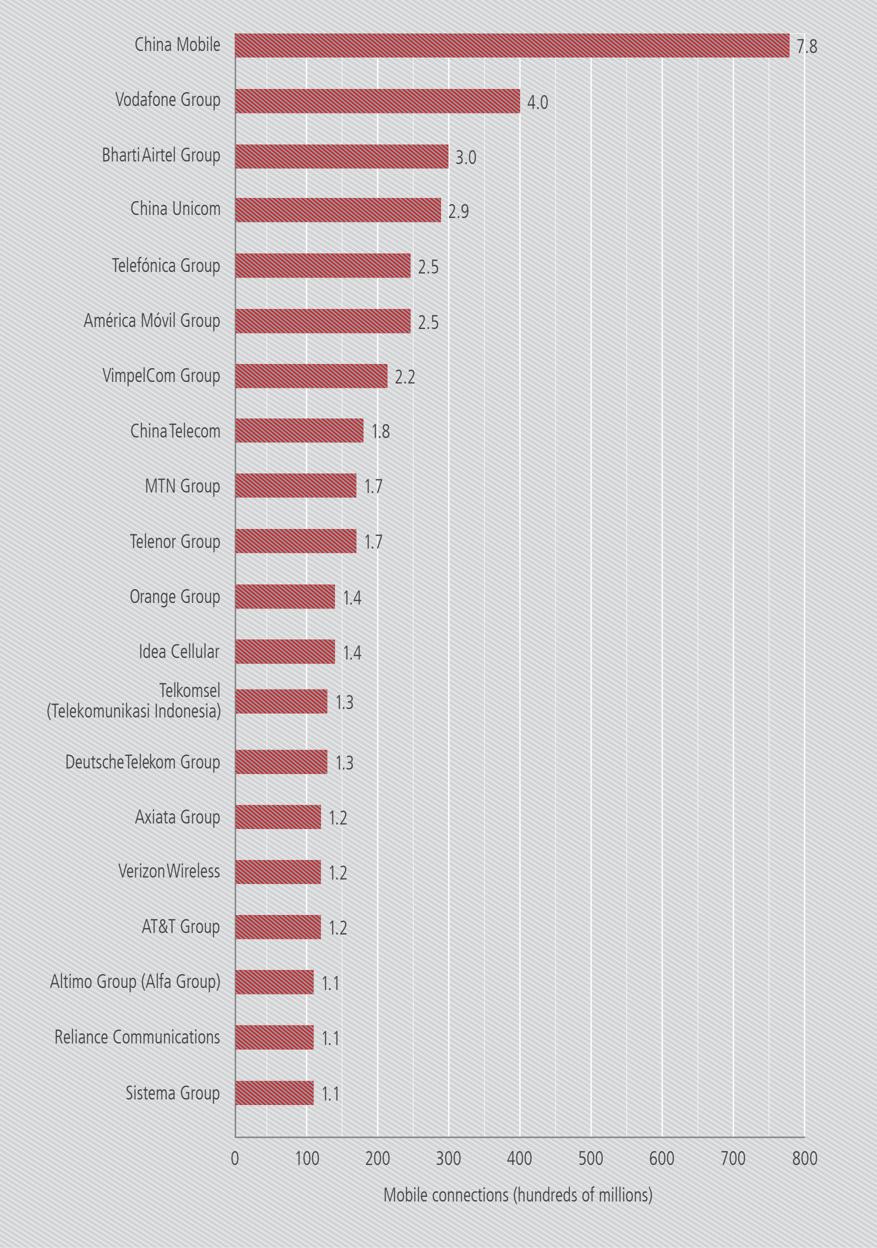
The global unique subscriber base has been growing at a rate of 7.3% per annum: growth is forecast to continue, but at a slower rate of 3.5% out to 2020. However, this growth is far from uniform across the regions of the world. Growth is now largely coming from developing markets, which are forecast to add nearly 880 million subscribers over the next seven years, compared to only 56 million new additions in developed markets over the same period.

Unique subscriber penetration rates vary significantly across regions. Europe has the highest penetration rates, followed by North America and then the Commonwealth of Independent States ('CIS'). Sub-Saharan Africa had the lowest penetration rate at the end of 2013 (at just under a third of the population), despite having seen the fastest subscriber growth of any region over recent years.



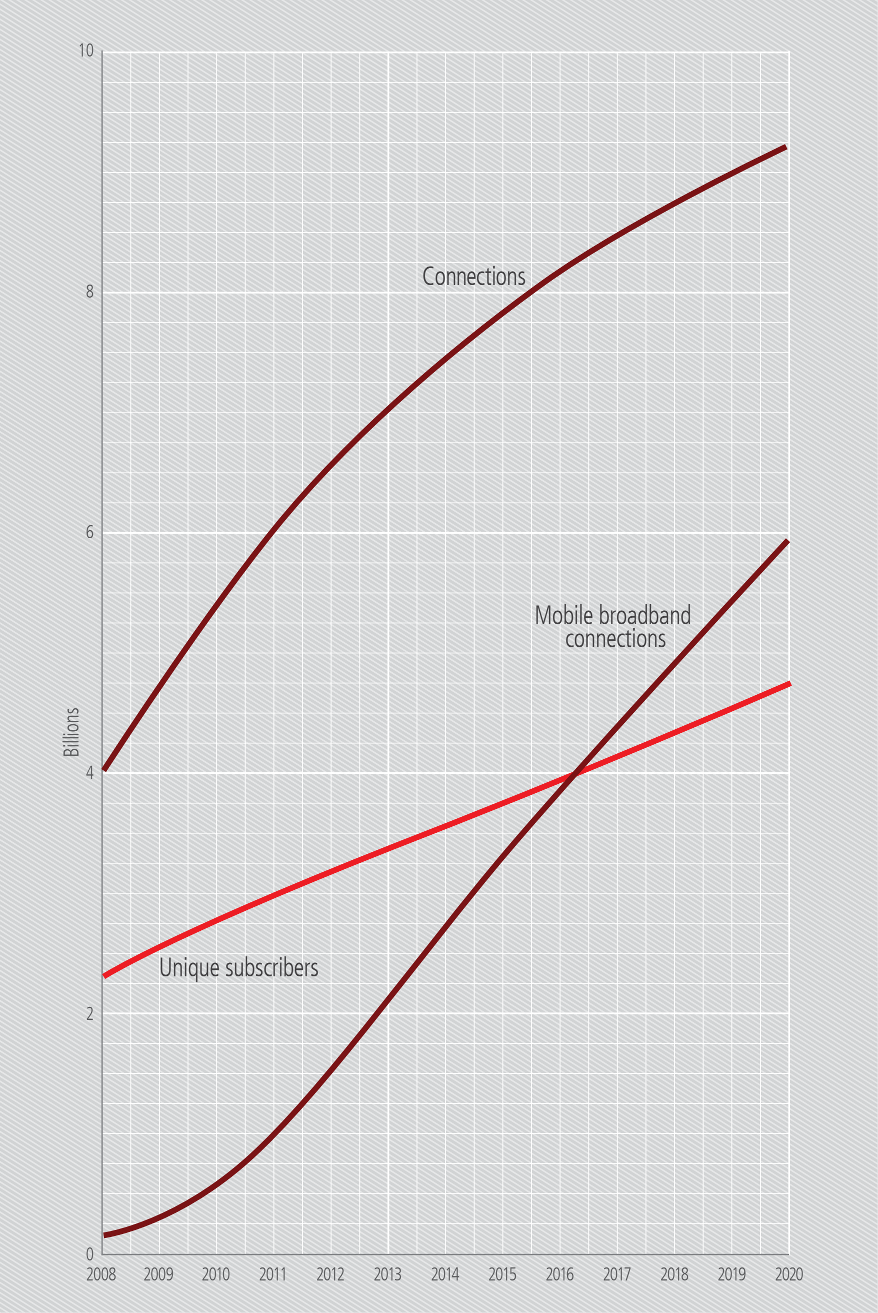
Mobile operator group global ranking by connections Q1 2014

Source: GSMA Intelligence, company reports



Global connection trends

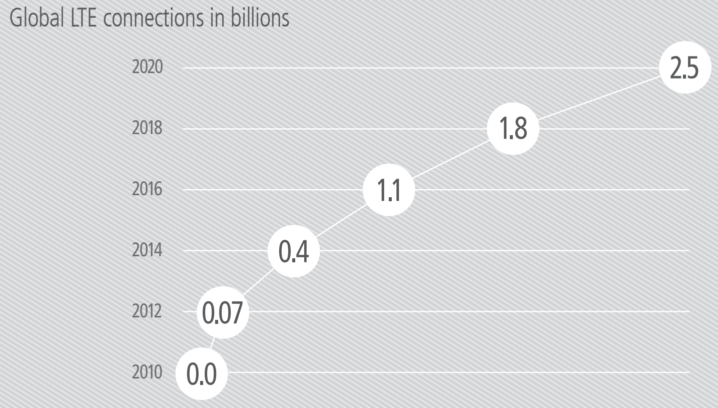
Source: GSMA Intelligence

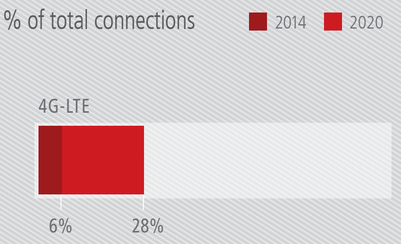


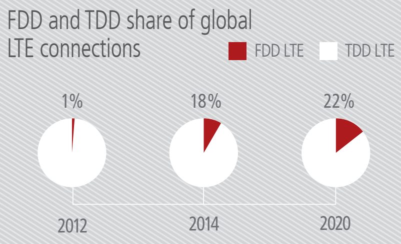
Global 4G-LTE connections forecast: 2010 – 2020

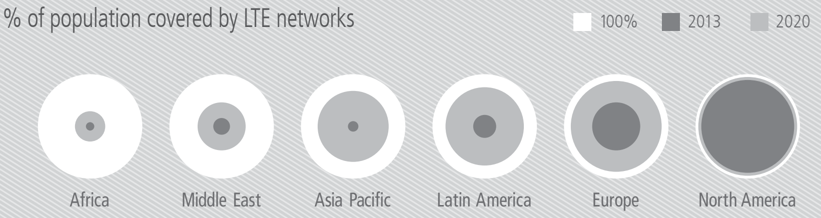
264 LTE networks commercially launched across 101 countries worldwide between December 2009 and January 2014, and almost as many additional LTE networks are expected to launch over the next five years, leading to 2,500,000,000 4G-LTE (FDD/TDD) connections expected worldwide in 2020.

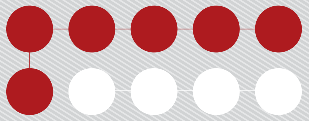
Source: GSMA Intelligence



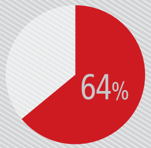








6 in 10 global 4G-LTE connections will come from the developing world in 2020, up from 5% in 2013, largely driven by TD-LTE growth in China.



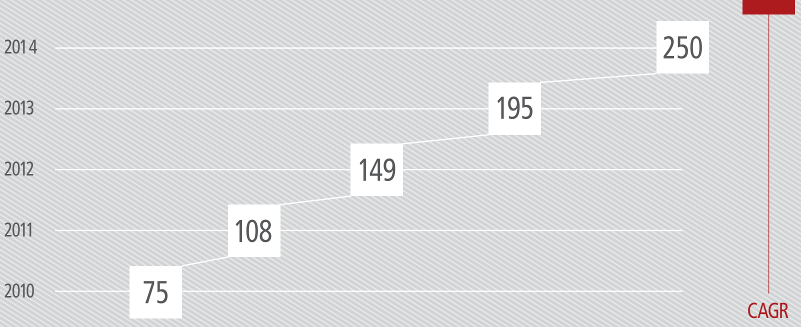
64% of the world's population will be covered by 4G-LTE networks by the end of 2020.

Global machine-to-machine (M2M) connections

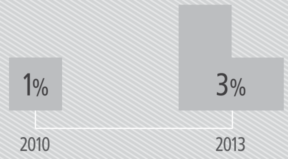
Source: GSMA Intelligence

GSMA Intelligence refers to M2M connections as SIM connections that enable mobile data transmissions between machines. It does not count SIMs used in computing devices in consumer electronics such as smartphones, dongles, tablets, e-readers, routers or hotspots.

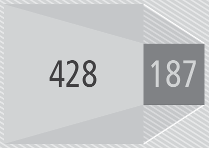
Global M2M connections (million)



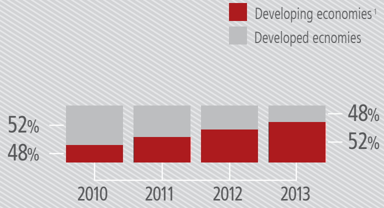
M2M as a % of total global connections



428 operators have launched M2M services in 187 countries, January 2014

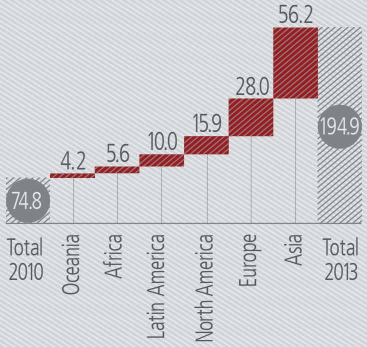


Regional share of global M2M connections



M2M connections growth has generally been stronger in developing markets over the last three years. This is party due to growth in China, the world's largest mobile market, and now the single largest M2M market, too.

Growth of M2M connections (millions)



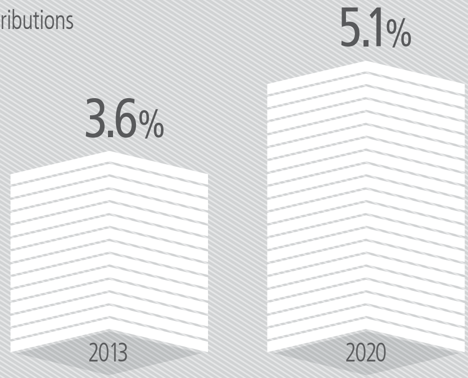
([1] World Bank definition)

An industry empowering people and society

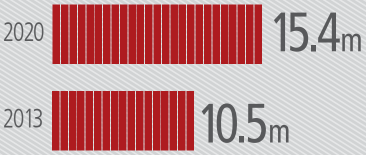
Source: GSMA Intelligence

US$2.4tn
2013 mobile industry impact

Global GDP contributions

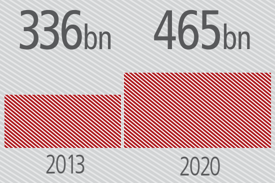


Jobs supported by the mobile ecosystem



Contribution to public funding in US$

(excluding regulatory and spectrum fees)



Mobile Ecosystem GDP Impact

US$870bn

The mobile ecosystem directly contributed around 1.3% of global GDP in 2013.

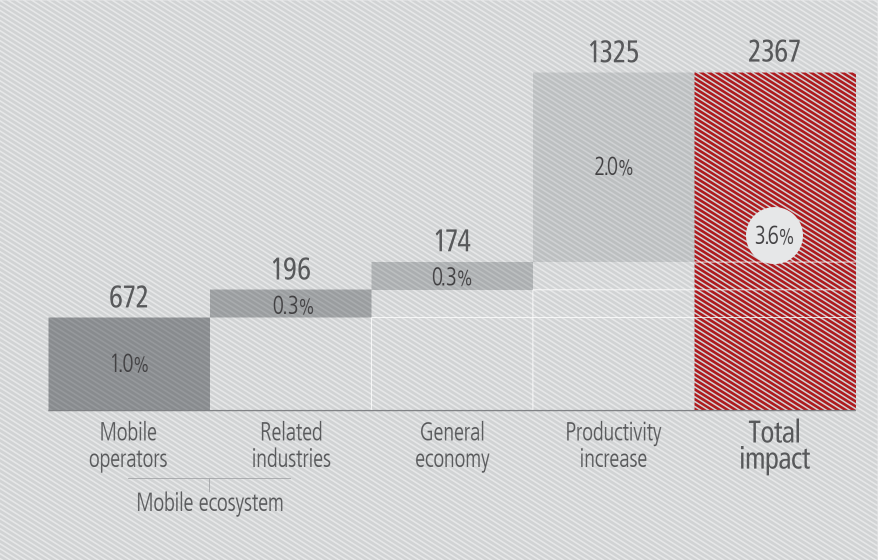
Infrastructure and support services	Handset manufacturers	Distributers/ retailers	Mobile operators
0.1%	0.1%	0.1%	1%

Figures provided are approximate

Industry contribution to global GDP

2013 Public impact (US$ Bn)

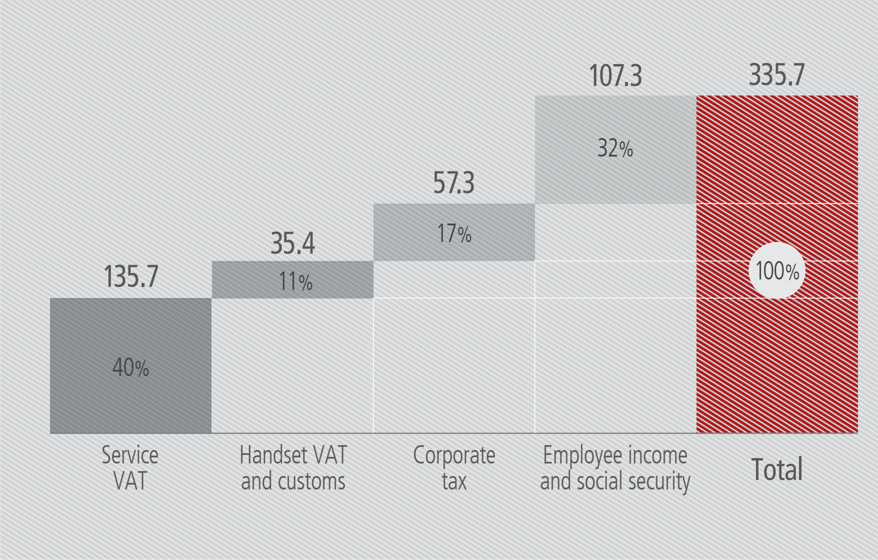
Source: GSMA Intelligence, annual reports, Factiva, BCG Analysis



Mobile ecosystem contribution to public funding

2013 Public funding (US$ Bn)

Source: GSMA Intelligence, annual reports, Factiva, BCG Analysis



Spectrum auction revenues*

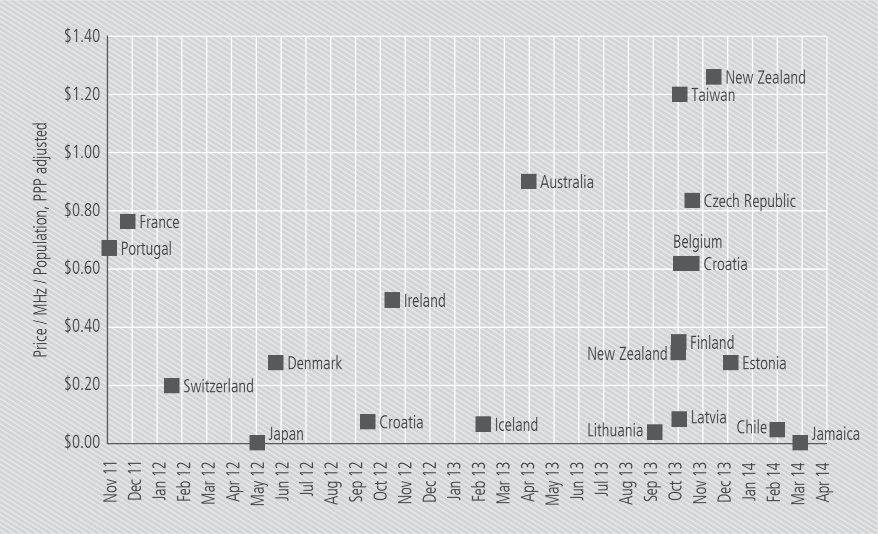
Source: GSMA Intelligence

Country	Country Frequency (MHz)	Date	Block (MHz)	Price ($)	$ MHz/Pop (PPP)
Pakistan	2100 MHz	Apr 2014	60.0	$902,820,000	$0.00
Pakistan	1800 MHz	Apr 2014	20.0	$210,000,000	$0.00
Jamaica	700 MHz	Apr 2014	24.0	$25,000,000	$0.01
Chile	700 MHz	Feb 2014	70.0	$22,374,884	$0.00
Nigeria	2300 MHz	Feb 2014	30.0	$23,250,000	$0.00
New Zealand	700 MHz	Jan 2014	10.0	$68,716,530	$1.05
Estonia	800 MHz	Jan 2014	20.0	$6,939,143	$0.50
Czech Republic	2600 MHz	Nov 2013	120.0	$49,161,600	$0.00
Czech Republic	1800 MHz	Nov 2013	18.0	$14,748,480	$0.01
Czech Republic	800 MHz	Nov 2013	60.0	$372,885,615	$0.04
Sierra Leone	900 MHz	Nov 2013	9.6	$2,500,000	$0.00
Belgium	800 MHz	Nov 2013	60.0	$490,014,000	$0.88
Croatia	800 MHz	Nov 2013	20.0	$38,515,449	$0.12
Armenia	800 MHz	Nov 2013	20.0	$15,314,000	$0.00
Finland	800 MHz	Oct 2013	60.0	$147,017,812	$0.50
Latvia	800 MHz	Oct 2013	60.0	$6,417,246	$0.15
New Zealand	700 MHz	Oct 2013	80.0	$145,712,160	$0.28
Taiwan	900 MHz	Oct 2013	60.0	$317,545,000	$0.43
Taiwan	1800 MHz	Oct 2013	120.0	$2,677,130	$1.80
Taiwan	700 MHz	Oct 2013	70.0	$1,037,080	$1.20
Algeria	2100 MHz	Oct 2013	90.0	$112,860,000	$0.08
Lithuania	800 MHz	Oct 2013	60.0	$3,212,614	$0.01
Bangladesh	2100 MHz	Sep 2013	50.0	$525,000,000	$0.00
Korea, South	1800 MHz	Aug 2013	50.0	$1,755,090,000	$0.00
Korea, South	2600 MHz	Aug 2013	40.0	$431,100,000	$0.00
Estonia	800 MHz	Aug 2013	20.0	$6,737,424	$0.49

*This table includes a selection of all spectrum auctions held during this period.

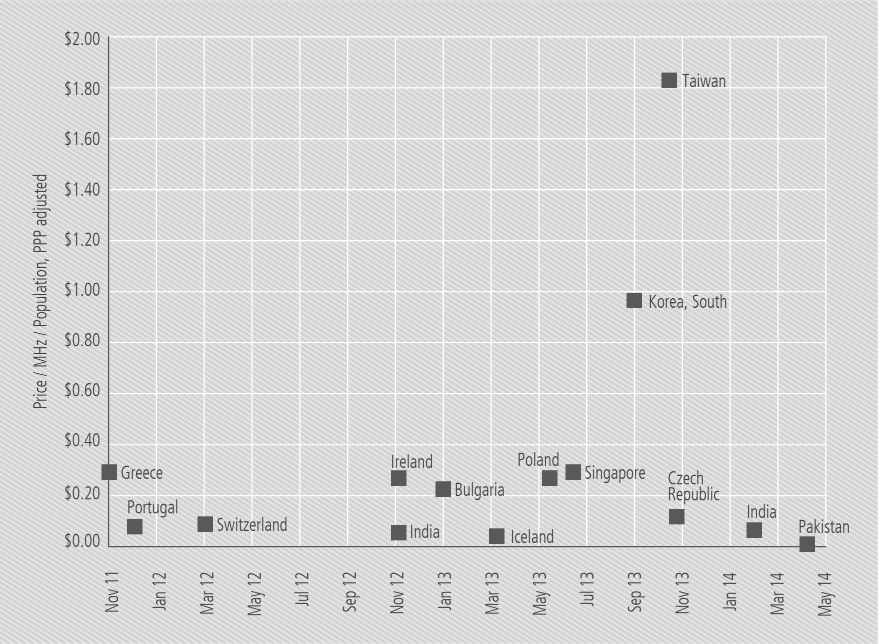
Comparative prices of Digital Dividend spectrum

Source: GSMA Intelligence



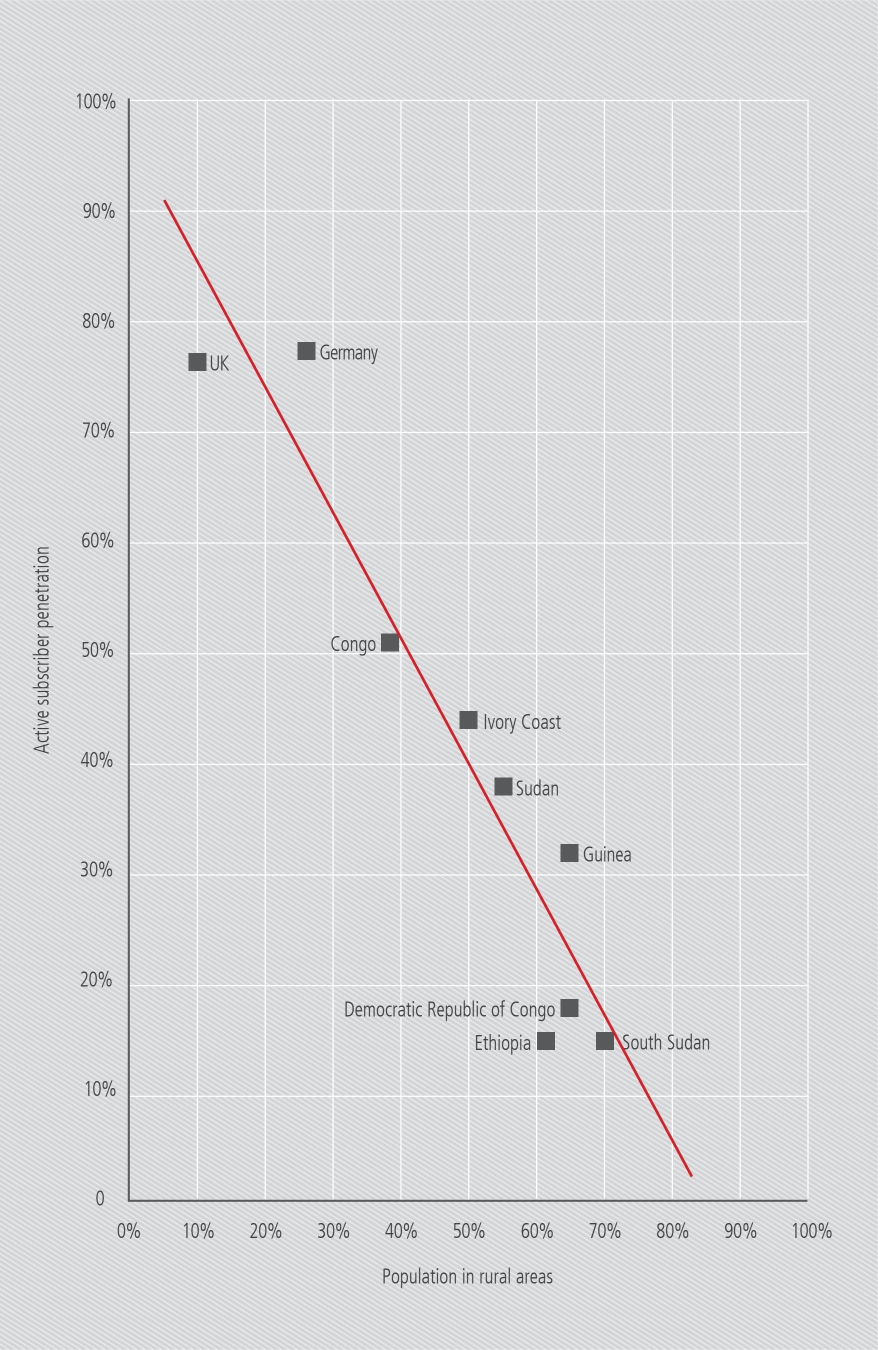
Comparative prices of 1800/1900MHz spectrum

Source: GSMA Intelligence



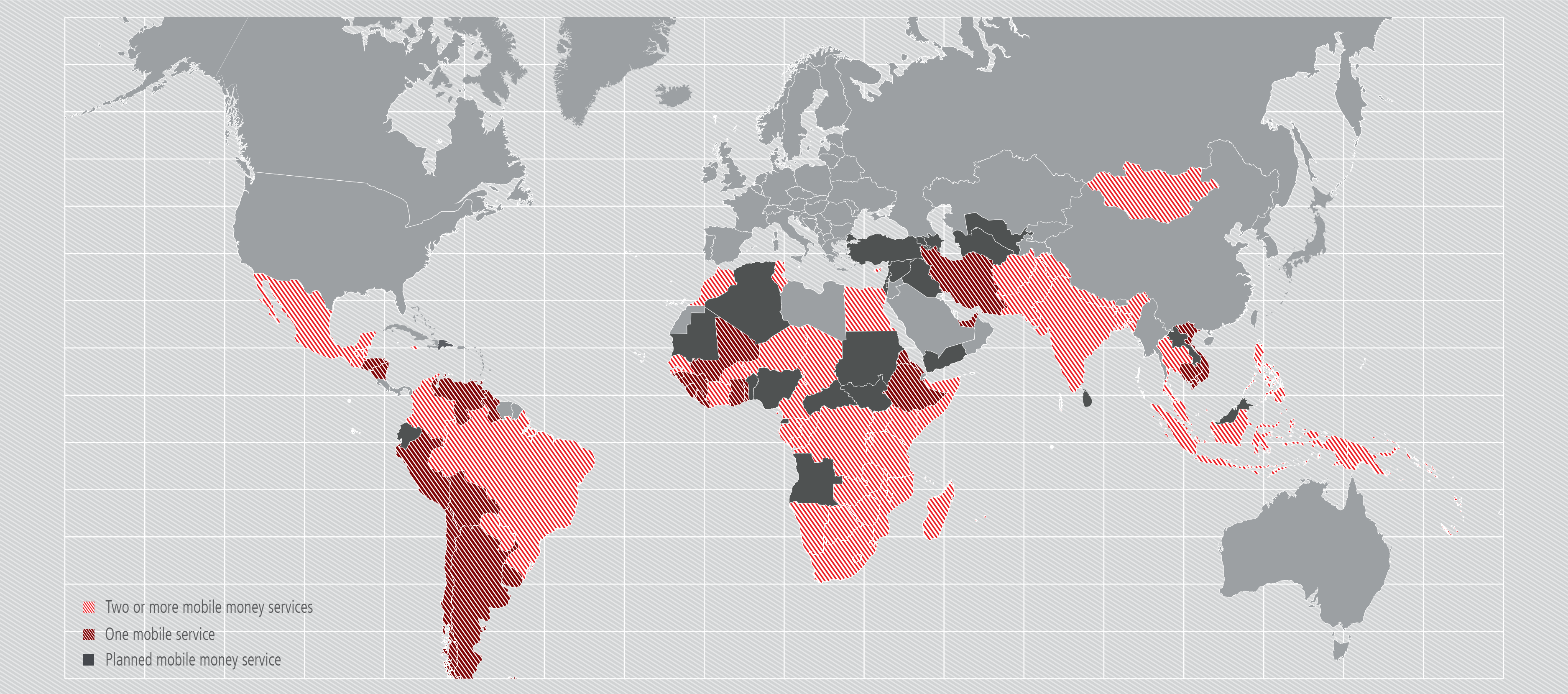
Mobile adoption vs rural population

Source: GSMA Intelligence



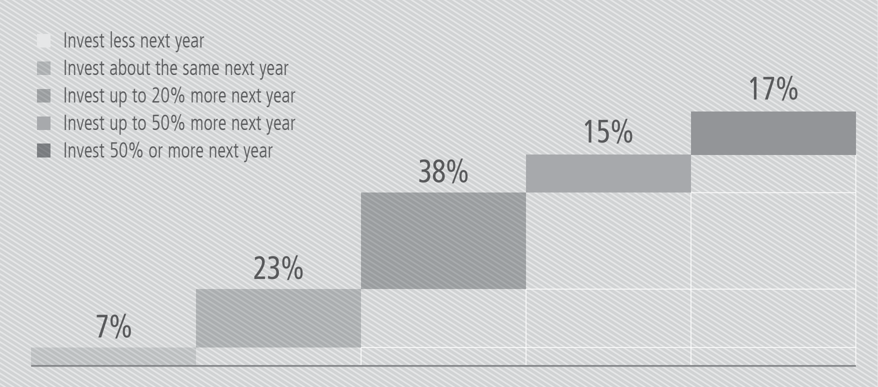
Number of live mobile money services by country

Source: GSMA


Two or more mobile money services
One mobile service
Planned mobile money service

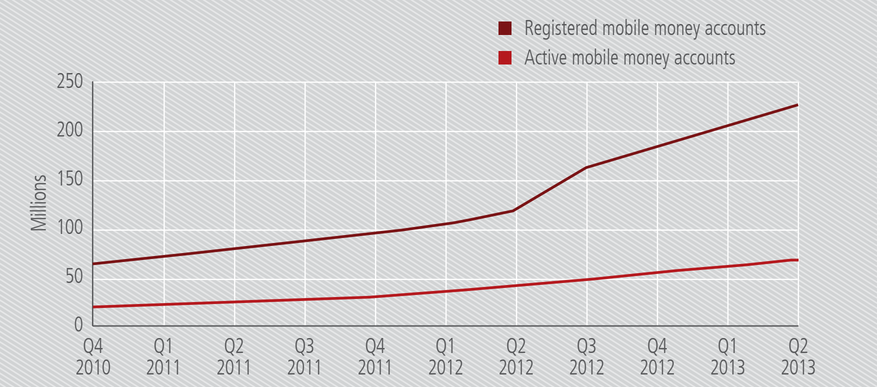
Planned investments in mobile money for 2014

Source: GSMA



Number of active and registered MM accounts

Source: GSMA



http://www.gsma.com/publicpolicy/handbook