GSMA

Mobile Policy Handbook

An insider's guide to the issues

About the GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at **www.gsma.com**

Follow the GSMA on Twitter: **@GSMA**

Do you have the knowledge?

Can you take a position?

Will you lead the debate?

About this handbook

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

The GSMA believes that a country's citizens benefit most when the private and public sectors work together in a spirit of openness and trust, and that policymakers and regulators create the conditions to attract telecoms investment, encourage innovation and strengthen digital trust. This is why we are committed to supporting governments and regulators in their efforts to introduce pro-investment telecommunications policies.

The Mobile Policy Handbook: An Insider's Guide to the Issues is an effort by the GSMA to promote this collaboration. A unique resource that assembles a range of policy topics and mobile industry positions and initiatives under one cover, the handbook is a signpost for regulatory best practice. As the global trade association of mobile operators, the GSMA conducts and commissions research on policy trends and challenges in the fast-moving mobile communications market. This handbook draws on the unique insight of the GSMA 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 eighth edition of the *Mobile Policy Handbook*, new policy topics and industry positions have been introduced, covering areas such as 5G and spectrum sharing. Throughout the handbook, the content has been refreshed with up-to-date statistics, new resources and industry insights.

The online version of this resource – www.gsma.com/publicpolicy/mobilepolicyhandbook – offers an always up-to-date catalogue of the policy positions of the mobile industry.

We encourage you to contact the GSMA with any questions or requests for more information. Email us at handbook@gsma.com.

World-changing trends

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

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

5G is appearing in cities first, where mobile data volumes are growing fastest and mobile operators can secure a return on investment. It is coexisting seamlessly with earlier mobile generations, and will connect citizens to the mobile internet for years to come.

Many countries are now home to their first commercial 5G network deployments. This is important because the digital economy needs 5G to respond to booming demand for mobile data, enable a massive Internet of Things (IoT) and support an array of services that require fast, dependable and low-latency connectivity.

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

5G networks will be at the core of this next-generation digital economy and society, and supportive policy and regulations are needed to make it a reality. We hope this handbook will serve as a compass to navigate the policy and regulatory challenges that lie ahead.

Contents

#BetterFuture

The mobile industry is united behind a common purpose to intelligently connect everyone and everything to a better future.

Mobile connectivity is transforming the lives of billions of people around the world and is at the heart of solutions that will tackle some of society's greatest challenges. Innovative and emerging mobile solutions, big data, artificial intelligence (AI) and 5G can all be leveraged as a force for good.

Today, understanding and responding to social, environmental and ethical issues are widely understood as being good for business, and the mobile industry strives to advance responsible, sustainable and trusted leadership.

Underpinning this vision is the industry's commitment to the Sustainable Development Goals (SDGs). Every year, the sector reports its collective progress in the *GSMA Mobile Industry SDG Impact Report* and shares policy actions needed to achieve the 2030 Agenda.

Throughout the COVID-19 pandemic, digital technologies have played a vital role in enabling social and economic activities to continue. People around the world have relied on the internet to stay connected to friends and family, access education and health services and work remotely. This underscores the importance of connectivity in our daily lives and the value of mobile networks, which remain the only form of internet access for many. Mobile operators in every region have been proactive during the pandemic, reaching out to their customers and working with public authorities and third parties to provide a range of essential services and support the communities in which they operate.

Closing the digital divide is a priority for the industry. When people are connected, equality, prosperity and well-being follow. Countries with high levels of mobile connectivity have made the most progress in meeting their SDG commitments. Mobile operators are continuing to deploy, extend and upgrade networks, and the number of people with no 3G or 4G network coverage has dropped to fewer than 450 million worldwide. Still, 3.8 billion people have been left behind. Even if they have mobile coverage, they are not reaping the benefits, whether because of a lack of digital skills, financial resources or locally adapted services.

With more than 5.2 billion people using a mobile phone in 2020, 13.1 billion IoT connections[1] and $900 billion in capital expenditure for 2021–2025 (80 per cent of which will be for 5G), the mobile industry has shown it has the power and the scale to make a meaningful difference to economies and societies.

Resources:

The GSMA 2021 Mobile Industry Impact Report: SDGs
The GSMA Sustainability Assessment Framework 2021

1. GSMA. (2021). *The Mobile Economy 2021.*

Mobile for Development

Introduction

The transformative power of mobile is most apparent in low- and middle-income countries (LMICs), where it is typically the most widespread technology and supported with far-reaching infrastructure. This puts the mobile industry in a unique position to connect people with essential services.

Mobile for Development (M4D) is a dedicated global team within the GSMA that brings together our mobile operator members, tech innovators, the development community and governments. Singularly positioned at the intersection of the mobile ecosystem and the development sector, the M4D team stimulates digital innovation to deliver both sustainable business and large-scale socio-economic and climate impact for the underserved.

The team identifies opportunities and provides support for innovations in digital inclusion, financial inclusion, gender equality, agriculture, essential urban services, humanitarian response and climate resilience and adaptation.

A key part of the M4D strategy is taking advantage of the synergies between these areas to amplify their impact. For example, identifying ways to use mobile money payments and machine-to-machine (M2M) communication to improve access to energy, clean water and sanitation while, at the same time, working in a variety of contexts to make digital services accessible and helpful for populations otherwise at risk of being left behind, particularly women and persons with disabilities.

M4D has impacted more than 120 million people in the past decade thanks to the support of funding partners and stakeholders from the public and private sectors. It has supported the growth of the mobile money industry from a concept to a transformational financial inclusion tool boasting more than 1.2 billion registered accounts. Similarly, it has supported the early stages and growth of the pay-as-you-go (PAYG) solar industry, which today provides clean energy to millions of households. Digital skills campaigns based on M4D content and gender strategies developed by mobile operators with M4D support have enabled tens of millions of users to get online for the first time.

In addition to the policy activities detailed in this handbook, M4D publishes foundational research, provides on-the-ground technical assistance to projects, creates technology assets to strengthen collaboration among industry players and de-risks pioneering digital solutions through the GSMA Innovation Funds, which have already provided capital to more than 100 ventures.

Through these activities and more, M4D tests the feasibility of new ideas and business models, supports the growth of those with the most potential for impact and scale and, ultimately, helps digital solutions address the challenges faced by our societies, our economies and our planet.

Digital inclusion

Background

The world is more connected than ever before, with more than four billion people and countless organisations relying on mobile operators to access the internet. Despite this achievement, 3.8 billion people remain unconnected and excluded from the benefits of mobile internet. The vast majority (89 per cent or 3.4 billion people) live in areas already covered by mobile broadband (this is known as the "usage gap"). Another 450 million do not have access to a network, mainly in Sub-Saharan Africa.

Unsurprisingly, most unconnected people live in LMICs (93 per cent) and are more likely to be poorer, less educated, female and rural. Although the gender gap in mobile internet use has narrowed, it is still significant. Women in LMICs are 15 per cent less likely to use mobile internet than men, which means there are 234 million fewer women using mobile internet. Expanding mobile broadband connectivity and accelerating mobile adoption are critical to the growth of the digital economy, achieving the SDGs and ensuring no one is left behind.

Through the Connected Women and Connected Society programmes, the GSMA works with the mobile industry, governments and other key stakeholders on digital inclusion initiatives that help to expand mobile broadband coverage and address the barriers to mobile internet adoption and use, with particular emphasis on underserved groups, such as women and persons with disabilities.

Public policy considerations

All stakeholders can and must do more to measure, understand and address the challenges perpetuating the digital divide. If no action is taken, based on current trends, almost 40 per cent of the world's population will still be offline by 2025. The reasons for the mobile digital divide are complex and rooted in a variety of economic, social and cultural factors. Accelerating mobile internet adoption and closing the digital gender gap will require deliberate and strategic efforts by the mobile industry, policymakers and the international community.

Resources:

GSMA Connected Society Website
GSMA Connected Women Website
GSMA Report: State of Mobile Internet Connectivity 2021
GSMA Report: The Mobile Gender Gap Report 2021
GSMA Report: Enabling Rural Coverage: Regulatory and Policy Recommendations to Foster Mobile Broadband Coverage in Developing Countries
GSMA Report: Accelerating Mobile Internet Adoption: Policies to Bridge the Digital Divide in Low- and Middle-Income Countries
GSMA Report: Reaching 50 Million Women with Mobile
GSMA Mobile Connectivity Index
GSMA Mobile Coverage Maps Website
GSMA Capacity Building Course: Unlocking Mobile Rural Coverage
GSMA Capacity Building Course: Bridging the Mobile Gender Gap

From a policy perspective, stakeholders should focus on the following key areas:

Enabling rural broadband expansion. People without network coverage typically have low incomes and live in sparsely populated, rural areas without enabling infrastructure, such as electricity. Such factors have an adverse impact on the business case for mobile network expansion. Policymakers should recognise that the mobile industry cannot fully close the coverage gap without government support. Instead, they can create better incentives to invest in rural infrastructure by aligning key policies around best practices. For example, adopting coverage-driven spectrum allocation and pricing, implementing investment-friendly tax policies, facilitating access to public infrastructure, reducing red tape for deploying mobile infrastructure and encouraging voluntary infrastructure sharing.

Addressing barriers to mobile internet adoption and use. 3.4 billion people live in areas covered by a mobile network but do not use mobile internet. Closing the usage gap will require tackling five main barriers: the affordability of handsets and data bundles; knowledge of mobile internet and digital skills; lack of relevant content and services; safety and security concerns; and access to key enablers, such as formal IDs or accessibility features. Policy considerations include measures that help lower the cost of handsets and data; improve literacy and digital skills focused on the life goals and needs of targeted user groups; create an environment for businesses and organisations to digitally transform or for start-ups to grow; and address online safety and security concerns, such as harassment, disinformation or handset theft. Responsibility for these and other policy measures cuts across various ministries, regulators and other agencies. Successful policy strategies recognise this and address these barriers holistically through a whole-of-government approach and in collaboration with key stakeholders, including with the private sector. The usage gap will only be closed when all stakeholders share responsibility for accelerating mobile internet adoption and use.

Closing the mobile gender gap. The mobile gender gap is not going to close on its own. Targeted intervention is needed from industry, policymakers, the development community and other stakeholders to ensure that women are no longer left behind. To address the gender gap, policymakers and regulators should:

- Ensure there is a focus on gender equality and reaching women at an organisational and policy level through senior leaders championing the issue and setting specific gender equity targets.
- Understand the mobile gender gap by improving the quality and availability of gender-disaggregated data and understand women's needs and the barriers they face to mobile ownership and use.
- Explicitly address women's needs, circumstances and challenges in the design and implementation of interventions and policies. This includes addressing the barriers women face related to mobile access, affordability, safety and security, knowledge and skills and the availability of relevant content, products and services.
- Collaborate and create partnerships with different stakeholders to address the mobile gender gap.

Mobile for Humanitarian Innovation (M4H)

Background

The GSMA Mobile for Humanitarian Innovation (M4H) programme was launched in 2018 with support from the UK Foreign, Commonwealth & Development Office (FCDO). The mission of M4H is to accelerate the delivery and impact of digital humanitarian assistance through improved access to and use of life-enhancing mobile-enabled services during humanitarian preparedness, response and recovery.

The mobile industry continues to invest in partnerships and solutions that have the potential to deliver impactful, safe and efficient digital humanitarian assistance. Nearly 160 mobile operators in 111 countries have committed to the GSMA Humanitarian Connectivity Charter, an initiative to improve the preparedness and response of mobile networks during humanitarian crises. The M4H programme has shown that a well-developed digital ecosystem has the potential to not only provide people affected by crisis with a suite of life-enhancing mobile services, but also strengthen the business case for mobile operators, and across the private sector, by expanding the range of digital services and platforms that can be tested, implemented and scaled.

The GSMA is in a unique position to support system- and industry-wide transformation for an inclusive and impactful digital humanitarian future. M4H works to achieve this aim by catalysing innovations, supporting partnerships, generating evidence and advocating for enabling policy environments that accelerate the delivery and impact of digital humanitarian assistance. The programme's high-quality monitoring, evaluation and learning framework allows it to assess the impact of its work and drive adaptive programming.

Public policy considerations

The M4H programme has developed the following policy considerations for multilateral agencies, governments, national regulatory authorities and mobile operators to accelerate the delivery and impact of digital humanitarian assistance:

Recognise the role of government in humanitarian preparedness, response and recovery. This includes the coordination of response to sudden-onset disasters, protracted emergencies and situations of forced displacement. This is a necessary role that enables governments to work with and empower the mobile industry and humanitarian partners to manage the risks associated with humanitarian crises and respond effectively.

Resources:

GSMA and UNHCR Report: Displaced and Disconnected
GSMA Report: Access to Mobile Services and Proof of ID
GSMA Report: Proportionate Regulation in Uganda
GSMA Report: National Emergency Telecommunications Plans: Enablers and Safeguards – A Brief Evaluation Guide for Policy Practitioners
GSMA Report: Policy and Regulatory Recommendations to facilitate Mobile Humanitarian and Social Assistance during COVID-19

Encourage mobile operators to have up-to-date business continuity plans or disaster recovery plans to ensure communications services are available, and to minimise the impact on telecommunications services during emergencies.

Promote the adoption of robust privacy and data protection principles when dealing with personal data, particularly those of marginalised persons, in the absence of relevant legal frameworks.

Create an industry-conducive emergency telecommunications plan to enable all stakeholders to think through the life cycle of a potential emergency, determine the capacities required and establish a governance framework using a multi-stakeholder approach.

Create clear and consistent legal and regulatory instruments for managing humanitarian digital identity and break down barriers that may inhibit the roll-out of mobile enabled-identification (ID) services or create regulatory uncertainty.

Create an inclusive and comprehensive ID enrolment policy to provide formal identities for the millions who are unregistered. Ensure persons of concern (PoC) have an acceptable and recognisable form of ID to access mobile and other identity-linked services.

Establish a proportionate risk assessment process that considers different types of PoC when developing proof-of-identity policies, procedures and rules.

Promote the acceptance of other forms of ID issued by humanitarian organisations to satisfy know-your-customer (KYC) requirements in markets where these are mandated.

Create a clear and conducive legal pathway for non-nationals, such as refugees, to access mobile connectivity and mobile money services in their own name. Harmonise ID-related SIM registration rules with the lowest tier of KYC requirements in countries and markets that mandate SIM registration.

Promote robust validation processes for humanitarian ID while being sensitive to data protection and privacy rules, particularly for marginalised groups and populations. Provide for relaxed rules or regulations during emergencies to ensure the provision of mission-critical telecommunications services during any phase of a humanitarian crisis, and to allow mobile operators to adjust to unforeseen circumstances.

Promote partnerships, collaboration and coordination within government, across public and private sector agencies and within communities at risk to facilitate timely and effective responses.

Facilitate agreements among mobile operators that give all mobile customers access to their networks during emergencies.

Mobile Money

Background

Mobile money has done more to extend the reach of financial services in the past decade than bricks-and-mortar banking has in the past century. This has been due to the ubiquity of mobile phones and mobile operators' extensive networks and retail distribution channels, which together provide customers a more secure and convenient way to access, send, receive and store funds.

Mobile money has transformed the financial services landscape in many LMICs by complementing and disrupting traditional banking. Mobile money platforms now process more than $2 billion a day through more than 1.2 billion registered mobile money accounts. More than $1 billion in international remittances is received into mobile money accounts every month, and $500 million is converted into e-money daily by 5.2 million unique mobile money agent outlets worldwide.

The mobile money industry has proven to be both viable and sustainable: as of 2020, there were 310 services in 96 countries. The services provided by mobile money providers (MMPs) are deepening, with the number of merchants accepting mobile money payments surging 29 per cent between December 2019 and June 2020. In 2020, the volume, activity and value of mobile money-enabled merchant payments all grew. Payments increased by 43 per cent, up from 28 per cent in 2019, generating more than $2.3 billion in monthly transactions in 2020, on average.

Public policy considerations

Regulation has a major impact on the uptake of mobile money services. Evidence from the Global Findex Survey and GSMA research show that enabling regulatory frameworks accelerate the development and adoption of digital financial services. When banks and non-bank providers, especially mobile operators, are allowed to deploy mobile money services and establish sound commercial partnerships, mobile money can be a catalyst for financial sector development. It significantly expands financial inclusion through lower transaction costs, better rural access and greater customer convenience. It can also provide the infrastructure to support a broad range of financial services, including insurance, savings and loans.

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

Global players in the financial services industry are adapting their business models to embrace the cloud and use new solutions provided by financial technology providers (fintechs) to

Resources:

GSMA Mobile Money Programme Website
GSMA Mobile Money Metrics Website (Mobile Money Regulatory Index)
GSMA Mobile Money Certification Website
GSMA Report: Demystifying Regulatory Concerns for the Use of Cloud Services in Mobile Money
GSMA Report: 2021 State of the Industry Report on Mobile Money

improve services and lower investment costs. The mobile money sector is gradually adopting these technological changes to scale up their services and increase financial inclusion sustainably. However, regulatory concerns about using the cloud for mobile money services, such as data privacy and supervision and oversight by local regulators, should be addressed without restricting use for mobile money providers.

Mobile money can help governments achieve policy objectives for safe, secure and efficient payment systems. It also makes a country's financial system less vulnerable by lowering the risks created by the informal economy and the widespread use of cash. For example, mobile money can usher more people from the informal to the formal economy and this, in turn, helps governments become more transparent and make more informed economic policy decisions. Government agencies can also reap the benefits of mobile money. Sending government-to-person (G2P) and person-to-government (P2G) payments via mobile money reduces cash-handling costs, security risks and theft of funds while improving transparency, speed and efficiency.

Trust is key to the success of mobile money. Over the past decade, mobile money has evolved from a niche product in a few markets to an emerging market phenomenon, bringing reliable financial services to unbanked populations. In many LMICs, mobile money has become the leading payment platform for the digital economy. The GSMA Mobile Money Certification is a global initiative to bring safer, more transparent and resilient financial services to millions of mobile money users around the world. Certification will help take the industry to the next level by improving quality of services and customer satisfaction, facilitating trusted partnerships, building trust with regulators and encouraging appropriate and proportional regulatory standards. Enhancing trust in mobile money is in the collective interest of the private sector, governments, regulators and consumers.

For mobile money to succeed, non-bank mobile money providers must be able to enter the market on an equal footing. This level playing field must be established via an enabling policy and regulatory framework. Policymakers and regulators should:

- Embrace reforms to enable mobile operators to launch and scale mobile money services.
- Allow market-led solutions to be implemented at the right time for consumers and providers, and ensure that government-led instant payment schemes have fair and inclusive governance principles and operating rules.
- Engage with mobile money providers and provide adequate guidance to ensure that regulatory uncertainty on cross-border data flows is not a barrier to the use of cloud services in the mobile money industry.
- Ensure that fiscal policy (taxation) is broad-based and not sector-specific. Taxes that discriminate against players and users in the financial services sector should be avoided, particularly given the positive externalities of mobile money services.
- Adopt risk-based approaches to risk management and encourage the implementation of appropriate and proportional regulatory standards.

GSMA Capacity Building

Background

The GSMA Capacity Building programme offers free training courses for policymakers and regulators. Since its launch in 2013, it has become the world's premier provider of specialist telecoms regulatory training, delivering courses to more than 8,000 regulatory professionals from more than 170 countries. Through a combination of engaging and interactive courses, expert trainers and in-depth research and analysis, the programme helps policymakers and regulators shape the development and reach of mobile services in their country and ensure they deliver the most benefit to citizens.

The courses help students understand and keep track of the latest policy and regulatory developments around the globe. Using real-world examples of regulatory good practice from different regions, the courses examine the impact of different approaches on the delivery of mobile services. Core areas covered include 5G, spectrum, competition policy, rural coverage and how to leverage mobile technology to achieve SDG targets.

The in-house policy experts who develop and teach the courses have backgrounds in telecommunications, law and financial services. Many also hold advanced academic qualifications. Through their work with the GSMA, they are in constant contact with governments and regulatory authorities around the world, which gives them a unique understanding of the most pressing issues facing regulatory authorities today.

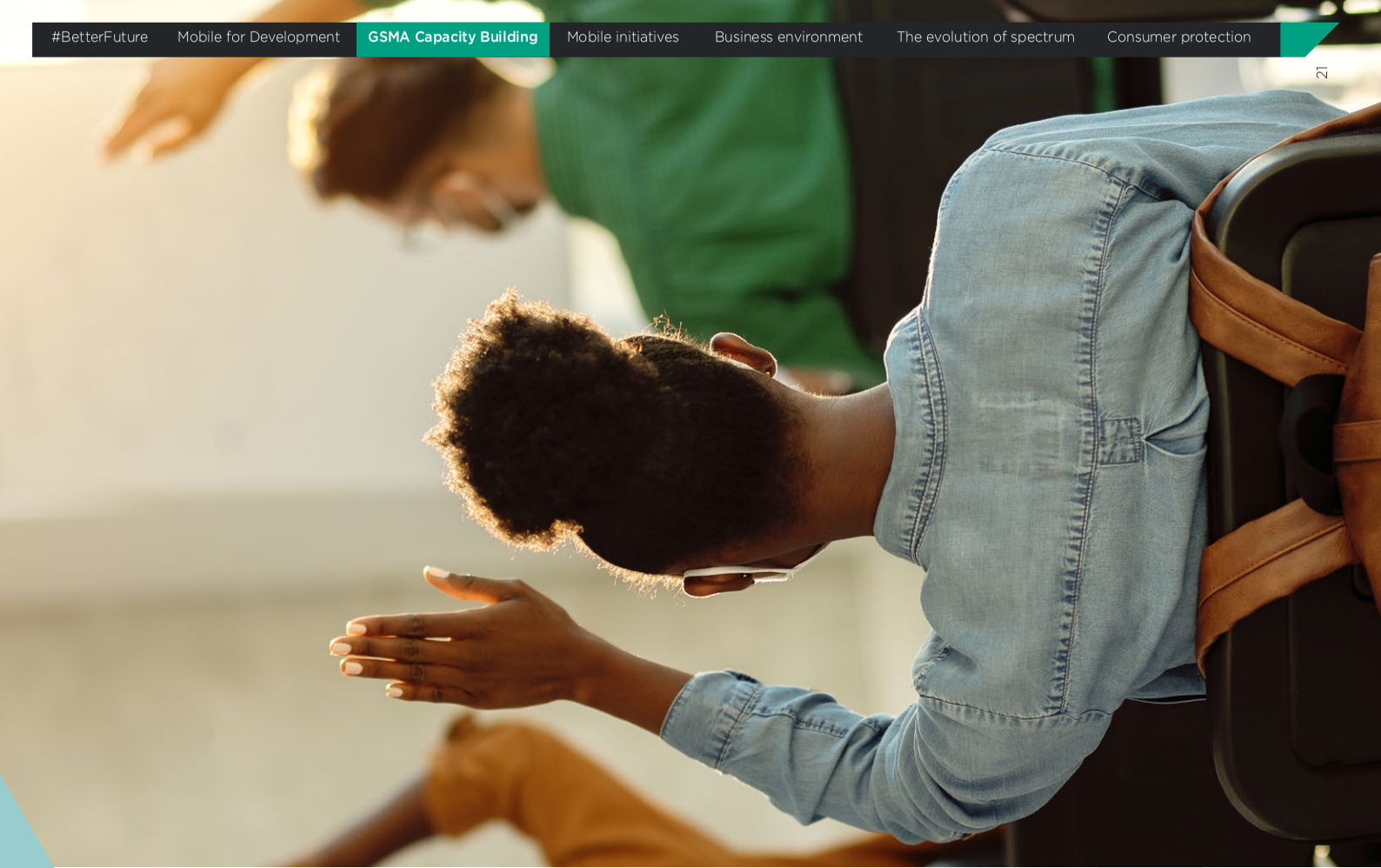
The courses are packed with the latest and most robust market statistics, analysis and insights thanks to the support of a global team of researchers, forecasters and analysts from GSMA Intelligence, the research arm of the GSMA. Training materials are accredited by the United Kingdom Telecommunications Academy.

Courses are suitable for professionals at any stage of their career and are offered in English and French. Available both face-to-face and online, policymakers and regulators have maximum flexibility in how they study. The in-person courses are between one and three days, while the online courses last between three and seven weeks.

To learn more about the training or to register for a course, visit: **www.gsmatraining.com**

Courses:

- **5G — The Path to the Next Generation**
- **Big Data Analytics and Artificial Intelligence for Impact**
- **Bridging the Mobile Gender Gap**
- **Competition Policy in the Digital Age**
- **Digital Identity for the Underserved**
- **Internet of Things**
- **Leveraging Mobile to Achieve SDG Targets**
- **Mobile Sector Taxation**
- **Personal Data in the Context of Mobile Networks**
- **Principles of Mobile Privacy**
- **Radio Signals and Health**
- **Spectrum Management for Mobile Telecommunications**
- **The Role of Mobile in Humanitarian Action**
- **Unlocking Rural Mobile Coverage**



Meet our students

Student profile

Pamela Tan,
Deputy Director,
Access and Interconnection Department,
Market Regulation Division of the Malaysian Communications and Multimedia Commission (MCMC)

Pamela Tan has been with the MCMC since 2006 and has a range of experience in policy planning, implementation and compliance. In her role as Deputy Director, Pamela assists in the development of policies and regulatory instruments for access regulation, monitoring licensee compliance, evaluating and ensuring access agreement registrations and access complaint resolution. She also works on capacity building initiatives.

Pamela took the 5G – The Path to the Next Generation course. She found it useful because it provided a basic understanding of 5G and the need for regulation and policies to evolve to encourage adoption and support the growth of the technology. While taking the course, Pamela was researching how to regulate 5G, which is already being rolled out in Malaysia nationwide, and found the information on network slicing particularly interesting. Pamela also took the Competition Policy in the Digital Age course. She appreciated the holistic view of competition policy the course provided and found it useful for the development of access and interconnection policies and regulatory instruments. The course also taught her about emerging bottlenecks in telecommunications and helped her understand the market definition process.

Pamela felt that the knowledge she gained from both courses assisted her in the review of the Access List, which is currently at a preliminary stage in Malaysia. The Access List ensures that all network facilities providers, network service providers and applications service providers can gain access to the necessary facilities and services on reasonable terms and conditions. The aim is to encourage downstream activities to flourish and create a more robust market environment that offers consumers more choice and value for money.

"*The courses helped me to progress further with my work, research, policy development and reviewing the relevant instruments.*"

Were the courses useful for Pamela's career? "*Knowledge of 5G is surely useful for a career in telecommunications, whether in Malaysia or other countries, since this is the next generation.*"

Student profile

Sumit Mishra,
Director of Compliance,
Department of Telecommunications (DoT),
Government of India

Sumit Mishra has more than 20 years of experience in telecoms management in the Indian Department of Telecommunications (DoT), as well as in telecom companies such as BSNL and RailTel Corporation of India. In his role as Director of Compliance at the DoT, Sumit is responsible for the coordination and monitoring of all service providers. This involves checking that the services offered by licensees are compliant, not only with licence conditions, but also with any directions issued in the public interest by the licensor. This includes the imposition of penalties, if they have been issued, in accordance with Government of India guidelines for Gujarat state.

Sumit enrolled in the 5G – The Path to the Next Generation course to ensure that he understood the basic concepts of 5G and the challenges that lay ahead for licensors and regulators. At the time he took the course, India was on the verge of rolling out 5G and the government was working with the major telecom operators to conduct trials of various 5G technologies and applications in different areas of the country. For example, Vodafone Ideal was conducting trials of 5G apps and services in the Gujarat area, including 360-degree virtual reality (VR) content playback and fixed wireless access broadband services.

The 5G course helped him better understand the role 5G technology can play in expanding broadband services in rural areas, which will soon be a driving force of the rural economy in India.

"*The 5G – The Path to the Next Generation course explained 5G-related topics in a very simple but effective manner and this will surely help when the actual field trials start.*"

Sumit really enjoyed learning about the experience of 5G in other countries and would welcome regular refreshers on 5G to stay abreast of rapid developments in this emerging technology.

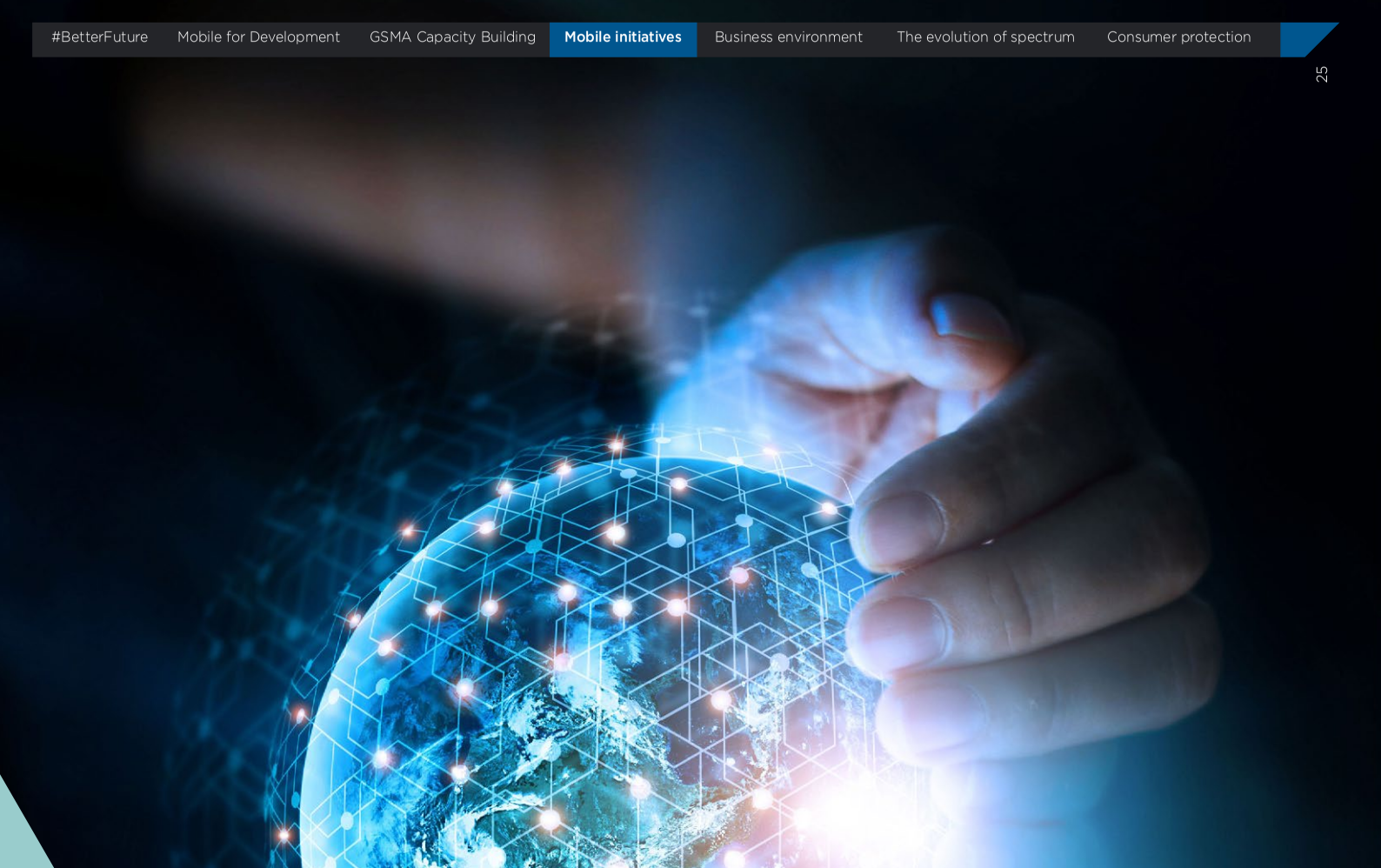
Mobile initiatives

Innovation and investment by the mobile industry continue to have an enormous impact on the lives of billions around the world. Mobile does not just provide connectivity; it also empowers people with an ever-growing range of life-enhancing services.

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

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

Each of the initiatives discussed in the following pages has its own public policy considerations and is related to one or more of the public policy topics covered in this handbook.



Future Networks

Introduction

The mobile industry continues to roll out fifth generation (5G) technology. Building on the achievements of 4G, 5G networks help the mobile industry capture the huge opportunity presented by the Internet of Things (IoT), usher in an era of even faster mobile broadband and pave the way for ultra-reliable, ultra-low latency services that may include exciting technologies such as tactile internet, augmented reality and autonomous vehicles.

As mobile operators deploy 5G networks, close collaboration between industry, policymakers and regulators will be needed to deliver on the promise of this next-generation technology and provide the infrastructure to operate it.

The GSMA is playing its part, providing guidance on innovations such as network slicing in 5G, while also working to boost population coverage of high-speed broadband and reduce the capital intensity required to roll out 5G technology. Work on infrastructure sharing and improvements to radio networks, for example, have already helped identify a potential four per cent reduction. This will be vital in helping the industry achieve its target of making 5G available to a third of the world's population by 2025.

Governments and regulators also have crucial roles to play. By adopting national policy measures that encourage long-term, heavy investment in 5G networks, and ensuring that sufficient harmonised spectrum is made available for 5G services, future 5G infrastructure will deliver significant benefits for citizens. Decisions made today will have lasting impacts, and the ultimate success of the technology will depend on governments and regulators making the roll-out of 5G a priority.

While they explore 5G technologies, mobile operators are also upgrading their networks to transition to all IP-based services. This is important, not just for consumers and business to reap the benefits of today's most advanced services, but also because IP-based networks and services will be the launchpad for 5G services.

5G: reaping the benefits

Background

Mobile telecommunications have had a phenomenal and transformational impact on society. From the earliest days of first-generation analogue phones, every subsequent generational leap has brought huge benefits to societies around the world and propelled the digitisation of more and more segments of the global economy. The mobile industry is now transitioning to 5G technology, building on the achievements of 4G while also creating new opportunities for innovation.

Industry, research, academic and government groups around the world are working to define the technology for 5G. 3GPP are completing their Release-17 definition of 5G and starting to work on Release-18, 5G-Advanced. One of the key objectives is a more sustainable mobile and technology sector and, because 5G will drive significant investments in energy, the mobile industry is moving to boost network efficiency as part of Release-18. This includes sleep modes for base stations when they are not transmitting, power amplifier improvements and the use of AI and machine learning to enhance data collection and internode communication to optimise energy savings. Other Release-18 goals include enhancing the performance and efficiency of 5G Massive MIMO; improving mobility for devices operating in sub-7GHz and mmWave frequencies; expanding the capability of integrated access and backhaul on cars and trains; and using smart repeaters that amplify signal but not noise.

2021 marked the first large-scale commercial launches of 5G, a mixed deployment of optimised 4G networks (5G Non-Standalone or NSA) and new 5G networks (5G Standalone or SA). By 2025, 5G could account for more than a billion connections and 5G networks are likely to cover a third of the world's population. The impact on the mobile industry and its customers will be profound. 5G is more than a new generation of technologies. It will also usher in an era in which connectivity is more fluid and flexible, with 5G networks adapting to applications and performance tailored precisely to the needs of users.

The key focus areas for 5G development and innovation include:

Internet of Things: 5G is needed to capture the huge opportunity presented by IoT. Conservative estimates suggest that, by 2025, there will be twice as many IoT devices as personal communication devices. As the ecosystem grows, the mobile industry will be expected to support bespoke services across industry verticals and develop next-generation services not possible with 4G networks.

Resources:

GSMA 5G Website
GSMA Blog: Five Things You Wanted to Know about 5G, But Never Dared to Ask
GSMA Report: The 5G Era: Age of Boundless Connectivity and Intelligent Automation
GSMA Report: 5G in China: Outlook and Regional Perspectives
GSMA Report: Smart 5G Networks: Enabled by Network Slicing and Tailored to Customers' Needs

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

Ultra-reliable, ultra-low latency services: Superior speed, high reliability and low latency will allow 5G to nurture new services that cannot be supported on existing 4G networks. Some of the services being considered include tactile internet, virtual/augmented reality, autonomous vehicles and factory automation.

Private networks: Private 5G networks allow private and public sector enterprises to bring a bespoke experience to indoor or outdoor facilities where high-speed, high-capacity or low-latency connectivity is crucial. They also address the need for dedicated bandwidth capacity and range, specialised security policies, high-quality connections and consistent, always-on service to help reduce downtime.

The GSMA aims to play a significant role in shaping the strategic, commercial and regulatory development of the 5G ecosystem, including the identification and alignment of suitable spectrum bands. Working closely with the mobile operators pioneering 5G, the GSMA is also engaging with governments and vertical industries (such as the automotive, financial services, health care, transport and utilities sectors) to develop business cases for 5G.

Public policy considerations

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

Additional spectrum will be required for 5G services, especially in very high frequency bands, to support significantly faster data speeds and enhanced capabilities.

However, progressive refarming of existing mobile bands should also be encouraged to support wider area 5G services. Governments and regulators can enable refarming and encourage heavy investment in 5G networks by supporting long-term, technology-neutral mobile spectrum licences with clear renewal procedures.

Three key frequency ranges are needed for 5G to deliver widespread coverage and support all use cases: sub-1 GHz, 1–6 GHz and above 6 GHz. Higher frequencies (mmWave), especially above 24 GHz, will be needed to support superfast speeds in hotspots. Lower frequencies will be needed to support wider area broadband access and IoT services. Exclusive licensing remains the principal and preferred regime for managing mobile broadband spectrum to guarantee quality of service and network investment.

However, the licensing regime in higher frequency bands, such as above 6 GHz, could be more varied than in previous mobile technology generations to suit more flexible sharing arrangements.

IP communication services

Background

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

IP communications is comprised of Voice over LTE (VoLTE), Video over LTE (ViLTE), Voice over Wi-Fi (VoWiFi) and Rich Communication Services (RCS):

» **VoLTE:** This offers a path from circuit-switched 2G and 3G voice services to all-IP packet-switched voice and includes a range of enhanced features for customers, such as high-definition audio quality and shorter call connection times. As of 2022, 233 mobile operators offered VoLTE services commercially in 106 countries.

» **ViLTE:** This enables operators to deploy a commercially viable, carrier-grade, person-to-person video calling service. Like VoLTE, it is based on IMS technology. As of 2022, there were 16 ViLTE services commercially available in 15 countries.

» **VoWiFi:** This allows operators to offer voice calling over Wi-Fi, providing many of the same benefits of VoLTE. As of 2022, there were 95 VoWiFi services commercially available in 51 countries.

» **RCS:** RCS marks the transition from messaging with circuit-switched technology to an all-IP world, using the same IMS capabilities as VoLTE and ViLTE. It incorporates messaging, video sharing and file sharing, enriching the communication experience of consumers.

The GSMA is working with leading mobile operators and equipment vendors to accelerate the launch of IP-based services around the world. This involves developing specifications, assisting operators with technical and commercial preparations for service launches and resolving technical and logistical barriers to interconnect.

Resources:

GSMA Report: Building the Case for an IP-Communications Future
GSMA All-IP Business Guide
Greenwich Consulting Report: The Value of Reach in an IP World
GSMA Report: AA.35: Procedures for the Development of Industry Specifications

Public policy considerations

To support the exponential growth in IP traffic, large-scale investments in network capacity will be necessary. Financing these investments will depend on predictable and stable regulatory environments in which operator-led communications can be closely aligned with regulatory requirements for mobile telecommunications, and mobile operators will have systems in place to ensure compliance.

Open standards. The GSMA is responsible for the industry specifications that many stakeholders use, including for eSIM, VoLTE, ViLTE, VoWiFi and RCS. In November 2019, the GSMA revised their procedures for the development and maintenance of industry specifications to reflect industry best practice and incorporate stronger measures for balance, openness and transparency in standard setting.

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

Lawful intercept. Mobile operators are subject to a range of laws and licence conditions that require them to intercept customer communications (and sometimes retain certain data, such as the time and content of the communication and the location, numbers or IP addresses of the participants) for disclosure to law enforcement agencies upon request. Specifications for IP communications are being developed to support the capabilities needed to meet these lawful interception obligations.

Voice over LTE

Background

Consumers expect seamless, carrier-grade voice services from mobile operators, regardless of the technology. Since the introduction of digital mobile technologies in the early 1990s, carrier-grade public mobile voice services have been delivered using the circuit-switched capabilities of 2G and 3G networks.

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

Some operators now have LTE networks that offer full national coverage and use VoLTE for voice calls while others still have only partial LTE network coverage. In most markets, full LTE coverage will take several years, requiring partial reliance on legacy voice services. For voice services, the transition is facilitated by the fact that VoLTE has been designed to support the seamless handover of calls to and from 2G and 3G networks.

As the industry starts to roll out 5G, communication services over 5G will become critical. In 2021, the GSMA published new and updated specifications to support 5G-based communications services and the application of VoLTE to Voice over New Radio (VoNR) for 5G.

VoLTE has several characteristics that distinguish it from internet-based voice services. These include carrier-grade call quality and reliability, support for emergency calls and universal interconnection with other carrier-operated voice services, which means customers can make calls to, or receive calls from, any phone number in the world. By contrast, most internet-based voice services are not managed for service quality and may be restricted to closed user groups.

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

Public policy considerations

Since VoLTE is an evolution of carrier-grade mobile voice services historically provided by circuit-switched 2G and 3G networks, regulators should not apply additional or specific regulations to VoLTE services.

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

Resources:

GSMA Networks Group Website
EEWorld Online: VoLTE — What Makes Voice Over IP "Carrier-grade"?

Internet of Things (IoT)

Introduction

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

IoT involves connecting devices to the internet across multiple networks to allow them to communicate with us, applications and each other. It will add intelligence to devices we use every day and, in turn, have positive impacts on the economy and broader society.

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

The GSMA is encouraging the development of the nascent IoT ecosystem by defining industry standards, promoting interoperability and encouraging governments to create a supportive environment that will speed the growth of IoT globally.

Advanced air mobility

Background

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

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

The rapid development of this market means regulators are struggling to keep pace. However, regulatory efforts are focused on creating frameworks that will allow the sector to develop and innovate while also limiting risks related to safety, privacy and data protection. The fact that drones fly across borders adds another layer of complexity.

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

Resources:

GSMA Internet of Things – Advanced Air Mobility Website

Public policy considerations

New regulatory frameworks for drones should ensure that they can, where required, be equipped with SIM cards and a communications modem to allow the drone ecosystem to benefit from mobile connectivity. This would have many benefits for the drone industry:

- Mobile networks provide a global, interoperable and scalable platform that allows the drone market to develop and benefit from the existing mobile ecosystem.
- Many mobile operators already run 4G LTE networks, which meet extremely high-bandwidth and low-latency requirements while also offering huge scalability and exceptional quality of service.
- The mobile industry already works with IoT partners throughout the value chain to embed privacy and security in IoT technologies. These collaborations allow the drone market to benefit from initiatives such as the GSMA *Security Guidelines and Privacy by Design Toolkit*.

By providing secure, high-quality connectivity with control centres, mobile connectivity can also help ensure that drones are controlled and operated safely. This has several potential benefits for the drone ecosystem:

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

To ensure licensed mobile spectrum is available for drone connectivity, there needs to be cooperation between the regulatory authorities responsible for spectrum and the regulators responsible for drones. By working together, they could remove barriers to the use of existing licensed mobile spectrum for drone connectivity.

Connected vehicles

Background

The automotive world is about to undergo the single greatest revolution in its history. Autonomous vehicles and intelligent transport systems (ITS) are set to transform the efficiency, comfort, safety and environmental impact of road transport.

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

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

The primary platform for these activities is the Connected Vehicle Forum. Established by the GSMA, the Forum promotes dialogue among all stakeholders in the automotive and C-ITS ecosystem and seeks innovative ways for these sectors to leverage mobile technology.

One example is the GSMA Embedded SIM Specification, which provides a single mechanism for the remote provisioning and management of M2M connections, allowing "over-the-air" provisioning of an initial operator subscription, as well as subscription changes from one operator to another.

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

Resources:

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

Public policy considerations

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

Connected vehicle apps and services have several distinct features: they need to operate globally, support long device life, integrate with local intelligent transport solutions and comply with local security, data protection, privacy and emergency regulations. Policymakers and regulators must appreciate and understand these differences if they are to implement policies that allow global business models to develop, and to ensure that rules apply consistently to all players in the value chain.

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

Regulators should adopt a technology-neutral approach to this spectrum rather than mandating or favouring one approach. It is equally important that technology-neutral spectrum licences are adopted, as this will allow existing mobile bands to be refarmed for 5G and enable lower latency connectivity and improved emergency response times.

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

Privacy and data protection for IoT

Background

The IoT offers significant opportunities and potential for data-driven innovation to achieve economic, social and public policy objectives and improve our daily lives. It enables new apps and services that can empower consumers to monitor their health, manage their energy consumption and benefit from smart home and city solutions. This can lead to many positive outcomes, such as lower pollution levels and healthier lifestyles.

Many IoT services will be designed to create, collect or share data, some of which will not be considered personal, such as data about the physical state of machines or weather conditions. However, some IoT services aimed at consumers are likely to involve generating, distributing and using detailed personal data. For example, a smart home appliance may use data about a person's eating or exercise habits to draw inferences about their health, or develop a profile based on their shopping habits to offer them personalised discounts.

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

Resources:

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

Public policy considerations

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

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

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

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

Smart cities and IoT

Background

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

National and local governments are increasingly interested in "smart cities" and using mobile communications technology and the IoT to solve many of the challenges cities face today. For example, smart city technology can tackle traffic congestion, improve public transport infrastructure, create safer streets with better lighting and add intelligence to utilities infrastructure via smart meters and smart grid solutions. It also opens new commercial and investment opportunities for cities.

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

Resources:

GSMA Smart Cities Website
GSMA Report: Maximising the Smart Cities Opportunity: Recom
GSMA Report: Keys to the Smart City
GSMA Video Case Study: Smart City Tainan

Public policy considerations

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

» **Adopt an agile institutional framework and governance mechanisms.** A smart city needs an institutional framework that ensures coordination and support throughout the life of a project. The smart city agency will need to be agile and, ideally, independent from traditional city departments. It should, however, be accountable to a governance body represented by city institutions.

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

» **Communicate the objectives and benefits of smart city projects effectively.** Establishing dialogue with the local community is essential to the design and functionality of smart city services. Digital media can help to involve citizens at each step and highlight the tangible benefits a smart city project will deliver.

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

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

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

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

Identity

Introduction

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

The digital economy is predicated on trust, and interactions, whether social, commercial, financial or intellectual, require a proportionate level of trust in the other party or parties involved. Today, consumers are seeking easy access to digital services that also protect their privacy. Online service providers must therefore reduce friction in digital transactions while maintaining a seamless and secure user experience. Increasingly, governments are regulating and demanding that digital identity solutions use global standards to ensure interoperability, privacy, scale and cost-effectiveness.

To this end, the mobile industry is developing a consistent and standardised set of services for managing digital identity. The unique advantages of mobile operators, such as SIM cards, registration processes, contextual network information and fraud mitigation processes, give them the ability to provide strong customer authentication and interoperable, federated identity management solutions to enable consumers, businesses and governments to interact in a private and secure environment.

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

Together, mobile operators are bringing mobile identity solutions to market that can reach tremendous scale. By using consistent, easy-to-access technologies across the digital identity ecosystem, these solutions can provide a consumer experience that is scalable, safe and secure, and puts users in control of their data and personal information.

There are many advantages to mobile operators providing a digital identity service:

- **Flexibility to innovate:** flexibility to provide multiple authentication factors and the ability to add consumer functionality, such as “add to bill” or “click to call”.
- **The mobile device:** ubiquitous, personal and portable; sensitive to location; and capable of being disabled and locked.
- **The SIM card:** strong, real-time authentication; encryption for storing certificates; and other secure information.
- **KYC standards:** strong registration and fraud detection processes.
- **Verified subscriber data:** ready-for-mobile identity.
- **Robust regulatory requirements:** established systems to handle personal data safely.
- **Customer service:** sophisticated customer care processes and billing relationships.
- **The network:** secure by design, a mobile network can disable a device’s SIM card and flag the device as lost or stolen in a global database.
- **Business processes:** ensures that the user has a way to report events, such as lost/stolen devices or an account compromise/takeover.

Mobile Connect

Background

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

The key benefits of Mobile Connect include:

» **Ease of use:** passwords are not required since the mobile phone itself is used for authentication.

» **Secure and strong customer authentication:** user experience is improved as there are no passwords to steal.

» **Secure and trustworthy digital transactions:** security and trust are built into the transaction since it confirms the user's location, identity and usage.

» **Privacy protection:** the operator confirms the user's credentials and the user gives consent to share this information.

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

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

Resources:

GSMA Mobile Connect Website
GSMA Identity Website
GSMA Report: Mobile Connect for Cross-Border Digital Services: Lessons Learned from the eIDAS Pilot
Mobile Connect Privacy Principles
GSMA Report: Mobile Connect: Mobile High-Security Authentication
GSMA Report: Mobile Identity: A Regulatory Overview
GSMA, World Bank and SIA White Paper: Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation

Public policy considerations

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

» **Identifying and assessing existing legal, regulatory and policy challenges and barriers** that affect the development of mobile identity services.

» **Applying best practices and advances in technology** to foster the deployment of widescale mobile identity services and transactions.

» **Engaging with mobile operators and the wider digital identity ecosystem** to facilitate greater collaboration between the public and private sectors and encourage interoperability and innovation.

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

The mobile industry has a proven track record of delivering secure networks and developing 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 enhance the security features used to protect mobile networks and their customers.

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

AI for Impact

Mobile big data analytics and artificial intelligence (AI) are emerging as powerful forces for change in business and society, and the potential of these technologies to unlock life-changing benefits is only beginning to be seen. When grounded in ethical principles that protect privacy, these solutions can truly change the world for the better.

The mobile industry is harnessing big data to work with governments and global agencies to tackle some of the greatest challenges of our time: humanitarian crises, infectious disease, natural disasters and climate change. Protecting privacy is at the core of big data developments, and the mobile industry is committed to the responsible use of data and protection of privacy. By aggregating and anonymising the data collected by their networks, mobile operators can provide insights into human movement patterns without compromising individuals' privacy. When this data is enriched with third-party data sources, it can enable the public sector to make evidence-based decisions on when, where and how to deploy resources.

Climate Action

The mobile industry recognises the urgency of tackling the global climate crisis, which is why we are taking action to mitigate our impacts and combat climate change as part of the solution.

The COVID-19 pandemic has shown us how vital digital infrastructure and connectivity has become to working, socialising, accessing medical care, learning and many other aspects of our lives. The mobile sector stands ready to help societies transition to lower carbon ways of living and a net-zero carbon economy. This requires not only a common vision, but also an understanding of diverse markets and the steps needed to create the investment incentives, infrastructure and policy frameworks to create a net-zero carbon economy.

In 2019, the GSMA, with the support of our board members, launched an industry-wide Climate Action initiative and made a milestone commitment: to transform the mobile industry to reach net-zero carbon emissions by 2050, at the latest. Progress is being made:

Resources:

GSMA AI Ethics Principles
The GSMA COVID-19 Privacy Guidelines
GSMA AI for Impact Toolkit
GSMA Report: GSMA Climate Policy
GSMA Report: Mobile Net Zero: State of the Industry on Climate Action 2021
GSMA Report: The Enablement Effect
GSMA Climate Action Website
COP26 – Climate Hub

- The mobile sector has worked collaboratively to create an industry-wide climate action roadmap to achieve net-zero greenhouse gas (GHG) emissions by 2050, in line with the Paris Agreement.
- Eighty per cent of the global mobile industry by revenue is now disclosing their climate impacts, energy and GHG emissions via the internationally recognised CDP global disclosure system.
- Sixty-five per cent of the global mobile industry by revenue has committed to science-based targets to cut their carbon emissions rapidly over the next decade.
- The mobile sector has been recognised by the UN Race to Zero as a breakthrough industry.

The GSMA is providing support and guidance for mobile operators to commit to and set targets aligned with the net-zero pathway. While the mobile industry is taking major steps to reduce emissions, it is having an even greater impact by supporting other sectors to reduce their emissions through efficiencies created by smart-connected M2M technologies and behaviour change. Research conducted by the GSMA with the Carbon Trust in 2019 found that while the mobile industry is currently responsible for around 0.4 per cent of carbon emissions globally, it enables carbon reductions in other sectors that are 10 times greater, equivalent to approximately four per cent of global emissions.

Business environment

Introduction

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

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

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

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

Policies for progress

Resetting policy and regulation to drive the digital economy

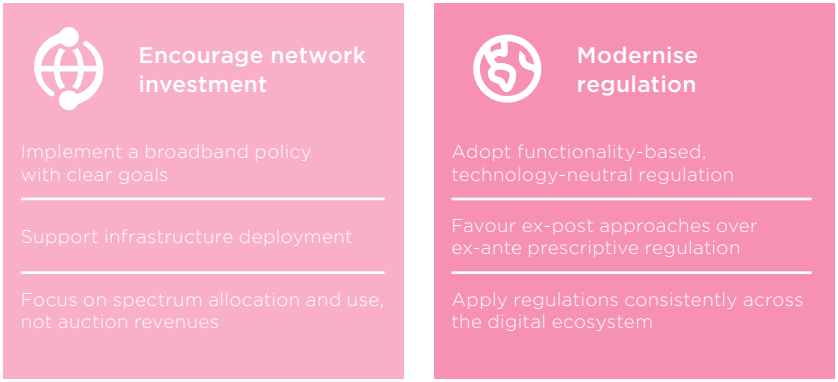
Digital technologies have fundamentally changed our daily lives, from shopping and entertainment to managing household finances. When given the opportunity, consumers have been quick to embrace digital tools. Many governments, recognising the value of mobile to society, have implemented bold policies to cultivate the digital economy while extending connectivity to underserved communities.

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

Figure 1 identifies four areas of policy action related to network investment, regulation, promoting the digital economy and demonstrating digital leadership.[2]

Emerging technologies are driving new business models and blurring boundaries between once-distinct markets. Yet, regulatory systems developed during the early years of mobile telecoms are still in place in many countries, and reforms have not kept pace with the converging and

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



2. GSMA. (February 2017). Embracing the Digital Revolution: Policies for Building the Digital Economy

dynamic digital ecosystem. Tomorrow's technologies cannot be allowed to be stifled by yesterday's regulations, which need to be reframed for the digital and mobile age. The good news is that policymakers recognise the need for change. In many jurisdictions, such as the European Union, reforms are underway that will protect competition and consumers without impeding social and economic progress. By updating the regulatory framework, policymakers can ensure that government and industry are aligned and working to foster an inclusive digital society for all.

Promote the digital economy

Support data security and privacy

Push digital literacy and lifelong learning

Encourage the digitalisation of companies

Demonstrate digital leadership

Encourage the use of digital IDs

Support digital financial infrastructure

Introduce digital government services

Community networks

Background

Community networks are a "do-it-yourself" approach to connectivity: local, community-owned (or community-managed) networks that address specific local connectivity needs. They are usually established in areas that are not commercially viable for mobile operators to cover and typically operate on a small scale, addressing discrete market failures. They can therefore be effective complements to connectivity efforts led by mobile operators.

Community networks have been made possible by advances in technology that have reduced barriers to network deployment and management and enabled non-operators to build and deploy mobile and internet connectivity solutions. Largely technology-neutral, these solutions are tailored to the needs of the community or local setting, and can include the use of modular and simplified infrastructure, renewable energy, a variety of backhaul methods (including an ISP or Wi-Fi backbone, VSAT and WiMAX) and open connectivity standards. Community networks often use Wi-Fi technology in unlicensed spectrum, although very few countries have assigned spectrum specifically for their operation.

Community networks are generally funded through mechanisms such as crowdfunding, local financial contributions, the donation of connectivity expertise and equipment and sometimes customer usage fees. Since they offer a specific solution to often unique geographical, commercial and logistical connectivity challenges, they are often context-specific and difficult to scale. Only a few community networks have established a lasting and financially sustainable business model.

Debate:

- ***What role can community networks play in a national connectivity approach?***
- ***How can mobile operators leverage community networks to support their rural connectivity strategies?***
- ***How should community networks be supported and regulated to ensure high-quality, local connectivity while maintaining a level playing field with mobile operators?***

Resources:

The Internet Society: Community Networks
WNDW Report: Wireless Networking in the Developing World

Industry position

Community networks can complement the efforts of mobile operators to expand coverage since they are an opportunity to deliver the transformative benefits of connectivity to locations that are not commercially viable. By doing so, they can drive ICT usage, increase digital skills, support local business development and increase uptake of digitally delivered public services within the communities they serve.

Community networks have limitations, however. They typically do not have the resources or expertise to sustain investment in new innovations or address cybersecurity risks as effectively as scaled commercial networks. Regulatory uncertainty or constraints can also limit the potential of community networks and hamper the roll-out of larger-scale commercial connectivity networks.

A level playing field is essential, and regulation should empower both community networks and mobile operators to drive connectivity and accelerate digital inclusion. The regulation and policies applied to community networks should not impair or discourage the deployment of larger-scale commercial network operations and put mobile operators at a disadvantage.

Where Wi-Fi cannot provide a suitable solution, voluntary spectrum sharing can be an interesting opportunity to open access to new spectrum for community networks. However, careful planning is required, and it is essential that the chosen approach protects the needs of incumbents, supports the needs of new users and does not limit the evolution of the spectrum band.

Voluntary spectrum trading through secondary market transactions should be considered to enable spectrum access for community networks. Countries should have a regulatory framework that allows mobile operators to engage in voluntary spectrum trading.

Spectrum that is set aside for community networks in mobile bands may be underused. As a result, it may not just waste a valuable resource, but also threaten the success of commercial networks through reduced coverage, slower roll outs and worse performance.

Competition

Background

Mobile phones are the most widely adopted consumer technology in history. In large part, this success is due to competition in the mobile industry that has driven innovation.

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

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

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

Current competition policy is also being challenged by the competitive advantage conferred on some companies through their ability to collect and analyse large troves of data. Combined with powerful network effects and the tendency for markets to tip in favour of dominant platforms, this can harm consumers, hinder competition and stifle innovation.

The ability of competition policy and enforcement to deal with issues arising in digital markets is, therefore, key to the competitive development of the entire digital economy.

Debate:

- ***How should markets be defined in the digital age?***
- ***How can traditional competition tools be applied in the digital age?***
- ***Are significant market power (SMP) access remedies still appropriate?***

Resources:

GSMA Competition Policy Website
GSMA Handbook: Competition Policy in the Digital Age
GSMA Report: The Data Value Chain

Industry position

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

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

Regulators and competition authorities must recognise the dynamic nature of competition in the digital age. Internet players adopt new and different business models to offer services to customers, such as advertising-supported services that rely on sophisticated web analytics. Regulators and competition authorities need to understand these models and map their competitive impact before imposing regulatory obligations or competition law commitments. Otherwise, services that are in competition with each other may end up being regulated differently. For example, players that adopt traditional business models that are better understood may find themselves subject to greater scrutiny.

Including these new types of competitors in market assessment reviews could reveal there is much more competition in communications services than regulatory and competition authorities currently recognise. It could also demonstrate the potential for regulatory policy goals to be achieved through competition law. A basic principle of economic regulation is that regulation should not be imposed if competition law is sufficient to deal with the issues identified. Therefore, regulation of licensed providers could be lessened or may no longer be needed. Competition law itself could also be improved and updated to tackle the issues arising in digital markets more effectively.

Deeper dive: Competition in digital markets

The global economy is undergoing a major transformation. The rapid uptake of technologies, including mobile communications, digital platforms, big data, cloud computing and social media, is changing the nature of products and services and how people interact. This transformation disrupts existing business models and industries while also offering significant potential to enrich lives and raise living standards.

Figure 2 **Characteristics of the digital economy**

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

Competition in digital markets has certain features that distinguish it from competition in traditional markets, including:

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

These differences in the digital ecosystem challenge existing policies and demand an update of the competition framework and a more nuanced approach to competition policy.

Deeper dive: Recommendations for resetting competition policy frameworks

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

Figure 3 **Resetting competition policy frameworks: recommendations**

Market definition and market power

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

The total welfare standard

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

Ex-ante and ex-post regulation

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

Institutional arrangements

- Adopt interim measures to accelerate ex-post enforcement and mitigate potential harm from anti-competitive conduct.
- Reassess institutional arrangements.

Efficient mobile market structures

Background

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

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

The high level of competition in the mobile services market has caused the tariffs charged to mobile users to fall steadily and significantly over the past few years. At the same time, consumption of mobile services, particularly mobile data, has grown steadily, with users typically getting more for their money.

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

Some regulators have used spectrum caps – limits on the amount of spectrum one entity can hold – to influence market structure. However, spectrum caps can have unintended consequences, including inefficient allocations of spectrum and/or reduced incentives to invest. Since this ultimately produces poor outcomes for consumers, they must be considered carefully.

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

Resources:

GSMA Report: Assessing the Case for In-country Mobile Consolidation
GSMA Report: Assessing the Case for In-country Mobile Consolidation in Emerging Markets
GSMA Report: Assessing the Impact of Mobile Consolidation on Innovation and Quality
GSMA Report: Assessing the Impact of Market Structure on Innovation and Quality in Central America

Industry position

When assessing mobile mergers, policymakers should consider the full range of benefits of mergers, including price effects, innovation, investments and the use of spectrum over the short- and longer term.

Investment and quality of service. Competition authorities should consider placing greater emphasis on how mergers may affect an operator's ability to invest. Growing demand for data services requiring ever-increasing bandwidth necessitates continuous investment in new capacity and technology.

Positive spill-over effects in the wider economy. Improvements to digital infrastructure support economic growth by increasing productivity across the economy.

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

Unit prices. There is no robust evidence to suggest that four-player markets have produced lower prices than three-player markets in the past decade, in Europe or elsewhere. Mergers can accelerate the transition between technology cycles in the mobile industry (which are responsible for significant reductions in unit prices), leading to improvements in quality and innovation in services. As the market moves from voice to data, the global volume growth rate of mobile networks is accelerating. This requires more concentrated market structures to meet the investment challenge, drive mobile data unit prices down and fuel demand for mobile data services.

Effects of remedies on investments and use of spectrum. Mergers that compel mobile operators to provide third parties with access to their networks could reduce incentives to invest and significantly diminish benefits for consumers. In three cases where the European Commission's Directorate-General for Competition made a network entry option available (Ireland, Germany and Austria), nobody took the option, even though it was arguably offered on favourable terms. Remedies that involve reallocating network assets or reserving spectrum for other operators could, in some cases, deter investment and lead to the underuse or misuse of resources.

Debate:

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

Deeper dive: The dynamic benefits of mergers

Recently, there has been heated debate about the effects of consolidation on the performance of mobile markets following mergers in key European markets, including Austria, Germany, Ireland and the UK. While some argue that consolidation has a detrimental effect on competition and prices, others argue that, without consolidation, mobile markets will not achieve the necessary scale and fail to attract sufficient investment.

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

Since 2015, at least seven other studies[4] have examined the relationship between market structure, innovation and investment, as measured by mobile operators' capital expenditure (CapEx). None found that greater market concentration resulted in lower investment per operator or lower total country investment.

Meanwhile, initial studies have found that investment always increases with market concentration, suggesting that the Hutchison/Orange merger would have had a positive effect on Austrian consumers.

CERRE (2015) found that, on average, a 10 per cent increase in the Herfindahl-Hirschman Index boosts the CapEx of mobile operators that have merged by 24 per cent. In 2016, Houngbonon & Jeanjean and found that markets with four players average 14 per cent lower investment per operator than markets with three players, and that a higher number of operators tends to decrease investment. DG Competition (2017) found that investment

3. GSMA. (2017). *Assessing the Impact of Mobile Consolidation on Innovation and Quality: An Evaluation of the Hutchison/Orange Merger in Austria.*

4. CERRE (2015), Frontier (2015), Houngbonon and Jeanjean (2015), Houngbonon and Jeanjean (2016), HSBC (2015), WIK (2015) and DG Competition (2017).

5. Although WIK (2015) found that market structures that provide higher profit margins and greater economies of scale (both enhanced by market consolidation) boost total CapEx per country.

per operator increased as a result of the five-to-four merger in the UK in 2010, although no statistically significant effect was found when analysing investment per subscriber.

A second set of studies (Houngbonon and Jeanjean, 2016, and HSBC, 2015) suggests that greater market concentration increases CapEx per operator only when their profit margins are less than 37 to 44 per cent. Operators in most four-player markets are below this threshold, including the Austrian operators before the merger. These studies suggest that the introduction of competition initially has a positive effect on investment, but that as mobile markets become less concentrated it has a negative effect. Other studies have found that investment does not depend on market structure (WIK, 2015 and Frontier, 2015), suggesting that a mobile merger would have a neutral effect on outcomes such as network quality and coverage.[5]

While many believe that consolidation is likely to lead to less investment by operators, there was evidence that concentration leads to increased investment after a merger. This is because larger operators enjoy economies of scale that enable them to extend coverage and undertake network upgrades. They are also financially stronger due to higher profit margins and better access to complementary assets and commercial partnerships, which can lead them to expect higher returns from their investments.

Infrastructure sharing

Background

Common in many countries, infrastructure sharing can provide additional capacity in congested areas where space for sites and towers is limited and help to expand coverage in underserved geographical areas.

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 also reducing costs for operators.

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

Industry position

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

While it may, at times, be advantageous for mobile operators to share infrastructure, network deployment remains an important 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.

National regulatory frameworks should facilitate all types of infrastructure-sharing arrangements. This can include sharing various components of mobile networks, including so-called passive and active sharing. In some cases, site sharing (a type of passive sharing) increases competition by giving operators access to sites necessary to compete on quality of service and coverage.

Infrastructure-sharing agreements should be governed by 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: Unlocking Rural Coverage: Enablers for Commercially Sustainable Mobile Network Expansion
ITU Mobile Infrastructure Sharing Website
ZDNet Article: Learning to Share: Could Tower-Sharing be the Solution to Rural Networks' Problems?

Debate:

- *Should regulators oversee, approve or manage infrastructure-sharing arrangements?*
- *What role should governments play in the development and management of core infrastructure?*

Deeper dive: Types of infrastructure sharing

Infrastructure sharing can be passive or active. Passive sharing includes site sharing, when 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, when 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. RAN sharing may create operational and architectural challenges. With core network sharing, operators also share the core functionality, demanding more effort and alignment, particularly the compatibility of the operators' technology platforms.

Infrastructure sharing optimises the use of assets, reduces costs and avoids duplication of infrastructure (in line with urban and national planning objectives).

Figure 4 **Mast sharing**

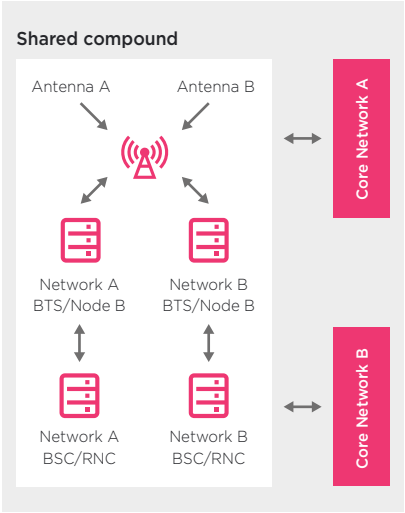
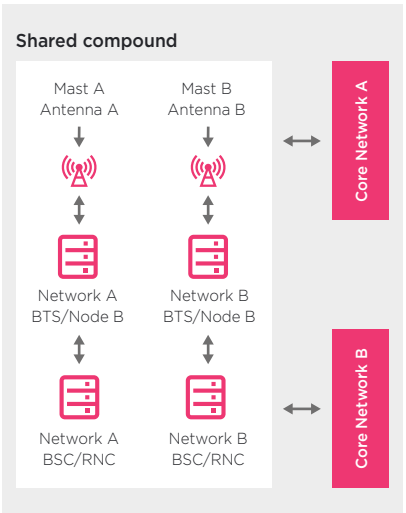


Figure 5 **Site sharing**



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; and
- Reduce costs for operators.

Figure 6 Full RAN sharing

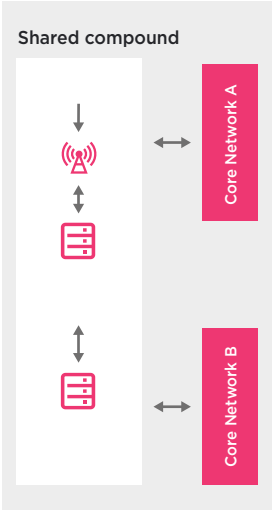
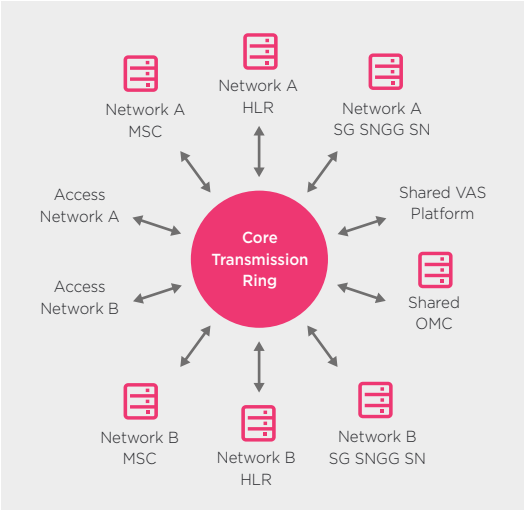


Figure 7 Shared core network elements and platforms



Intellectual property rights

Background

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

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

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

However, in the past few years, there have been radical changes in the licensing of telecommunications technology (i.e. the prime use of patent portfolios in telecommunications). Initially, patents were used to preserve a company's "freedom to operate" (i.e. its ability to bring its products to market by seeking large portfolio cross-licences). Increasingly, patents have become tradeable, income-generating assets (via the "secondary patent market") capable of being asserted against start-ups, small and large companies, and, in certain cases, used to stifle competition.

Debate:

- ***Now that patents have become tradeable and an income-generating asset, can they still be considered a tool to support and promote innovation?***
- ***Are Patent Assertion Entities (PAEs) having a negative effect on competition?***

Industry position

The secondary patent market has greatly encouraged the rise of non-innovating, non-practicing, patent monetisation and licensing or enforcement entities, known as PAEs. Usually, PAEs are purchasing patents (rather than developing and licensing technology) to be asserted against manufacturers and operators already using the technology.

There are several reasons mobile operator networks have become a premium target for so-called "patent trolls" in Europe, America and Asia. These include:

» The complexity of mobile operator networks;

» The scale of investments needed to build them;

» The level of revenues they generate; and

» The reliance of these networks on standards-based technology.

The multiple costs associated with PAE litigation and threats of injunction (as leverage in demands for disproportionately high licensing fees) have a detrimental effect, not only on a mobile operator's business, but also on innovation and standardisation in mobile telecommunications.

Increasing PAE litigations and adversarial/ litigious licensing negotiations highlight the need for greater clarity on the licensing of standard essential technology.

These efforts should focus on:

» The reliance of the public on mobile telecommunications technology and the ability of mobile operators to deliver such services;

» The fact that disruption to these services, even somewhat, will have a severe negative effect on people's lives;

» The importance of maintaining the integrity of mobile telecommunication services and ensuring continuous investment and adoption of new technologies in the telecommunications market; and

» The need to incorporate appropriate rules and regulations in frameworks governing the seeking and granting of injunctions in predatory patent assertion cases (to allow the judiciary to consider the above points).

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 IMR prices and the lack of price transparency, which can cause bill shock for consumers.

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

In the European Union, roaming regulation has been in place since 2007 and, in June 2017, "roam-like-at-home" was introduced across the EU, with mobile operators required to include it by default in contracts. Travellers can call, text and surf on their mobile devices in any EU country for no more than what they pay at home. Operators can implement "fair use" policies to prevent the abuse of regulated roaming services.

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

Resources:

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

Industry position

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

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

» **Transparency:** In June 2012, the GSMA launched the Mobile Data Roaming Transparency Scheme, a voluntary commitment by mobile operators to give consumers greater visibility of roaming charges and their mobile data usage 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 structural barriers have been removed. The costs and benefits of regulation must be assessed carefully and consider unique economic factors, such as national variations in income, GDP, inflation, exchange rates, mobile penetration rates, the percentage of the population that travels internationally and the 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 also deters investment.

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?*

Mobile termination rates

Background

Mobile termination rates (MTRs) are the fees charged by mobile operators to connect a phone call originating from a different network. Setting regulated MTRs continues to be a focus of regulators in both high- and low-income countries, and many different approaches have been developed to calculate 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 an appropriate regulated rate for call termination be calculated?*
- *Is the drive towards ever lower mobile termination rates, especially in Europe, a productive and appropriate activity for regulators?*
- *Once termination rates have fallen below a certain threshold, is continued regulation productive?*
- *What is the long-term role of regulated termination rates in an all-IP environment?*

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

Resources:

Vodafone Report: The Impact of Recent Cuts in Mobile Termination Rates Across Europe
GSMA Report: The Setting of Mobile Termination Rates: Best Practice in Cost Modelling
GSMA Report: Comparison of Fixed and Mobile Cost Structures

Industry position

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

Evidence suggests that reductions in MTRs are not beneficial after a certain point. The setting of regulated MTRs is complex and requires a detailed cost analysis, as well as careful consideration of its impact on consumer prices and, more broadly, on competition.

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

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

Net neutrality

Background

While there is no single definition of net neutrality, it often refers to issues concerning the optimisation of traffic over networks. Advocates assert that all traffic carried over a network should be treated equally, but others contend that offering different service levels for different applications enhances the user experience.

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

Mobile operators face unique operational and technical challenges in providing fast, reliable internet access to their customers, due to the shared use of network resources and limited available spectrum. Unlike fixed broadband networks where a known number of subscribers share capacity, the capacity demand at any given cell site is much more variable, as the number and mix of subscribers constantly changes, often unpredictably. The available bandwidth can also fluctuate due to variations in radio frequency signal strength and quality, which can be affected by weather, traffic, speed and the presence of interfering devices, such as wireless microphones.

Not all traffic has equal demands on a network. Voice traffic is time-sensitive while video streaming typically requires large amounts of bandwidth. Networks need to be managed in a way that accommodates all types of traffic and supports innovations with 5G and IoT. The principle of the open internet and allowing operators to offer their customers a variety of service options are not mutually exclusive. As the net neutrality debate has evolved, policymakers have come to accept that network management plays an important role in service quality.

Resources:

GSMA Net Neutrality Website

Statement

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

Industry position

Mobile operators need to be able to actively manage network traffic to meet the different needs of consumers.

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

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

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 by comparing performance differences in a transparent way.

Mobile operators compete in many areas, including 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.

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?***

Deeper dive: Traffic management

Traffic growth, the deployment of next-generation technologies and the emergence of new types of services are presenting mobile 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 meets different consumer needs and service attributes.

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

Traffic management techniques are applied at different layers of the network, including admission control, packet scheduling and load management. In addition, operators need to cater to different consumer preferences so that 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 with and establish new business models that align investment incentives with technological and market developments, and to create additional value for their customers. As the operational and business models of networks evolve, a host of innovative services and business opportunities will emerge.

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

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

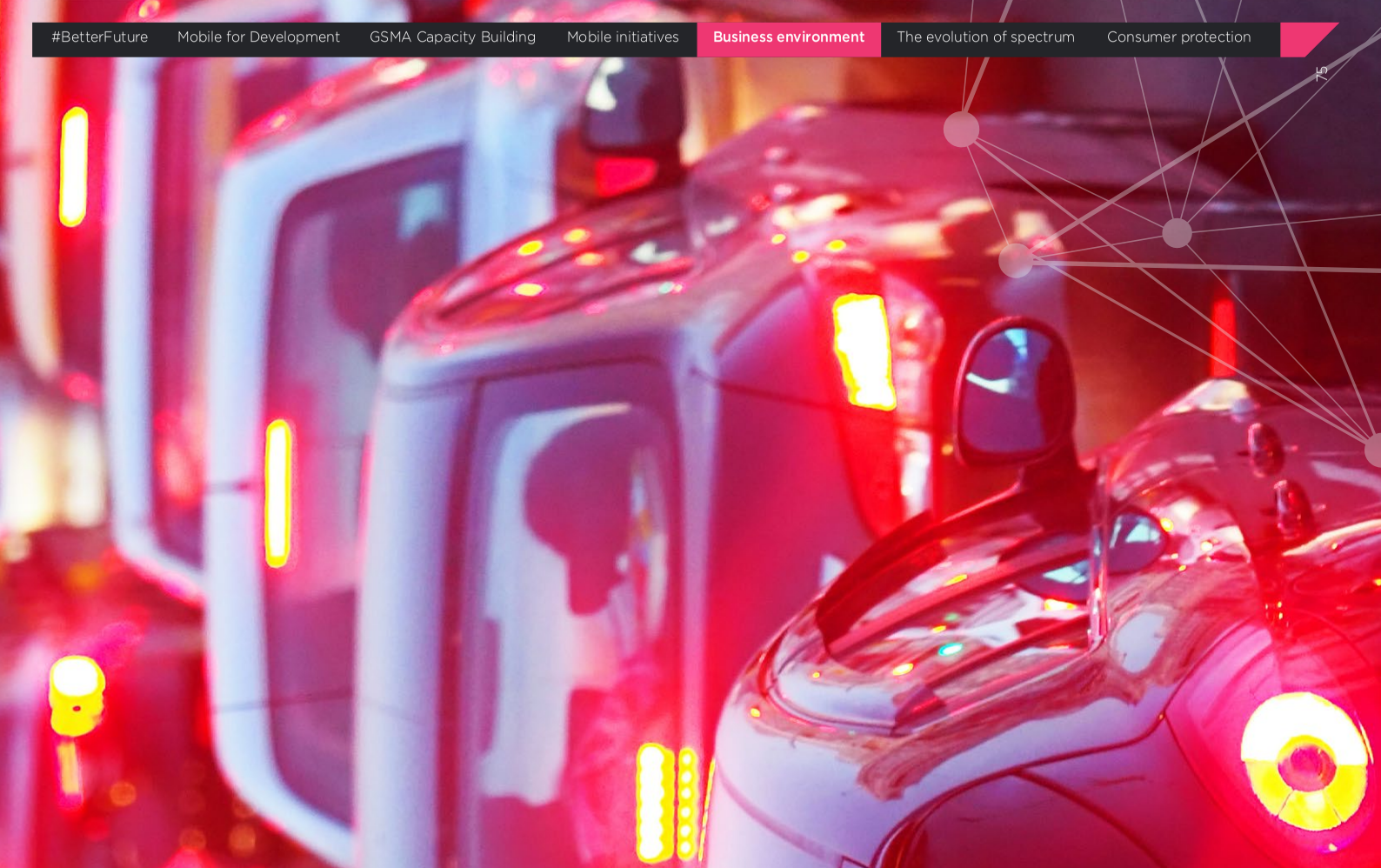
» **Network integrity:** Protecting the network and customers from external threats, such as malware and denial-of-service attacks.

» **Child protection:** Applying content filters that limit access to age-inappropriate content.

» **Subscription-triggered services:** Taking appropriate action when a customer exceeds their 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, and considering the time sensitivities of services, such as remote alarm monitoring.



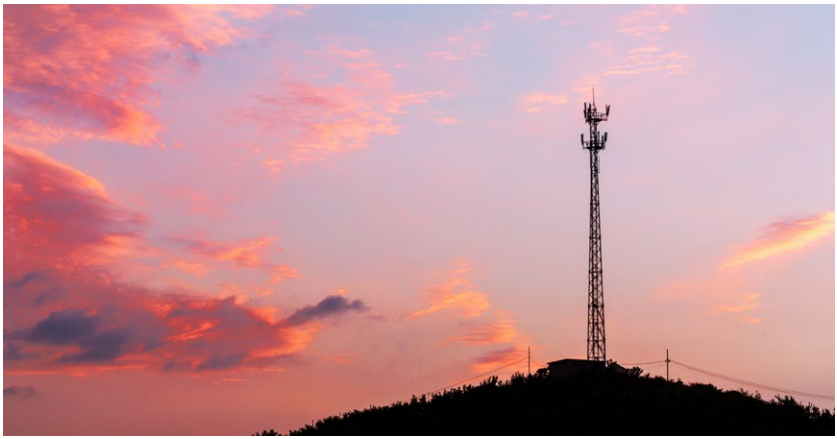
Passive infrastructure providers

Background

Many mobile operators share infrastructure on commercial terms to reduce costs, avoid unnecessary duplication and 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 signal transmission and reception.

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

Increasingly, independent tower companies provide tower-sharing facilities to mobile 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 support passive infrastructure-sharing arrangements, there is a lack of regulatory clarity in some countries, particularly in relation to independent tower companies.



Resources:

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

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 mobile 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 operators should be permitted to use infrastructure from passive infrastructure companies through commercial agreements without explicit regulatory approval. Infrastructure-sharing agreements should be governed by 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 development of this industry, which makes more efficient, lower-cost forms of infrastructure supply possible.

Debate:

- *What benefits do independent tower companies offer to mobile operators?*
- *Should passive infrastructure sharing ever be mandated by a regulatory authority?*
- *What steps should regulators take to provide clarity for tower companies and mobile operators?*

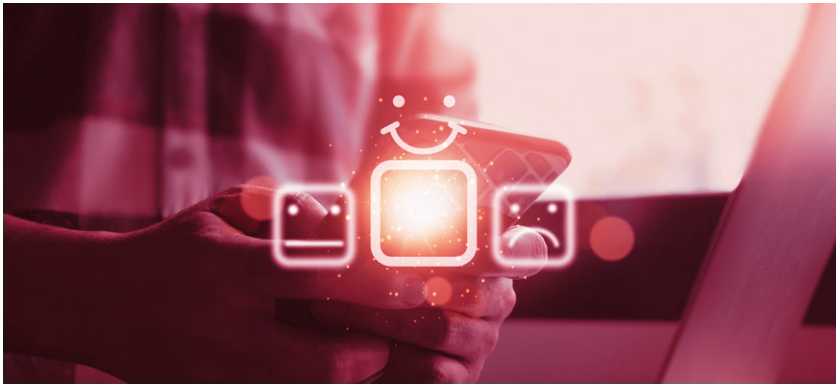
Quality of service

Background

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

Mobile operators must manage changing traffic patterns and congestion, as these normal fluctuations result in customers experiencing different qualities of service.

Connection throughput is viewed 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.



Resources:

GSMA Reference Document: Definition of Quality of Service Parameters and their Computation
GSMA Latin America Brochure: The Quality of Mobile Services in Latin America

Industry position

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

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

Mobile networks are technically different from fixed networks since 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 a 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 that rigidly defines a particular service quality level is unnecessary and likely to affect the development of these services.

Competitive markets with different commercial offerings and information that allows consumers to make informed choices 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.

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?*

Deeper dive: A network of interconnections

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

Factors beyond an operator's control include:

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

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

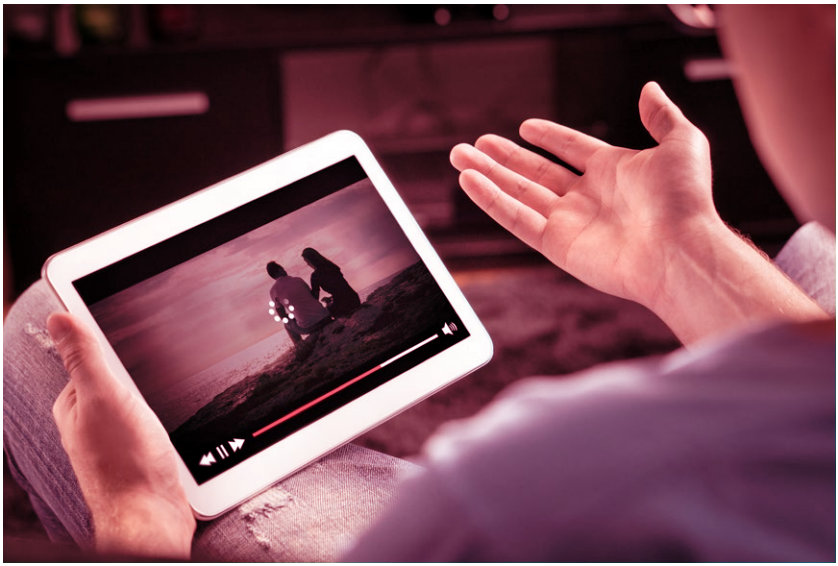
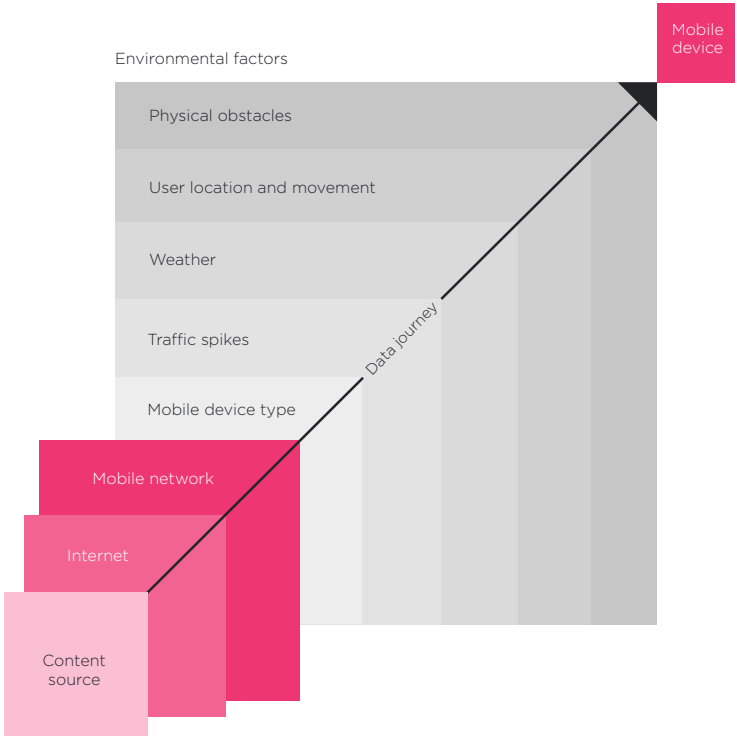


Figure 8 **Factors affecting quality of service**



For these reasons, regulation on 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 inefficient use of the capital invested in networks.

Single wholesale networks

Background

Policymakers in some countries are considering establishing single wholesale networks (SWNs) or wholesale open access networks (WOAN) instead of relying on competing mobile networks to deliver mobile broadband services. 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 generally be defined as government-initiated network monopolies that compel mobile operators and others to rely on wholesale services provided by the SWN to serve and compete for retail customers.

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

In 2000, there were almost as many countries served by a single mobile network as there were countries served by multiple competing networks. Today, however, only about 30 markets are served by a single mobile network.[6] Many are small islands with populations in the thousands and, in total, represent less than two per cent of the world's population. During the same period, network competition has produced unprecedented growth and innovation in mobile services, particularly in developing countries. The number of unique mobile subscribers has now surpassed five billion.[7] This success has fuelled innovation and helped increase speeds, improved network coverage and cut costs.

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

Resources:

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

6. GSMA and Frontier Economics. (2014). *Assessing the Case for Single Wholesale Networks in Mobile Communications.*
7. GSMAi

Industry position

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

Although some supporters claim they provide greater network coverage than network competition, this is often because there are public subsidies and other forms of favourable support for SWNs that are not available to competing mobile operators, making it an unfair comparison. Commercial networks can deliver coverage even in areas where duplicate networks are not economical. This can be achieved in many ways, including through voluntary network sharing among operators.

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

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

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?*

Deeper dive: The risks of SWNs

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

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

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

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

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

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

The Altán consortium has yet to prove their service is a valuable offering for Mexican consumers and businesses, as the network is only available in areas that already have coverage. Consequently, uptake among the large operators, which would help increase the impact of the project, has been slow. This makes the goal of reaching 92.2 per cent of the population by 2024 look very optimistic.

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

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

While it is often a fiercely competitive industry, mobile operators are not shying away from cooperation to expand coverage. The connectivity gap can only be overcome through close collaboration between the telecoms industry and governments. The basic building blocks are:

» Cost-effective access to low-frequency spectrum;

» Support for flexible spectrum use (e.g. refarming and technology-neutral licences);

» Support for all forms of voluntary infrastructure sharing;

» Better use of government Universal Service Funds (USF)/subsidiaries to incentivise extended coverage;

» Elimination of sector-specific taxation on operators, vendors and consumers;

» Non-discriminatory access to public infrastructure;

» Support for streamlined planning and administrative processes;

» Relaxation of quality-of-service requirements;

» Context-appropriate competition policy, especially concerning market structure; and

» Support for multisided business models, such as zero-rated and sponsored data.

Taxation

Background

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

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

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

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

Industry position

Governments should reduce or remove mobile-specific taxes because the social impact and the long-term positive impact on GDP (and hence tax revenues) will outweigh any short-term reduction in contributions to government budgets.

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

» Taxes should be broad-based. Different taxes have different economic properties and, in general, broad-based consumption taxes are less distortionary than taxes on income or profits.

» Taxes should account for sector and product externalities.

» The tax and regulatory system should be simple, easily understandable and enforceable.

Resources:

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

» Dynamic incentives for operators should not be affected – taxation should not disincentivise efficient investment or competition in the information and communication technology (ICT) sector.

» Taxes should be equitable and the burden of taxation should not fall disproportionately on lower income members of society.

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

Governments often levy special taxes to finance spending in sectors where private investment is lacking. However, this approach is inefficient. Fiscal policy that applies a special tax to the telecommunications sector causes distortions that discourage private spending and prevent the positive spill overs of mobile throughout the economy, ultimately diminishing social and economic 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 consumer adoption and use of mobile broadband. Lowering the taxation burden on the sector increases mobile uptake and use, creating a multiplier effect in the wider economy.

Taxing international calls has a negative impact on consumers, businesses and citizens abroad, damaging a country's competitiveness.

Debate:

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

Deeper dive: Taxes and fees on mobile consumers and operators

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

In addition to consumer-facing charges, mobile operators also face a range of other charges, including licensing fees, corporation tax, revenue charges and many more. Taxes and fees that specifically target the mobile sector affect the willingness of operators to invest in rolling out networks. 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 on to consumers as higher prices, or a combination of both.

Research conducted by Deloitte for the GSMA revealed that:

» Mobile operators paid $32 billion in 2015 in 27 nations surveyed. Sector-specific taxes accounted for around $8 billion of this total. Sector-specific excise duties were present in 81 per cent of surveyed nations, as were spectrum fees.

» A little less than a third (28 per cent) of operator revenues were spent on taxes, excluding non-recurring payments, such as spectrum auction fees.

» In eight countries, including Brazil, Chad and the Democratic Republic of Congo (DRC), taxes accounted for 40 per cent or more of sector revenue.

Of the countries surveyed, it was only in South Africa and Italy that the sector's tax contribution as a proportion of the total tax take closely matched its contribution to the entire economy. In four countries the sector paid more than double, in three others more than triple and in three others more than four times.

Taxes and fees on mobile services affect the affordability of mobile access and usage, and may have a disproportionate impact on lower income consumers since mobile services account for a larger share of the annual income of poorer households. In the DRC, the most extreme case, these fees represented 21 per cent of gross national income (GNI) of the bottom 20 per cent of income earners.

Eight steps governments can take to rebalance taxation and promote digital inclusion:

1. Phased reductions of sector-specific taxes and fees can be an effective way for governments to signal their support for boosting connectivity.

2. To enable more users to afford mobile services, governments should choose to lower so-called "luxury" taxes on devices and connections.

3. Uncertainty over future taxation reduces investment because the risk of tax hikes is priced into investment decisions. Governments should seek to limit unpredictable tax and fee changes and streamline how taxes and fees are levied.

4. The spectrum award approach needs to balance the relationship between ex-ante and ex-post fees in a transparent way, to ensure operators do not pay twice for access to the same resource.

5. Eliminating import duties for mobile network equipment and other local taxes levied directly on mobile sites has the potential to boost investment in networks.

6. Governments should avoid disproportionate taxation of services such as mobile money, as it puts a wide range of positive externalities at risk.

7. Removal of surtaxes on international incoming calls can ease barriers to regional and international trade by lowering the cost of international communication. It can also make it more affordable, enabling more consumers to reap the benefits of mobile services.

8. Governments should apply fees on profits rather than revenues to prevent discouraging investment and innovation. These fees require the same payment from an operator regardless of whether they retain their profit or use it to invest in new infrastructure and services.

Universal service funds

Background

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

Several countries have established universal service funds (USFs) to extend coverage in areas that are not commercially viable for the private sector. USFs are typically funded by levies on telecommunications sector revenues and the funds are disbursed either through direct subsidies or competitive bidding. USFs can also provide non-financial support to connectivity initiatives.

Despite these goals, USFs often perform poorly, and countries with USFs have typically not experienced stronger internet growth.[8] Studies by the GSMA and the ITU show that disbursement rates remain very low across the world and that many funds have been unable to distribute any of the levies collected.

When not administered effectively, USFs can be counterproductive. By effectively taxing communications customers, services become less affordable.

Industry position

USFs should only be considered once all policy and regulatory measures to maximise coverage through market-driven mechanisms have been exhausted and after careful assessment of alternative mechanisms, such as coverage obligations and reverse spectrum auctions.

Reducing costs and regulatory barriers is critical to expand the reach of mobile connectivity. Importantly, governments can help by removing sector-specific taxes, stimulating demand and developing infrastructure.

In markets where they already exist, USFs should be targeted, time-bound and managed transparently. Alternative funding mechanisms should be considered to ensure a broad base of stakeholders contribute to USFs, not just mobile operators. The allocation of funds, in consultation with the industry, should be competitive, technology-neutral and target projects with the greatest possible impact. USFs should adhere to the following best practices:

Resources:

A4AI Report: Universal Service And Access Funds: An Untapped Resource to Close the Gender Digital Divide
GSMA Report: Survey of Universal Service Funds, Key Findings
GSMA Connected Society: Are Universal Service Funds an Effective Way to Achieve Universal Access?
GSMA News: Press Release: GSMA, Vodafone and GIFEC Partner to Deliver Connectivity to Rural Communities
ITU Report: Universal Service Fund and Digital Inclusion for All
UN ESCAP Working Paper: The Impact of Universal Service Funds on Fixed-Broadband Deployment and Internet Adoption in Asia and the Pacific

8. UN ESCAP. (2017). *The Impact of Universal Service Funds on Fixed-Broadband Deployment and Internet Adoption in Asia and the Pacific.*

- Clear targets that ensure effective and timely disbursement of funds;
- Continuous evaluations, annual reporting and regular independent audits of government administration to ensure transparency in fund financing, disbursements and operations;
- Solid, clear and transparent underlying legal frameworks that support flexible services and technology neutrality;
- Based on an independent fund structure to avoid political interference;
- Administered effectively to avoid excessively bureaucratic structures or insufficient oversight;
- A thorough analysis of investment gaps and the impact of introducing levies on affordability and adoption to set appropriate USF levies;
- Consideration of a pay-or-play model by which mobile operators can choose to make a financial contribution to the USF or implement projects that meet the fund's goals;
- Consultation with mobile operators to ensure investments in coverage are targeted efficiently, include operational expenditure subsidies where necessary and avoid duplication of infrastructure; and
- If USFs cannot be managed efficiently within a reasonable time frame, a plan should be implemented to phase them out.

Debate:

- ***What policies and processes need to be in place to ensure USF financial resources are transparent and used efficiently?***
- ***What alternative strategies can governments take to enable the private sector to expand connectivity?***
- ***How relevant are USFs in mature markets?***

Public-private partnerships

Background

A public-private partnership (PPP) is a legal arrangement between two or more private and public sector parties to deliver a service via mutual investment. PPPs are common in infrastructure sectors such as telecoms where upfront investments are high and payback periods long.

PPPs can be an interesting mechanism to facilitate investment from different stakeholders and support the extension of network coverage in areas that are otherwise risky investments with limited commercial potential. Governments view PPPs as a way to drive investment in uncovered areas and leverage the expertise of the private sector. In turn, private companies benefit from the certainty of a viable business model thanks to the investment and guarantees provided by the public partner. Large-scale PPPs often attract the interest of multilateral organisations, which recognise the potential economy-wide benefits of such projects and are willing to support private companies and governments that lack the financial means to get these projects off the ground on their own.[9]

In the telecoms sector, PPPs are found across all network segments:

- First mile: submarine cables, satellite hubs, Internet Exchange Points (IXPs);
- Medium mile: fibre backbone and backhaul; and
- Last mile: radio access networks and wired local loops.

Resources:

European Commission Guide: The Broadband State Aid Rules Explained: An eGuide for Decision Makers: An eGuide for Decision Makers

9. An illustrative example is the ACE submarine cable along the coast of West Africa, one of the largest PPP investments in the ICT sector. The ACE submarine cable began operating in 2012 and now connects 23 countries to international fibre infrastructure, some for the first time. It is enabling faster speeds and lower prices for internet access. The World Bank financed part of the ACE submarine cable. Sources: World Bank. (2018). *Private Participation in Infrastructure Database*; World Bank (2018) *Implementation Completion and Results Report*.

10. "Todo Chile Communicado" is a typical example of the first case, where a PPP was created to bring mobile connectivity to 1,474 rural communities in Chile. Source: GSMA. (2016). *Closing the Coverage Gap*.

11. The ACE submarine cable is a good example of infrastructure that enabled faster and cheaper internet connectivity across 22 countries in Africa.

12. European Commission. (2013). *The Broadband State Aid Rules Explained*.

13. See GSMA. (2016). *Unlocking Rural Coverage: Enablers for Commercially Sustainable Mobile Expansion*.

Industry position

PPPs can be an effective way to deploy and operate network infrastructure in areas that do not have the economic potential to attract private investment. Public and private resources may support network deployment to deliver communications services directly to customers[10] or provide the infrastructure to deploy commercially viable networks.[11]

Governments should only consider PPPs in the most remote areas. Engaging with mobile operators and considering their roll-out plans is an essential part of the scoping phase,[12] as it prevents public investment from being wasted in areas where operators could have deployed networks on their own. Service delivery and customer engagement should be left to the private sector, which can provide the full suite of products and services to support digital inclusion.

Governments should only consider PPPs after exhausting all other policy and regulatory measures to maximise coverage through market-driven mechanisms. Creating an investment-friendly policy framework should be the first step in a coverage expansion strategy.[13] As a second step, governments should consider giving mobile operators the same preferential conditions PPPs often enjoy, such as subsidies, no-cost access to public infrastructure or less stringent quality-of-service obligations. This may be sufficient to create a favourable business case in remote areas.

When implementing a PPP, governments should avoid the single wholesale network approach. SWNs are PPPs that do not observe the best practices outlined above. SWNs have a geographic scope that overlaps with commercial networks and monopolises important resources, such as spectrum. They create an uneven playing field, use valuable public resources inefficiently and have multiple implementation challenges (see the 'Single wholesale networks' section for more details).

Debate:

- *Are PPPs an effective way to accelerate the deployment of infrastructure and drive digital inclusion?*
- *What alternatives do governments have to use their resources to catalyse investment?*
- *What are the characteristics of a PPP that maximises positive impacts while minimising negative consequences?*

The evolution of spectrum: to 2030 and beyond

Introduction

To close the connectivity gap, accommodate growth in data traffic, drive the Internet of Things and realise the full potential of 5G, mobile networks must evolve. To support this evolution, mobile operators need access to sufficient spectrum in low, mid and high bands.

Long-term planning and effective spectrum licensing play vital roles in providing operators with access to this necessary resource. To encourage investment in mobile services, it is important to have transparent, long-term national broadband plans that include a strategy for making sufficient spectrum available to the mobile industry. This creates certainty and allows the industry to invest, innovate and thrive.

How spectrum is priced also has a significant impact. Governments that seek to maximise state revenues from spectrum pricing risk deterring investors and undermining competition in communications markets. Research shows that high spectrum prices are linked to slower network speeds and lower coverage. The primary goal of pricing mechanisms should instead be broadband development.

Spectrum needs

Background

Mobile networks today operate across an evolving range of technologies, from 2G to 5G. Each of these technologies requires spectrum relative to the role they play in society. 2G voice applications use small tranches of spectrum compared to the much wider channels required for dense, high-throughput 5G usage. Governments can support mobile growth by having a long-term vision of the spectrum access mobile operators will receive.

In some regions, 2G and 3G networks are starting to be switched off. These technology sunsets allow spectrum to be refarmed for more efficient technologies such as 4G and 5G. However, the capacity burden on 5G networks, due to the higher number of devices that will need to be connected and the growth in average user data traffic, will be far higher than previous generations of mobile.

Meeting demand requires spectrum capacity in low, mid and high bands. Low-band spectrum has the best propagation, but also the smallest capacity, while high-band spectrum has huge capacity but the signals do not reach as far. Mid-band spectrum balances coverage and capacity for city-wide coverage.

Although countries in different regions have adopted different combinations of those bands, regional and global harmonisation have created economies of scale that, in turn, have made mobile services and handsets more affordable.

Low bands: sub-1 GHz

Low bands support wide-area coverage and improved indoor connectivity across urban, suburban and rural areas. Increased low-band capacity is required to create greater equality between urban and rural broadband connectivity and address the digital divide.

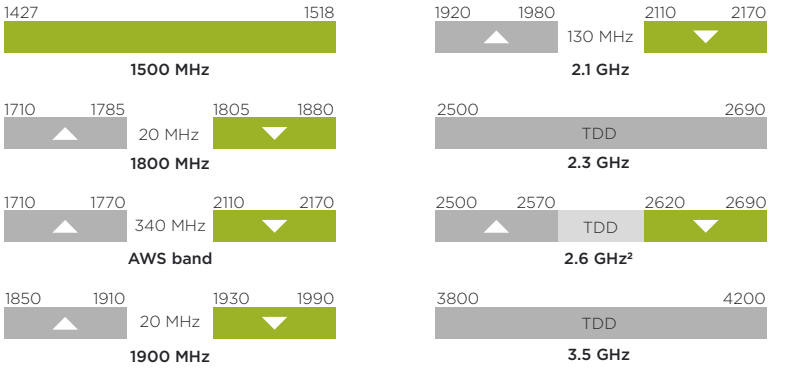
Figure 9 Low-band overview

**North America uses a more complex 700 MHz plan*

Mid-bands: 1–7 GHz

Mid bands offer a balance of coverage and capacity. Most commercial 5G launches so far have relied on spectrum within the 3.3–3.8 GHz range. Other bands, which may be assigned to or refarmed by operators for 5G include 1500 MHz, 1800 MHz, 2.1 GHz, 2.3 GHz and 2.6 GHz. More spectrum will be needed to maintain 5G-quality of service and meet growing long-term demand (e.g. 3.3–4.2 GHz, 4.8 GHz and 6 GHz).

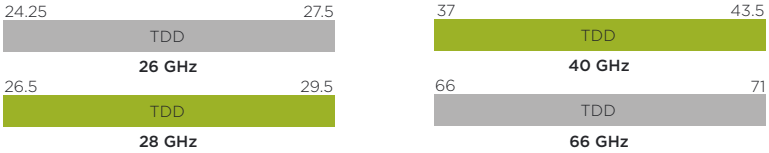
Figure 10 Mid-band overview



High bands (including mmWave)

High-band spectrum, such as mmWave, supports the ultra-high broadband speeds envisioned for 5G. These bands produce the highest throughput and lowest latency and include bands such as 26 GHz, 28 GHz and 40 GHz.

Figure 11 High-band overview



Planning spectrum: 2025–2030

Background

5G will support significantly faster mobile broadband speeds and heavier data usage than previous generations of mobile technology while also enabling the full potential of the Internet of Things. From connected cars and smart cities to the industrial internet and fibre-like FWA, 5G will allow more devices to access more data than ever before. The efficiency of 5G will be essential to preserving today's most popular mobile applications, such as on-demand video, in an environment of high-user demand. It will help ensure that growing capacity demands can be sustained, but requires access to low-, mid- and high-band spectrums.

The following usage scenarios are the four main pillars of 5G:

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

The success of 5G services will depend on national governments and regulators. The speed, reach and quality of services will require governments and regulators to support timely access to the right amount and type of spectrum under the right conditions.

Mobile operators need clarity on the access they will have to spectrum before launching new technologies, such as 5G, or upgrading network capacity to support long-term investment. Where spectrum shortages exist, mobile operators will need to create denser networks with more base stations, which will increase broadband costs for consumers as well as energy consumption.

The roadmap for spectrum access should be made transparent by governments and regulators to optimise network planning and reduce capital expenditure. By working together with industry, governments can help ensure connectivity is affordable.

Resources:

GSMA Report: Vision 2030: Insight for MId-Band Spectrum Needs
GSMA Public Policy Position: 5G Spectrum

Industry position

5G needs a significant amount of new harmonised mobile spectrum. Governments should carefully consider 5G spectrum demands when 5G usage reaches its peak, and advanced use cases will require additional spectrum.

The mobile industry believes that:

- Regulators should plan to make, on average, 2 GHz of harmonised mid-band spectrum available between 2025 and 2030 to support 5G. This includes making 80–100 MHz of contiguous mid-band spectrum per operator available at launch. Channels of around 1 GHz per operator in millimetre wave bands (i.e. above 24 GHz) will be required.
- Governments and regulators should support new harmonised bands globally to help 5G services grow over time (e.g. UHF, 3.3–4.2 GHz, 4.8 GHz and 6 GHz). This includes engaging in the World Radiocommunication Conference (WRC) process to ensure sufficient mid- and low-band spectrums are available.
- Exclusively licensed spectrum over wide geographic areas is vital to the success of 5G, although spectrum sharing and unlicensed spectrum can play a complementary role. The speed and quality of 5G relies on guaranteed spectrum access.
- Setting spectrum aside for local or vertical usage in harmonised 5G bands could jeopardise the success of public 5G services and may waste spectrum. Sharing approaches like leasing are typically better options.
- Governments and regulators should avoid inflating 5G spectrum prices as this is linked to slower broadband speeds and worse coverage. Excessive reserve prices, annual fees, limited spectrum supply (e.g. through set asides) and poor auction design should be avoided.
- Regulators should carefully consider 5G backhaul needs, including making additional bands available and supporting wider bandwidths in existing bands. Measures should also be taken to ensure licences are affordable and designed effectively.
- Regulators should carefully consider the right 5G spectrum licence terms, conditions and awards approach and consult with industry to maximise the benefits of 5G.
- Governments need to adopt national spectrum policy measures to encourage long-term heavy investment in 5G networks (e.g. long-term licences, clear and transparent renewal processes and spectrum road maps).

Debate:

- *The GSMA recognises an average total of 2 GHz of mid-band spectrum needs to be made available to licensed mobile. Regulators need to decide how to meet this demand for 5G capacity and which harmonised bands can be used.*

Spectrum harmonisation

Background

Spectrum harmonisation is the uniform allocation of radio frequency bands under common technical and regulatory regimes, across entire regions. Adherence to internationally identified spectrum bands has many advantages:

- Lower costs for consumers, as device manufacturers can mass produce devices that function in multiple countries and realise economies of scale;
- A wider range of devices supported by a larger international market;
- Roaming or the ability to use a mobile device abroad; and
- Fewer cross-border interference issues.

Harmonised bands for mobile are listed in the earlier part of this section. Work towards their harmonisation has taken different forms.

Historically, the first point towards harmonisation was agreement through the ITU at a World Radiocommunication Conference (WRC) treaty meeting. Past WRCs were responsible for all the early mobile bands, including 900 MHz, 1800 MHz and 2.6 GHz. Mobile allocation for a particular frequency band, and additional IMT identification, have always been sought at past WRCs to harmonise mobile use.

The WRC process is still a useful way to support harmonisation. At the WRC in 2015, for example, agreement was reached on the creation of three global spectrum bands for mobile: 700 MHz, 1427–1518 MHz and 3.4–3.6 GHz. In 2019, mmWave bands were discussed and the harmonised use of 26 GHz, 40 GHz and 66 GHz was agreed.

However, countries develop their communications systems at different rates, and negotiations at the ITU have struggled to keep pace with the needs of the fastest-moving markets. Over the past 10 years, countries have been developing bands for mobile use on their own, either regionally or unilaterally, to meet demand.

This has been clearest with activity around the 3.5 GHz range. Only 200 MHz of spectrum in the 3.3–4.2 GHz range was agreed by the WRC-15 but, even before the 2015 conference, demand in some parts of the world had already risen well above that figure. Today, as much as 700 MHz is available in this spectrum band in some countries, leaving WRCs to tidy up harmonisation rather than initiate it.

Spectrum harmonisation through the WRC process remains an important goal and helps enable lower cost mobile devices through economies of scale. However, many governments and regions, such as the EU or ASMG, are charting their own path, making inter-regional harmonisation and industry guidance on spectrum use vital to the spectrum development process.

Resources:

The GSMA at WRC-23 Website

Industry position

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

The mobile industry has had concerns about the pace of the WRC process for the past 15 years. Rapid growth in consumer demand for mobile has prompted countries and regions to look beyond WRCs to provide access to new mobile bands.

Where this has been necessary, multiregional harmonisation has been broadly achieved by loose consensus based on equipment availability. However, this approach risks leaving slower-moving nations without input into which bands are best used, as equipment will only be developed in bands used by early-adopter nations. For WRCs to once again be the starting point for spectrum development, they need to look at least 10 years ahead. Recent conferences have not managed to do so.

At a minimum, harmonisation of mobile bands at the regional level is crucial. Even small variations in standard band plans can result in many devices not being usable, with costly consequences for consumers.

All markets should harmonise regionally where possible, as this benefits the entire global mobile ecosystem. Sometimes technology advances, such as carrier aggregation or dynamic spectrum access, are believed to supersede the need for harmonisation. However, these are technical processes, requiring more complex handsets that need more power. While they are a help, they do not replace harmonisation as the best means of assuring affordable communications services.

Debate:

» *What planning tools, forecasts of spectrum needs and technology analysis are required to support long-term development?*

Deeper dive: World Radiocommunication Conference 2023 (WRC-23)

Spectrum harmonisation has created economies of scale for mobile networks that, in turn, have made mobile services and handsets more affordable. Widely harmonised mobile spectrum is again needed at the next WRC in 2023 to achieve these goals.

The 2023 conference will differ from earlier WRCs in that many of the bands it is likely to harmonise – 600 MHz, 3.6–3.8 GHz and 4.8 GHz – have already been developed for mobile and are in use today. Meanwhile, development of the 6 GHz range is well under development.

WRC-23 must therefore ensure that the harmonisation of these bands is spread as broadly as possible to achieve the greatest economies of scale. This will ensure 5G, and subsequent generations of mobile networks, meet expectations and deliver the full range of affordable services.

The work of any WRC is split into different portions of the agenda, with different subjects allotted their own agenda item or workstream. Mobile spectrum discussions cut across several agenda items.

Figure 12 **WRC-23 frequencies being considered**

Band	Agenda item
470–694 MHz	1.5
3.3–3.4 GHz	1.2
3.6–3.8 GHz	1.2, 1.3
4.8–4.99 GHz	1.1
6.425–7.125 GHz	1.2
10–10.5 GHz	1.2

470–694 MHz

As low-band signals propagate, they become more effective at covering wide areas. The mobile industry requires additional spectrum below 1 GHz to improve the performance of 5G networks in areas where higher frequencies, which have high capacity but do not propagate as far, are not affordable to use. These areas include wide rural and some suburban areas where dense networks would be too costly to provide efficient broadband. Low frequencies also provide better penetration in buildings.

For countries with large rural populations, the bands below 1 GHz will improve digital inclusion and help meet targets for equal digital opportunities, including health care and education. Additional spectrum for mobile in the UHF band can thus support several common policy goals, such as greater digital inclusion, a smaller urban/rural digital divide, better access to e-government and smart health care/education and lower consumer broadband prices.

3.3–3.8 GHz

The 3.5 GHz range is the 5G launch band in most countries and, as such, has the deepest ecosystem and most affordable devices. 3.3–3.4 GHz and 3600–3800 MHz are both being discussed at WRC-23 under Agenda Item 1.2 and 1.3. These two bands are being considered on either side of the 3.4–3.6 GHz band harmonised at WRC-15. Development of both sub-bands will help support the mid-band capacity requirements of 5G.

4.8–4.99 GHz

The GSMA believes that the 4.8–4.99 GHz band provides a good option for supplementary mobile spectrum. Following the implementation of 5G in the 3300–3800 MHz range, this band could expand the capacity of future networks and has already been considered through new assignments in China and Russia, nearby assignments in Japan, new announcements in the United States and the on-going activity of WRC-23.

6.425–7.125 GHz

The 6 GHz range is a high priority for the GSMA and our members in all three regions supporting 5G in this band. In a recent member survey, this band was supported by 90 per cent of GSMA operator members globally. The mobile industry believes that assigning an average of 2 GHz of mid-band spectrum for 5G will be very difficult in most cases without the use of this band.

10–10.5 GHz

The mobile industry believes that 10–10.5 GHz and 10–10.5 MHz would provide valuable additional capacity between mid-band and mmWave. This spectrum is being studied in the Americas as a potential supplement to mid-band capacity.

Coexistence of technologies

Background

Each of the WRC agenda items looks at the frequency bands developed, or under development, for 5G but also used by other services. Part of the work of WRCs is to consider the technical characteristics and sharing conditions to ensure compatibility and that different services can coexist. This may include national guidelines on coexistence or rules for cross-border coordination of services.

Governments need to ensure compatibility between a wide range of services. Particularly in LMICs, consumers use radio equipment such as satellite dishes for long periods, which means some less efficient terminals may be in circulation. To mitigate this, adherence to modern standards for new equipment is vital even if older equipment is still in use.

Industry position

The mobile industry benefits from WRC decisions that develop the use of harmonised bands for mobile and help to mitigate interference between services using radio spectrum.

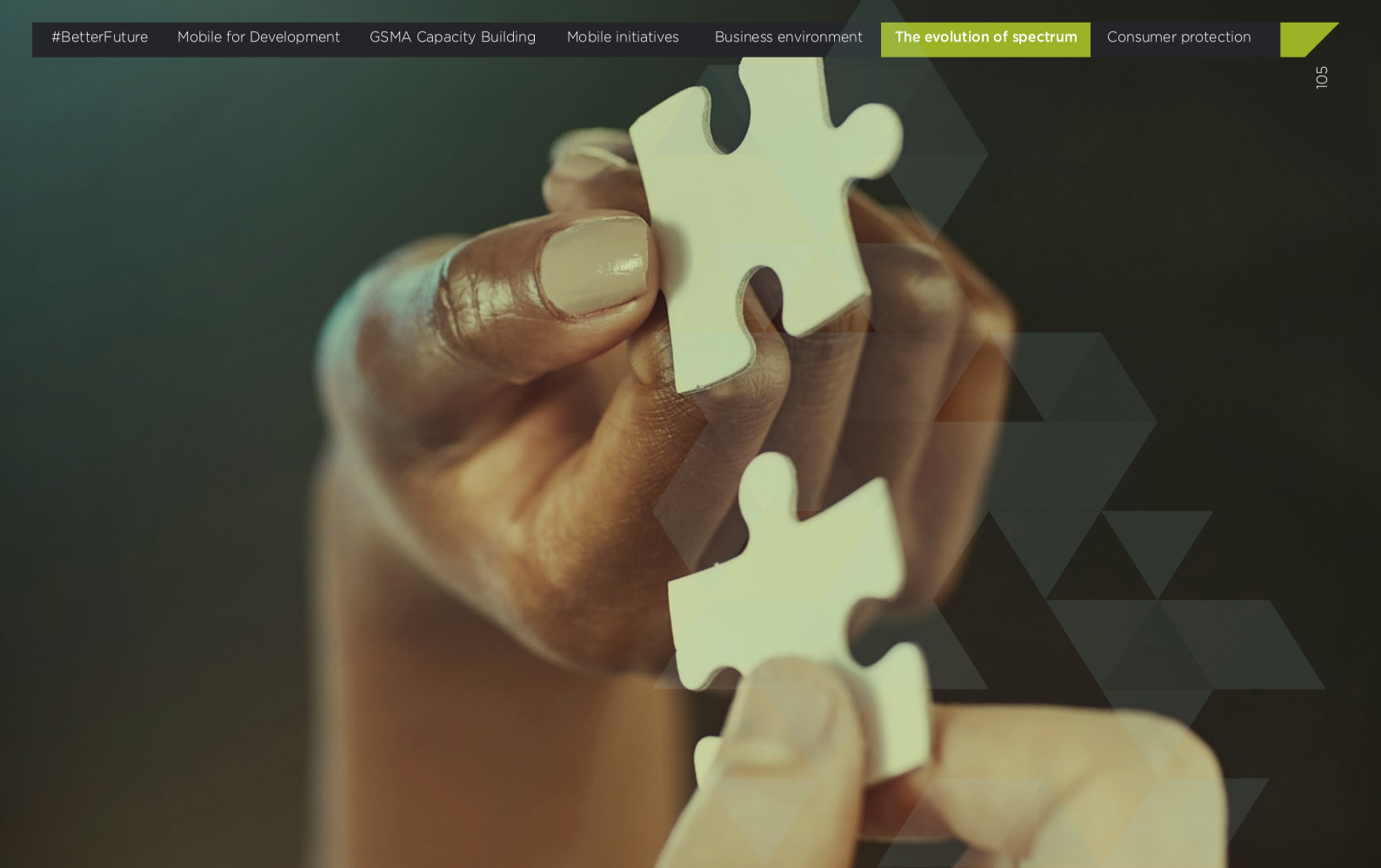
Harmonised use of frequencies is one of the benefits of agreements at the ITU. Defining radio transmitter and receiver parameters helps to ensure compatibility between radio systems operating in the same or adjacent frequency bands. Detailed technical coordination at the ITU and in standardisation bodies, such as 3GPP, helps advance spectral efficiency and minimise guard bands.

Each new generation of mobile technology is more efficient than the last and can use spectrum to provide greater connectivity, but additional spectrum needs still exist, driven by higher demand for connectivity beyond efficiency gains. 5G also uses active antenna systems (AAS), which provide a leap in efficiency with their precise targeting of connections where the user is located. This enhances compatibility with other services.

To maximise efficiency and support optimal coexistence, it is important to look at the receiver performances of legacy services. Older systems, including some satellite receivers, have historically been linked with claims that their susceptibility to interference require huge guard bands to ensure compatibility between services. In a modern communications environment, such guard bands are a barrier to economic development and should be avoided. More efficient satellite receivers should be used by service providers in this case, and filters used where necessary to ensure consumers get the best possible access to connectivity.

Debate:

» *How can governments 'future-proof' systems to ensure all new equipment meets modern compatibility standards?*



Spectrum licensing

Background

Spectrum licensing is central to the delivery of high-quality mobile broadband services and long-term investment in networks. The amount of spectrum made available and the terms on which it is licensed drive the cost and quality of mobile services.

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

Spectrum management for mobile telecommunications must include the release of new spectrum in harmonised mobile bands, renewal of licences coming to the end of their initial term and the assignment of new bands for mobile broadband services.

Industry position

Effective spectrum licensing is critical to the future expansion of mobile services. Licensing frameworks should encourage the investments needed to expand mobile access, meet increased demand and enhance the range of services offered.

At its core, a licensing framework should:

» Ensure operators have access to sufficient spectrum;

» Provide predictability to support the new network investment needed; and

» Avoid costly restrictions on the use of spectrum beyond those needed to manage interference.

Success depends on tailored approaches that consider specific market circumstances. The best approach should consider policy objectives as well as market conditions. The latter should include current spectrum use, the competitiveness of the market and the risks to investment and service quality.

Long-term planning is vital to encourage investment in mobile services. Success depends on having a transparent, long-term road map that includes a strategy for making sufficient spectrum available to the mobile industry.

Licence conditions, other than those relating to coexistence, should be kept to a minimum or removed entirely. Other objectives, including coverage requirements, can be addressed effectively through direct policy.

A licence duration of at least 20 years will incentivise network investment. A 20-year or longer licence period offers the certainty mobile operators need to expand and upgrade networks. The use of indefinite licence terms can make operators even more willing to invest.

Resources:

GSMA Report: Best Practice in Mobile Spectrum Licensing

As mentioned previously, spectrum pricing has a significant impact on investment and the quality of mobile services. Governments that seek to maximise state revenues from spectrum pricing, for example, risk deterring investors from upgrading their networks. Research also shows strong links between high spectrum prices, slower network speeds and lower coverage.

Debate:

» ***Spectrum licensing is the heart of mobile services. What measures can policy-makers implement to guarantee long-term investment and certainty?***

Spectrum licence renewal

Background

Managing spectrum renewals effectively is a vital part of any country's spectrum management strategy. The prospect of licences expiring creates significant uncertainty for mobile operators. A transparent, predictable and coherent approach to renewal is therefore important as it enables operators to make rational, long-term investment decisions.

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

Industry position

The right approach to licence renewals is an important part of a successful spectrum management strategy. Uncertainty over future rights to spectrum use may lead operators to cease investment in their networks and compete less to grow their customer base until issues are resolved.

The presumption of licence renewal and clear and timely renewal decisions are crucial to mobile network development, as they provide mobile operators the certainty they need to make large, long-term investments in their network and mobile services. A decision not to automatically renew a licence should only be made in circumstances where the benefits of reassigning spectrum would outweigh the costs.

Resources:

GSMA Report: Spectrum Leasing in the 5G Era

Recommendations on licensing and renewal approaches:

» Where spectrum is to be assigned for the first time, there is no single best licensing approach and authorities should make their decision based on the specific market context.

» When selecting an assignment approach, licensing authorities should prioritise efficient spectrum use and network investment while also ensuring effective competition.

» Whether an auction or administrative assignment is adopted, the details of the implementation should be transparent and provide certainty for the future.

» The decision to not automatically renew a spectrum licence should only be made when there are clear potential benefits from reassigning spectrum. This includes more efficient spectrum use or longer competition time that are likely to outweigh the costs (e.g. disruption to services and customers, the risk of deterring investment and customer service degradation and any required network reconfigurations).

» Licensing authorities should work in close partnership with stakeholders to enable a timely, fair and successful licensing process.

Debate:

» ***There is growing competition for access to spectrum. How can regulators balance the need for clarity on renewals with the spectrum needs of new stakeholders?***

Spectrum sharing, leasing and trading

Background

Ever-increasing data traffic means mobile services must have access to ever-increasing spectrum to meet demand. This creates the need for better spectrum management, to improve the efficiency of spectrum use and ensure its viable use in less economically viable areas. Also, completely clearing new frequency bands for future mobile use has become increasingly difficult.

At the same time, there is a growing thirst for spectrum from new parties, such as industry verticals. Where regulations permit their use, and if implemented correctly, tools such as spectrum sharing, trading and leasing can help make spectrum use more efficient.

Industry position

Spectrum sharing reduces the spectrum shortages faced by some mobile operators while also ensuring valuable spectrum does not lie fallow. It enables more intensive spectrum use and higher volumes of services, improves service quality and lowers the costs of service provision. All this supports greater capacity and more affordable services.

Spectrum leasing and trading enable the parties with the best information on the value of spectrum to determine its price. To justify the sale, a buyer or lessee needs to create more value from the acquired spectrum than the seller.

Voluntary leasing and trading also reduce risks for operators since they can sell or lease unused spectrum while having the opportunity to acquire new capacity as they grow. The ability to trade and lease licences can ensure that spectrum is used efficiently without additional charges needing to be imposed by government.

Trading is more likely when there is substantial available spectrum, when future spectrum and the regulatory framework are predictable and when there is a need to support network deployment by the lessee, such as for verticals.

Resources:

GSMA Public Policy Position: Spectrum Sharing
GSMA Report: Spectrum Leasing in the 5G Era

Recommendations on spectrum sharing, leasing and trading:

» Licensing authorities should allow voluntary spectrum sharing, leasing and trading among operators and facilitate these mechanisms through clearly defined spectrum rights, long licence terms and limited administrative costs.

» Authorities should only be notified of the agreements taking place so that it is clear who holds spectrum usage rights. Notification enables authorities to assess whether a proposed trade would create any risks to competition.

» Before a formal spectrum secondary market framework is established, authorities should be prepared to assess proposals for sharing, leasing and trading subject to consultation and consider risks to competition or of interference.

» Transparent and well-timed licence renewal processes, and information on spectrum availability, pricing and conditions, will facilitate sharing, leasing and trading.

» Competition issues should be assessed based on the specific circumstances of each sharing, leasing and trading agreement.

» Long licence terms allow the buyer or lessee of the rights to invest in using the spectrum.

Debate:

» ***Spectrum sharing can make spectrum use more efficient and create more value for consumers, but complex frameworks may hamper uptake. How can governments create a simple sharing framework that still ensures the robust and transparent definition of rights?***

Technology neutrality

Background

Where technology neutrality is written into the terms of licences, operators can upgrade their technology (e.g. from 2G to 4G) in a particular frequency band to meet market demand.

Restricting technology and service use exacerbates spectrum scarcity and prevents customers from gaining access to new and better services. Removing technology-specific restrictions (beyond those needed to manage coexistence) enables a market to maximise the benefits of its spectrum resources on an on-going basis. The ability of operators to introduce new, more spectrally efficient mobile technologies is critical to meeting growth in demand.

Allowing technology-neutral spectrum licences is now regarded as best practice all over the world. Countries that were among the first to implement them have been rewarded with better coverage and higher mobile broadband speeds. For example, Finland was the first to allow the 900 MHz band to be technology-neutral, which meant mobile users benefitted from far greater geographical 3G coverage than other European countries. In Asia, technology-neutrality in Singapore has created one of the world's most advanced mobile markets.

Resources:

GSMA Blog: The Benefits of Technology Neutral Spectrum Licences

Industry position

Governments should allow operators to deploy any mobile technology that can technically coexist within the international band plan.

Technology neutrality encourages innovation and promotes competition. This allows markets to determine which technologies succeed and ultimately benefits consumers and society.

Experience from technology-neutral spectrum licensing has raised certain issues. In general, attempts to extract additional revenue when including technology-neutrality in licences have backfired and held back the introduction of new mobile technologies.

While renewal processes provide an opportunity to reissue spectrum licences as neutral, regulators should not delay the introduction while waiting for the expiry dates of existing licences. However, when assigning new spectrum, regulators should do so in a technology-neutral manner and not restrict the introduction of next-generation technologies, such as 5G.

Debate:

» *New spectrum bands are needed to make the most of 5G, but reusing existing bands will also be possible. What are the best ways for regulators to apply technology neutrality and allow mobile operators to make the best use of existing bands for 5G?*

Spectrum assignment

Background

Governments need to manage the renewal of licences approaching the end of their initial term and release spectrum in both new and existing bands for mobile broadband services. At the same time, they should encourage important processes such as refarming.

Effective management of these processes is vital to encourage continued investment and development in the mobile sector.

Auctions are widely considered the most effective means of ensuring spectrum is held by those who can make the best use of it. Administrative assignments (e.g. "beauty contests") are also sometimes used when licensing the rights to use a particular spectrum band. Sometimes, a hybrid approach may also be used, where a shortlist of bidders is selected before an auction based on administrative criteria.

Auctions work best when there is excess demand for the spectrum and they help to select the operators most likely to put it to the best use and benefit society. Administrative assignments, on the other hand, may be suitable where there is less demand and may allow authorities to compare the range of policy objectives offered by the candidates.

Whichever approach is chosen, it must be implemented with care. This includes identifying issues through public consultation and weighing the trade-offs in specific design choices (noting the importance of efficient spectrum use and safeguarding competition). Sufficient time and transparency must be provided to allow potential candidates to make informed decisions.

Administrative assignments

Administrative assignments must be well planned to succeed. The selection criteria and process must be clear and the weight given to each objective should reflect its importance to society. The use of subjective criteria, or a lack of transparency, increase the risk of favouritism and corruption, as well as the potential for the outcome to be challenged in the courts. It may be necessary to make a trade-off between policy objectives and the licence fee. Even where the objective is clear, estimating the appropriate price can be challenging.

A particular problem of administrative assignment is the risk that successful applicants will not fulfil their offers, particularly if market or technology forecasts prove inaccurate. Licensing authorities should set out in advance what penalties will be imposed if commitments are not met.

DF 82/05
072
032
DX 01/87

Spectrum assignment

Auctions

Auctions are an efficient way to allocate spectrum when there is competition for scarce spectrum and demand is expected to exceed supply. However, to succeed, they need to be carefully planned. Excessively high reserve prices may result in spectrum going unsold.

There are several different auction designs to choose between, each with its strengths and limitations. While multiround auctions are often preferred, the best choice depends on market conditions and the objectives of the government and regulators. The most common are simple clock auctions, simultaneous multiple-round ascending auctions (SMRAs), sealed bids, combinatory clock auctions (CCAs) or hybrid approaches.

» When assigning spectrum via an auction, government objectives include:

» Maximum long-term value to the economy and society;

» Efficient technical implementation of services;

» Sufficient investment to roll out networks and new services;

» Revenue generation for the government;

» Adequate market competition; and

» A fair and transparent allocation process.

Auctions can lead to more efficient spectrum use, but auction design and rules are important. Certain design choices raise the risk of spectrum not being sold or limiting network investments. For regulators, the main challenge is balancing the objectives of efficient spectrum assignment and supporting competition in communications markets. Again, seeking to maximise auction revenues can have significant costs for society, especially the digital economy, if competition in communications markets is undermined and network investment is limited.

Low participation should also be a concern, especially in mature mobile markets. A wide variety of tools are available for regulators to address these issues, including the choice of auction format, determination of spectrum lots, spectrum caps and set-asides, bid information disclosure and reserve prices. However, these tools are often conflicting, and their effectiveness will depend on local market conditions.

Resources:

GSMA Report: Best Practice in Mobile Spectrum Licensing
GSMA Public Policy Position: Auction Best Practice

Industry position

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

Spectrum auctions must be designed to reflect market conditions and achieve the government's stated objectives. The choice of auction format (e.g. simultaneous auctions where multiple bands are auctioned together or sequential auctions where bands are auctioned one after the other), like other decisions in the spectrum assignment process, depends on specific market conditions. Having a clear spectrum road map with well-defined rights and conditions understood in advance is key.

Regulators should work with stakeholders to ensure the auction design is fair, transparent and appropriate for the market. Auctions should also be designed to maximise the long-term economic and social benefits of spectrum. The following key principles can help guide licensing authorities:

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

Debate:

- ***Auction design is a delicate balancing act, but there is little doubt that policy decisions have an impact on the quality of mobile services. How should governments decide which spectrum assignment method to use?***

Spectrum pricing

Background

High spectrum prices are associated with more expensive, lower quality mobile broadband services. They can lead to irrecoverable losses in consumer welfare worth billions of dollars worldwide. Research shows that when prices are too high, mobile operators are likely to invest less in their networks which, in turn, affects the quality and reach of their services.

High spectrum prices are particularly harmful in LMICs where the cost of mobile ownership accounts for a higher percentage of income than in high-income countries. In some cases, affordability has become a major roadblock to widespread mobile penetration.

The cause of extreme prices are typically policy factors that prioritise maximising short-term state revenues over long-term support for the digital economy. Examples include:

» Setting excessive reserve prices;

» Making insufficient spectrum available for auction; and

» A lack of clarity on future spectrum releases or the process for renewing expiring licences.

Such factors can create uncertainty and encourage bidding far above operators' true valuations of the licences on offer.

Resources:

GSMA Website: Effective spectrum pricing helps boost mobile services

Industry position

Spectrum is a valuable asset, but a long-term vision is needed to maximise its value. The primary goal in all awards should be to encourage the most efficient use of spectrum through investment in widespread, high-quality networks. Many countries around the world have successfully struck the right balance between increasing revenues and delivering efficient spectrum awards.

To do this, the GSMA recommends that governments and regulators:

- Set modest reserve prices and annual fees and rely on the market to set prices;
- License spectrum as soon as it is needed to avoid artificial scarcity;
- Avoid measures that increase risks for mobile operators and force them to overbid for spectrum; and
- Publish long-term spectrum award plans that prioritise societal benefits over state revenues.

Debate:

- *More and more telecom regulators are recognising the negative impact of high spectrum prices, but getting governments onboard is not always easy. How can regulators and mobile operators work together to highlight the benefits of affordable spectrum to all necessary levels of government?*

Spectrum for industries

Background

The development of new mobile technologies alongside the cloud, big data and machine learning is transforming how vertical industries can use connectivity. Verticals are companies, industries and public sector organisations operating in a specific sector. While they have traditionally deployed private networks to support their connectivity needs, this is changing as their requirements have evolved to include more advanced capabilities.

The new technologies range from creating smart utility grids and automating manufacturing, to delivering goods by drones and supporting advanced public safety and transport networks. Policymakers play a vital role by managing the spectrum that underpins these developments. However, great care needs to be taken to ensure verticals are fully supported without harming other wireless users, especially the consumers and businesses that rely on 4G and 5G.

Vertical industry needs are often met through partnerships with telecoms providers, including public mobile operators, using licensed spectrum. This allows them to benefit from the telecoms providers' extensive networks, substantial spectrum assets, expertise and, typically, lower cost base. However, some verticals may continue to operate private networks and thus may want access to additional spectrum to support advanced broadband capabilities.

This is a challenge for policymakers as widespread demand for additional spectrum outweighs supply. It is also difficult given that some verticals may want direct access to spectrum in priority 4G and 5G mobile bands (e.g. 700 MHz and 3.5 GHz) so they can benefit from the mobile equipment ecosystem and lower their deployment costs.

Spectrum for drones

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

These benefits can only be realised if regulators remove barriers to using mobile networks to support UAVs, most notably those associated with the use of licensed mobile spectrum. Licensed mobile spectrum enables widespread, high-quality connectivity for UAVs with sufficient capacity to support competitive services and rising usage levels.

Mobile services in licensed bands are well established and can be used to support UAV connectivity where permitted by regulators. Mobile operators typically have exclusive access to coverage spectrum to reliably cover very wide areas and capacity spectrum that supports faster data speeds. Taken together, this means operators can support safe, reliable, wide-area broadband connectivity for UAVs.

Regulators should also adopt a service- and technology-neutral framework to fully support UAVs. This will facilitate the development and growth of UAV connectivity. Spectrum licences that are technology specific may limit the ability to provide high-speed data connectivity for UAVs (e.g. 3G or 4G) or new IoT-specific cellular technologies that could provide simple narrow-band authentication and identification (e.g. NB-IoT or LTE-M).

Spectrum for IoT

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

According to data from GSMA Intelligence, the total number of IoT connections is predicted to grow from just over nine billion (9.1 billion) in 2018 to 25.2 billion by 2025, with the total IoT revenue opportunity worth $1.1 trillion by 2025.

The requirements of wide-area IoT services vary much more than those for traditional mobile services. This has meant that mobile technology standards are being continuously updated to support these use cases, which is driving innovation and ensuring that mobile IoT is well placed to compete effectively with other IoT solutions.

Licensed spectrum is vital to deliver the most reliable IoT services and has a unique ability to support quality of service guarantees over wide areas. Networks using licensed spectrum are not at risk of interference and operators can control usage levels on their networks.

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

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

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

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

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

Resources:

GSMA Public Policy Position: Mobile Networks for Industry Verticals: Spectrum Best Practice
GSMA Public Policy Position: Mobile spectrum for Unmanned Aerial Vehicles
GSMA Public Policy Position: Internet of Things

Industry position

Policymakers should ensure that verticals can get the connectivity they need to support their use cases without undermining other spectrum users while also upholding fair and efficient assignment of mobile bands.

A core concern is the use of dedicated set-asides for verticals since these pose significant risks to wider mobile services, most notably slower 5G networks and reduced coverage. There are other options to support verticals and other ways to provide access to spectrum for these networks.

Spectrum set-asides can lead to insufficient spectrum available for mobile operators to use and prevent them from meeting all 5G requirements and capabilities. Scarcity also encourages higher prices to be paid for spectrum, which is strongly linked to less network investment, slower roll-outs, limited coverage and reduced data speeds.

Where industries require access to specific licensed bands, they can do so via sharing and leasing agreements with mobile operators, for example.

The mobile industry believes:

» Commercial mobile operators already support the needs of a wide variety of vertical sectors and will have added capabilities with 5G.

Spectrum leasing or, when carefully planned, other types of spectrum sharing can be viable options for supporting verticals that want to build private networks.

» Spectrum that is set aside exclusively for verticals in core mobile bands risks being underused and can undermine fair spectrum awards.

» Spectrum that is set aside for mobile networks for verticals in core mobile bands can also threaten the wider success of 5G, including slower roll-outs, worse performance and reduced coverage.

» Policymakers should consider the coexistence challenges when different use cases need to be supported in the same mobile band.

» Unlicensed spectrum is likely to play an important role for numerous verticals.

» Policymakers should carefully consider their options and consult stakeholders to ensure they most efficiently support the needs of verticals without undermining other spectrum users.

Debate:

» *As governments turn their attention to supporting high-speed network roll-outs, regulators face the daunting challenge of deciding who gets access to spectrum. How can governments and regulators develop spectrum policies that support mobile networks for verticals without negatively affecting commercial 5G services?*

Wireless backhaul spectrum

Background

The evolution of advanced 4G and the emergence of 5G have created challenges for mobile backhaul – the connection between base stations and the mobile core. 4G and 5G access networks rely on high-quality backhaul networks. Therefore, backhaul must evolve to support significantly higher data speeds, greater resiliency and a wider variety of network deployments, as well as extend coverage further into rural areas.

While fibre remains the standard for backhaul due to its significant data capacity, wireless backhaul plays a vital role as fibre is not accessible or affordable at all sites. Terrestrial wireless backhaul is the most common backhaul method worldwide and will continue to be for the foreseeable future.

This is in large part due to the flexibility it offers, from high-frequency wireless backhaul bands that support the fastest 5G speeds, to lower microwave frequencies that support long-link distances for rural base stations.

Terrestrial wireless backhaul continues to evolve with new, extremely wide frequency bands, which will be essential for the fastest 5G speeds, and by supporting denser small cell networks in urban areas. New technologies can also support significantly more data on a given amount of bandwidth and enable bands to be aggregated to create wider bandwidths. Access spectrum is also sometimes used for backhaul in certain situations, known as 'in-band backhaul'.

Resources:

GSMA Backhaul Position Paper

Industry position

The combination of new bands and technologies can have a major impact on the performance of mobile networks and the kinds of services they can enable. Governments and national regulators have a role in opening new terrestrial backhaul bands vital for 5G while also evaluating how existing bands can evolve to be suitable for the 5G era and beyond.

This includes looking at widening channel sizes for key bands and, importantly, weighing the pros and cons of other users gaining access to backhaul bands. In the near term, the E-band (70–80 GHz) will be important, especially to support initial 5G growth, but the W-band (92–114 GHz) and D-band (130–175 GHz) will also be vital to powering 5G networks in years to come. V-band (66–71 GHz) is also likely to be used for backhaul and portions will be used for 5G access, as well. The E-band, D-band and W-band can handle 15 to 50 times more traffic than typical popular mid-microwave backhaul bands (e.g. 14–25 GHz).

Recommendations:

- New backhaul bands are needed to support evolving network requirements and increasing traffic (E, V, W and D bands).
- Current backhaul bands will still play an important role, but need support to maintain relevance in the 5G era, especially through wider channel sizes.
- Regulators need to carefully consider the most effective backhaul licensing terms approaches, terms and conditions.
- High backhaul spectrum prices are a barrier to the evolution of mobile networks, improved coverage and more spectrum-efficient backhaul technologies.
- Regulators should, in consultation with the industry, ensure the timely availability of a sufficient amount of affordable backhaul spectrum under reasonable licensing approaches, terms and conditions.

Debate:

- ***How can governments balance the need for new spectrum for 5G in currently used wireless backhaul bands and the future wireless backhaul needs of 5G?***

Consumer protection

Introduction

As mobile services become more economically and socially important, particularly the mobile internet, there is a corresponding need to ensure that the more than five billion people currently connected via these services can continue to enjoy them safely and securely. The challenge is providing this protection while also ensuring users have control over their privacy and personal data.

It is therefore essential for the mobile industry to deliver safe and secure technologies, services and apps that inspire trust and confidence. At the same time, consumers need to be educated about potential risks and be aware of the steps they can take to avoid those risks.

The mobile industry takes consumer protection seriously. The GSMA and its members play a leading role in developing and implementing appropriate safety and security solutions, technical standards and protocols. They also work with governments, multilateral organisations and non-governmental organisations (NGOs) to address concerns related to consumer protection by:

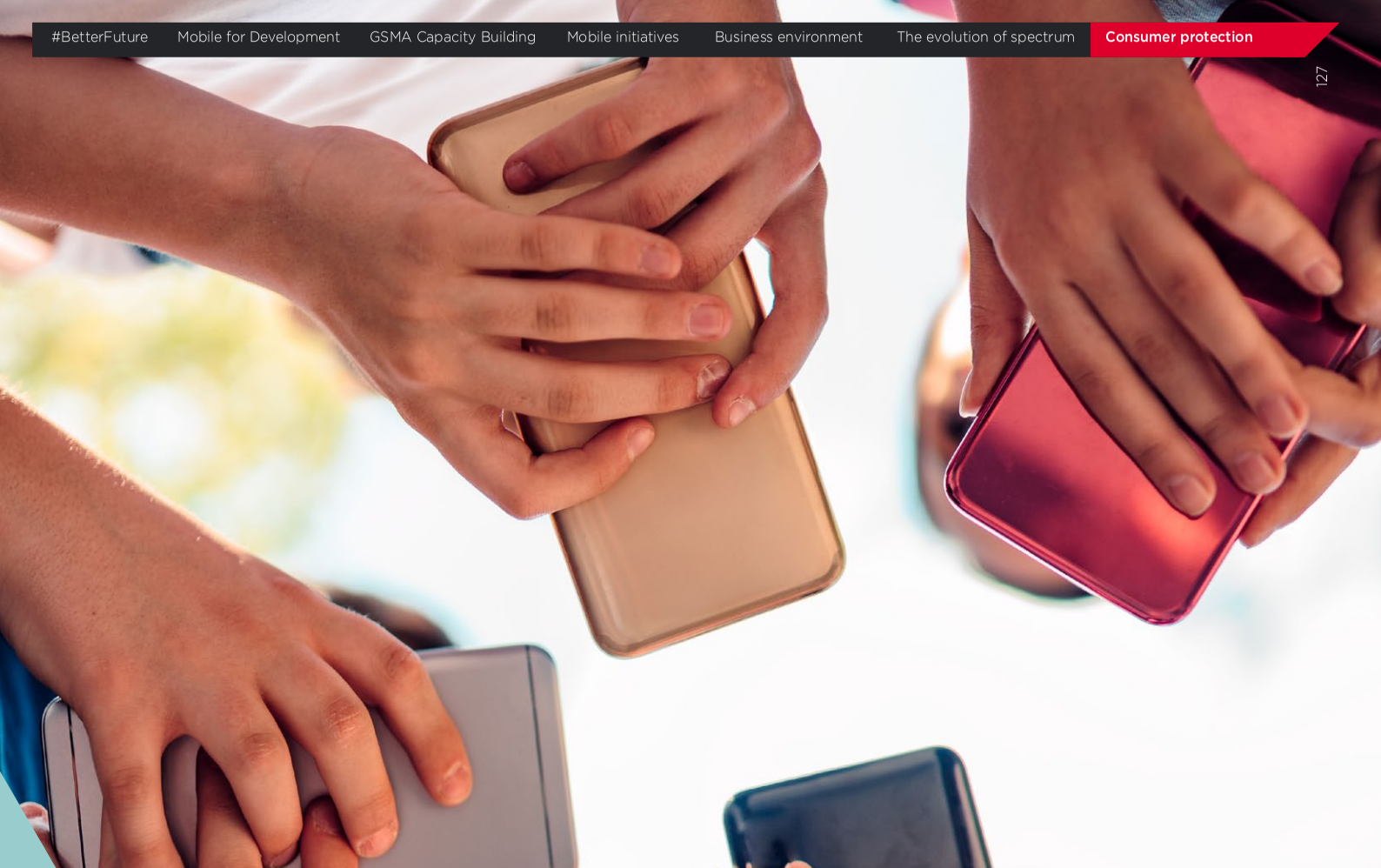
» Defining, sharing and promoting global best practice;

» Building and participating in cross-sector coalitions;

» Educating consumers and businesses in the safe use of mobile technologies and applications; and

» Commissioning research that offers real-world insight and evidence.

The following pages illustrate the work undertaken by the mobile industry to ensure consumers are appropriately protected and informed as they enjoy the full range of benefits made possible by mobile technology.



Cybersecurity

Background

The internet and mobile connectivity have become pervasive, making it vital to ensure that people can use essential services safely and securely.

Cyberattacks are not only harmful and criminal, but also undermine trust in digital services. The mobile industry is continually working to educate consumers while incorporating new features and enhancing existing security capabilities, such as encryption, integrity checking and user identity validation, to minimise the potential for fraud, identity theft and other possible threats. Governments and policymakers have put measures in place to prevent cyberattacks, and national and regional strategies have been adopted in many countries to strengthen resilience, build capacity and fight cybercrime.

'Cybersecurity' covers several areas,[14] but generally refers to the protection of network-related systems and devices and the software and data they contain. It typically comprises the protection of technical infrastructure, procedures and workflows, physical assets, national security, as well as the confidentiality, integrity and availability (CIA triad) of information.

The mobile industry has a long history of providing secure products and services to its customers:[15]

» **Protecting network infrastructure and devices**
Operators test for vulnerabilities and detect and deter malicious attacks on current generation and future networks. The GSMA and its members support the principles of 'security-by-design' to be applied across the value chain. The GSMA plays a central role in coordinating activity and leads industry-wide initiatives and programmes, such as the Fraud and Security Group (FASG), the Security Accreditation Scheme (SAS) and the Network Equipment Security Assurance Scheme (NESAS), which provides a security assurance framework to facilitate improvements in security levels across the mobile industry.[16]

» **Protecting public safety**
Mobile networks are considered to constitute critical national infrastructure in many jurisdictions, and the services they support play a key role in protecting the public. Operators have a legal obligation to assist law enforcement agencies, which they do while supporting human rights concerns.

Resources:

GSMA IoT Security
GSMA Report: The 5G Era: Age of Boundless Connectivity and Intelligent Automation
GSMA Report: Mobile Telecommunications Security Landscape 2021
GSMA Report: Cybersecurity: A Governance Framework for Mobile Money Providers
GSMA Blog Post: Cybersecurity and Mobile Money: Prioritising Consumer Trust and Awareness

14. ENISA. (2016). *Definition of Cybersecurity: Gaps and Overlaps in Standardisation.*
15. GSMA. (2017). *Safety, Privacy and Security Across the Mobile Ecosystem for All: Key Issues and Policy Implications.*
16. Network Equipment Security Assurance Scheme (NESAS).

- **Protecting consumers from fraud**
  Fraudulent attacks take many forms, such as identity theft, financial fraud, phishing, smishing or vishing, where victims are tricked into revealing sensitive personal information and service access credentials. Operators implement and offer solutions to prevent the use of networks to commit fraud and the use of devices to harm consumers.

- **Protecting consumer privacy**
  Information security implies that information, including personal data, is not accessible or disclosed to unauthorised individuals, entities or processes, and that it is maintained, complete and available, throughout its life. The GSMA has undertaken extensive work on data protection and data privacy.

Industry position

Cybersecurity is the shared responsibility of industry, government and regulators. Every actor in the digital value chain, across all sectors of the digital economy, needs to ensure the appropriate protection of infrastructure, products and services.

Given that cybersecurity risks are dynamic and not confined to national borders, sustained international multistakeholder cooperation in all areas of security is key to managing risks. Robust security measures must also be adopted by the entire digital value chain.

Mobile operators continue to invest in the security of their own networks, devices and services, building solutions and capabilities to detect and deter malicious attacks. They are improving preparedness and incidence response and contributing to the development of globally recognised, industry-led, voluntary consensus security standards, assurance programmes and conformity assessment schemes. They also continue to participate in capacity building, engage with experts in the field of cybersecurity and share best practices with other stakeholders.

Governments and law enforcement agencies should ensure there are appropriate legal frameworks, resources and processes in place to deter, identify, investigate and prosecute criminal behaviour. This requires global cooperation between governments and the wider ecosystem. Future-proofing across jurisdictions will ensure regulation and network security obligations are consistent and clear for all players involved in this complex and rapidly evolving area.

Debate:

- *In the context of 5G implementation and the expanding web of IoT devices and services, how can policymakers ensure that cybersecurity is the responsibility of everyone in the mobile ecosystem?*
- *What is needed to facilitate a more holistic response to cybersecurity?*

Children and mobile technology

Background

Young children and teenagers are enthusiastic users of mobile technology. Young people's knowledge of mobile apps and platforms often surpasses that of parents, guardians and teachers, and children now use social networking services more than their parents.

For growing numbers of young people, mobile technology is an increasingly important tool for communicating, accessing information, enjoying entertainment, learning, playing and being creative. As mobile technology becomes increasingly embedded in everyday life, mobile operators have an important role to play in protecting and promoting children's rights.

For children and youth, mobile devices can be key to accessing:

» Employment skills;

» Enhanced formal and informal education and learning;

» Information and services to aid in health and well-being;

» Improved social and civic engagement; and

» Opportunities to play and be creative.

Mobile devices increasingly play a role in formal education and informal learning. For people in LMICs 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, a mobile device can be used in ways that cause harm, so young people require guidance in order to benefit from mobile technologies safely and securely.

The mobile industry has taken active steps to help with the safe and responsible use of mobile services by children. The GSMA plays a leading role in self-regulatory initiatives on issues such as parental controls, education and awareness.

Resources:

UNICEF Guidelines for Industry on Child Online Protection Website
UNICEF Tools for Companies in the ICT Sector Website
ICT Coalition Website
GSMA mPower Youth: Enhancing Children's Lives through Mobile Website
GSMA and Child Helpline International: Internet Safety Guides
Global Kids Online: Research Results

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 reap the full benefits of mobile technology.

Addressing safe and responsible use of mobile by children and young people is best approached through multistakeholder efforts.

Working closely with UNICEF, the GSMA and its mobile operator members and a range of other organisations, including the the International Centre for Missing and Exploited Children (ICMEC) and INHOPE, hold national and regional multistakeholder workshops on the issue. These workshops bring together policymakers, NGOs, law enforcement and industry, to facilitate the development of collaborative approaches to safe and responsible use of the internet.

Through its mPower Youth programme, the GSMA also works closely with Child Helpline International to foster collaboration between mobile operators and child helplines in promoting children's rights – in particular their right to be heard – and to work together on areas of mutual concern, such as a safer internet.

The GSMA takes part in international initiatives related to safeguarding children online, including contributing to the ITU's Child Online Protection programme, and actively engages with governments and regulators looking to address this issue. Through its Capacity Building programme, for example, the GSMA helps policymakers better understand children's use of technology and discusses strategies for encouraging young people to become positive, engaged, responsible and resilient users of digital technology.

Young people are critical to the evolution of the mobile sector as they represent the first generation to have grown up in a connected, always-on world. They are future consumers and innovators who will deliver the next wave of innovation in mobile.

Debate:

- ***What potential harm are children exposed to in the online environment?***
- ***How can all stakeholders navigate the tensions between differing child rights in the digital world?***

As more young people are leading digital lives, they reach out to child helplines for support and guidance when they encounter problems online.

While many child helplines already have experience in this area, globally there are still many that would benefit from guidance on these issues. The GSMA and Child Helpline International wanted to extend their support to child helplines by harnessing the experience of experts from a range of stakeholder groups. In May 2016, they co-hosted an intensive one-day workshop that brought together the child helpline community, the Child Helpline International youth panel, mobile operators and other industry players, NGOs, child online safety experts, including a specialist child and adolescent psychiatrist and law enforcement.

The workshop kick-started the development of a series of high-level guides for child helpline counsellors and volunteers on nine common or challenging digital issues that lead young people to seek advice from helplines. The nine guides were launched in November 2016 and cover cyberbullying, discrimination and hate speech, grooming, illegal content, inappropriate content, privacy, sexual extortion, sexual harassment and unsolicited contact.

The guides were created with child helplines and their counsellors and volunteers in mind, especially those for whom internet safety issues were relatively new or where counsellor guidance and training was still under development. Each guide was created with input from a range of experts who also reviewed and approved the content. The guides are purposely high level to accommodate different local contexts, with each guide providing a definition and examples of the issue, discussion ideas with children, parents/caregivers, practical and technical advice, as well as 'red flags' that counsellors should watch for.

The 30th anniversary of the UN Convention on the Rights of the Child

1989 was a milestone year, as it marked both the agreement of the UN Convention on the Rights of the Child (UNCRC) and the birth of the World Wide Web.

The UNCRC sets out child-specific needs and rights that children everywhere are entitled to in order to survive and thrive, to learn and grow and to reach their full potential. It outlines children's rights to education, information, privacy and the highest attainable standard of health. It also outlines their rights to leisure and play, to be heard, as well as to protection from violence, sexual exploitation and abuse.

The provisions in the UNCRC were set out and agreed without knowledge of the technology revolution that would shortly follow. The UNCRC remains as important and relevant in today's connected world as it was for children at the time of its creation more than 30 years ago.

The GSMA supports its members as they seek to enable children to safely and positively

realise the many opportunities afforded through connectivity, while also taking steps to mitigate potential risks.

As the UNICEF State of the World's Children 2017 report notes, the internet "...reflects and amplifies the best and worst of human nature. It is a tool that will always be used for good and for ill. Our job is to mitigate the harms and expand the opportunities digital technology makes possible."

Cross-border data flows

Background

The global digital economy depends on cross-border flows of data to deliver crucial social and economic benefits to individuals, businesses and governments.

When data is allowed to flow freely across borders, it enables organisations to adopt data-driven digital transformation strategies that benefit individuals and society. Policies that inhibit the free flow of data through unjustified restrictions or local data storage requirements can have an adverse impact on consumers, businesses and the economy in general.[17]

Cross-border flows of personal data are currently regulated by several international, regional and national instruments and laws intended to protect the privacy of individuals, the local economy or national security.

While many of these instruments and laws adopt common privacy principles, they do not create an interoperable regulatory framework that reflects the realities, challenges and potential of a globally connected world. Emerging frameworks, such as APEC Cross-Border Privacy Rules and the EU Binding Corporate Rules, allow organisations to transfer personal data under certain conditions. They contain accountability mechanisms and are based on internationally accepted data protection principles.

However, their successful adoption is undermined by governments implementing data localisation rules (also known as 'data sovereignty') that impose local storage requirements or use of local technology.[18] Such localisation requirements can be found in a variety of sector- and subject-specific rules. They are sometimes imposed by countries based on the belief that supervisory authorities can more easily scrutinise data that is stored locally.[19]

Today, bilateral and multilateral trade agreements are incorporating more modern trading arrangements that recognise the potential of digital trade powered by open, cross-border data flows. These can act as a catalyst for continued growth that facilitates trade and improves productivity and economic well-being. Examples are the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the ASEAN Regional Comprehensive Economic Partnership (RCEP), the African Continental Free Trade Area (AfCFTA) and the EU Binding Corporate Rules.

Resources:

GSMA Mobile and Privacy Website
GSMA Report: Mobile Privacy Principles
GSMA Report: Smart Data Privacy Laws
GSMA Report: 5G and Data Privacy
GSMA Report: Safety, Privacy and Security Across the Mobile Ecosystem
GSMA Report: Protecting Privacy and Data in the Internet of Things

17. International Chamber of Commerce. (2016). *Trade in the Digital Economy*; ECIPE (2014) *The Cost of Data Localisation.*
18. Chander, A. and Le, U. (2015). "Data Nationalism". *Emory Law Journal*, 64(3); Hill, J.F. (2014). "The Growth of Data Localization Post-Snowden". The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, 2014.
19. European Commission Report. (2017). *Building a European Data Economy Communication.*

Industry position

Cross-border flows of data play a key role in innovation, competition and economic and social development. Governments can facilitate data flows in a way that is consistent with consumer privacy and local laws by supporting industry best practices and frameworks for the movement of data, and by working to make these frameworks interoperable.

Governments can also ensure these frameworks have strong accountability mechanisms and authorities have a role in overseeing and monitoring their implementation. Governments should only impose measures that restrict cross-border data flows if they are essential to achieving a legitimate public policy objective. The application of these measures should be proportionate and not arbitrary or discriminatory against foreign suppliers or services.

Mobile operators welcome frameworks such as the APEC Cross-Border Privacy Rules or the EU Binding Corporate Rules, which allow accountable organisations to transfer data globally provided they meet certain criteria. Such mechanisms are based on commonly recognised data privacy principles and require organisations to adopt a comprehensive approach to data privacy.

The frameworks encourage more effective protection for individuals than formal administrative requirements while also helping to realise potential social and economic benefits. Such frameworks should be made interoperable across countries and regions to the greatest extent possible. This would stimulate convergence between different approaches to privacy, while promoting appropriate standards of data protection and allow accountable companies to build scalable and consistent data privacy programmes.

Requirements for companies to use local data storage or technology create unnecessary duplication and costs. There is little evidence that the policies produce tangible benefits for local economies or improved privacy protections for individuals.

To the extent that governments need to scrutinise data for official purposes, mobile operators would encourage them to achieve this through existing lawful means and appropriate intergovernmental mechanisms that do not restrict the flow of data.

The GSMA and its members believe that cross-border data flows can be managed in ways that safeguard the personal data and privacy of individuals. We remain committed to working with stakeholders to ensure that restrictions are only implemented if they are necessary to achieve a legitimate public policy objective.

Debate:

- *How can industry, legislators, regulators and civil society engage effectively to develop policy that supports cross-border flows of data?*
- *How can data protection safeguards adequately address the legitimate concerns of governments that seek to impose localisation requirements?*

Deeper dive: National data privacy regimes

The challenge of regulating data privacy, including cross-border flows of data, is putting measures in place that consistently provide consumers with confidence in existing and new services without limiting service adoption or imposing significant additional costs on service providers.

To achieve this, it is crucial for privacy regulation to be based on shared core principles, which, according to United Nations Conference on Trade and Development (UNCTAD), are "at the heart of most national [privacy] laws and international regimes", as well as industry initiatives. This would allow companies to treat data consistently across their operations, innovate more rapidly, achieve greater scale and reduce costs. Consumers will benefit from wider choice, improved quality and lower prices of services.

The 2009 Madrid Resolution on International Standards for the Protection of Personal Data and Privacy, for example, encourages consistent international protection of personal data and embraces privacy approaches from all five continents. As well as being designed "to ease the international flow of personal data, essential in a globalised world"[20] the resolution advocates six privacy principles to be adopted by policymakers.

Figure 13

Lawful and fair	Purpose	Proportionate
Personal data must be lawfully and fairly processed	Processing should be limited to specified purposes.	Processing should be proportionate and not excessive.
Quality	**Openness**	**Accountable**
Data held should be accurate.	The processor should be open regarding their activities.	The processor should be accountable for their activities.

Similar principles are reflected repeatedly in laws and policy initiatives around the world, such as the Council of Europe Convention 108, the OECD Guidelines, the EU General Data Protection Regulation, the US Federal Trade Commission Fair Information Practice Principles and the APEC Privacy Framework. The mobile industry has also adopted the GSMA Mobile Privacy Principles to give consumers confidence that their personal data is being protected, irrespective of service, device or country.

20. International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution 2009.

Deeper dive: Localisation rules

There are several reasons why countries seek to justify imposing data localisation rules, including concerns about foreign surveillance and national security, as well as a desire to stimulate a national digital economy through in-country data analysis.

The range of localisation restrictions can include subjecting the data flows to certain restrictions to protect citizens' privacy and requiring organisations to keep data in-country but allowing the data to flow thereafter. It may also include requiring the data to be kept in-country or imposing requirements that have the indirect effect of keeping the data in-country, such as mandating the use of local infrastructure.

However, these restrictions do not necessarily lead to better protection of personal data and, in fact, can undermine it. For example, a fragmented approach results in inconsistent protection (e.g. differences across jurisdictions and sectors in what can be stored and for how long) and causes confusion, which ultimately has a negative impact on the secure management of personal data.

The risks identified by governments can be mitigated by various solutions and principles without restricting data flows. For example, internet platform companies and cloud computing providers are increasingly establishing regional hubs so that governments concerned about the surveillance activities of foreign countries can avoid data being held in particular jurisdictions. Encryption techniques also allow data to be protected from access and stored securely abroad. Requiring localisation on the grounds of a perceived economic benefit are equally flawed. Restricting data processing activities to a national rather than global scale, is likely to lead to significant operational costs per customer served and prevent citizens from accessing emerging innovative global digital services.

To address legitimate concerns about privacy, governments have adopted a patchwork of international, regional and national rules. In addition to the APEC Privacy Framework and the EU General Data Protection Regulation (GDPR), regional frameworks have emerged in the ASEAN region, Latin America and Africa. These frameworks are commendable in that they aim to align regional economies around a common understanding of data privacy. However, they need to be interoperable across regions to the greatest extent possible, to reflect the realities of a globally connected world. This would allow companies to build scalable and accountable data protection and privacy platforms.

Flows of data across borders are important for societal and economic reasons. Without them, economic growth and the potential benefits to society of digital transformation can be hampered. It is therefore incumbent on governments, regulators, industry and civil society groups to reject localisation measures and find other ways to enable the flow of data while also protecting individual privacy.

Data privacy

Background

Research shows that mobile customers are concerned about their privacy and want simple and clear choices for controlling how their private information is used. They also want to know they can trust companies with their data. A lack of trust can act as a barrier to growth in economies that are increasingly data-driven.

One of the major challenges created by the growth of the mobile internet is that the security and privacy of personal information is regulated by a patchwork of geographically bound privacy regulations while the mobile internet is, by definition, international. In many jurisdictions, the regulations governing how customer data is collected, processed and stored vary considerably between market participants. For example, the rules governing how personal data is treated by mobile operators may be different to those governing how it can be used by internet players.

This misalignment between national privacy laws and global standard practices makes it difficult for operators to provide customers with a consistent user experience. It may also cause legal uncertainty for operators, which can deter investment and innovation. Inconsistent levels of protection also create risks that consumers might unwittingly provide easy access to their personal information, leaving them exposed to unwanted or undesirable outcomes, such as identity theft and fraud.

Resources:

GSMA Mobile and Privacy Website
GSMA Report: Mobile Privacy Principles
GSMA Report: Smart Data Privacy Laws
GSMA Report: 5G and Data Privacy
GSMA Report: Protecting Privacy and Data in the Internet of Things
GSMA Report: Safety, Privacy and Security Across the Mobile Ecosystem

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.

Debate:

- *How can policymakers help create a privacy framework that supports innovation in data use while balancing the need for privacy across borders, regardless 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?*

Deeper dive: Smart data privacy practices and regulation

A combination of smart data privacy practices and regulation is required to sustain consumer trust in the digital ecosystem rapidly evolving around them.

The GSMA has developed eight Mobile Privacy Principles, as well as a range of resources to promote good practice. These resources include the GSMA's Privacy Design Guidelines for Mobile Application Development, which are considerations that should be taken into account when engaging in big data analytics and a Privacy by Design decision tree for use in developing IoT products and services. These guidelines seek to strike a balance between protecting privacy and enabling organisations to achieve commercial, public policy and societal goals.

If organisations adopt comprehensive policies, processes and practices to protect the privacy of individuals, and can easily demonstrate that these safeguards are effective, they will strengthen trust of consumers and regulators. Equally, if governments adopt smart data privacy rules, they can establish a regulatory environment that stimulates the digital economy while also unleashing its benefits for consumers and citizens.

While governments must ensure smart data privacy laws take account of citizens' privacy concerns, they must also recognise that these rules can have important consequences beyond the protection of privacy. As a result, when drafting these rules, governments must take into consideration how these laws sit within an economic and societal context.

Policymakers around the world have been studying the EU's GDPR and other regional and national frameworks or laws to inform their own legislative proposals. Among the lessons learned are that smart data privacy rules are:

- Horizontal, meaning they apply to all processing of personal data rather than focusing on just one technology or sector. This reduces the need for sectoral rules or operating licences that subject mobile operators to an additional set of competing privacy obligations.
- Principles-based, allowing innovation to thrive without having to reinvent the rules every time new technologies or business methods are introduced.
- Risk-based, encouraging companies to focus on preventing harm (for example, by setting a threshold for reporting data breaches rather than mandating that all breaches are reported), or encouraging organisations to implement Privacy by Design and privacy impact assessment processes.
- Based on the idea of accountability, holding companies to account, while allowing them to innovate and comply in a way that makes sense for their business and rewarding those that embed a culture of privacy in their organisations.
- Open to data flows, allowing data to cross borders provided there are sufficient safeguards to protect an individual's privacy (see the Cross-border data flows section).

Deeper dive: GSMA Mobile Privacy Principles

The GSMA has published a set of universal Mobile Privacy Principles that describe how mobile consumers' privacy should be respected and protected:

» **Openness, transparency and notice**
Responsible persons (e.g. application or service providers) shall be open and honest with users and will ensure users are provided with clear, prominent and timely information regarding their identity and data privacy practices.

» **Purpose and use**
The access, collection, sharing, disclosure and further use of personal information shall be limited to legitimate business purposes, such as providing applications or services as requested by users, or to otherwise meet legal obligations.

» **User choice and control**
Users shall be given opportunities to exercise meaningful choice and control over their personal information.

» **Data minimisation and retention**
Only the minimum personal information necessary to meet legitimate business purposes should be collected and otherwise accessed and used. Personal information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal retention obligations.

» **Respect user rights**
Users should be provided with information about, and an easy means to exercise, their rights over the use of their personal information.

» **Security**
Personal information must be protected, using reasonable safeguards appropriate to the sensitivity of the information.

» **Education**
Users should be provided with information about privacy and security issues and ways to manage and protect their privacy.

» **Children and adolescents**
An application or service that is directed at children and adolescents should ensure that the collection, access and use of personal information is appropriate in all given circumstances and is compatible with national law.

Privacy and big data

Background

Increases in computing power and falling prices of information technology systems make it possible to process huge volumes of data from a variety of sources, in a range of formats, at greater speed than ever before. It is now possible to analyse all data from one or more large data sets, rather than relying on smaller samples of data. This allows meaningful insights to be drawn, where appropriate, from mere correlations in the data rather than having to identify causal connections. These capabilities are often referred to as 'big data analytics' techniques.

At the same time, the Internet of Things (IoT) is equipping an ever-increasing number of devices with sensors that collect and communicate data.

Together, these capabilities represent a sea change in society's ability to create new products and services and solve some of the most pressing public policy needs of our time, from road management in congested and polluted urban areas to understanding and preventing the spread of diseases.

Mobile operators will increasingly use the information they collect for big data initiatives. They have an important role to play as responsible stewards of that data and potentially as facilitators in a future marketplace for access to this type of data.

However, big data capabilities also give rise to questions about security and privacy and how these important concerns can be addressed.

Resources:

GSMA Report: Mobile Privacy and Big Data Analytics
GSMA Report: Mobile Privacy Principles
GSMA Report: Privacy Design Guidelines for Mobile Applications
OECD Report: Data-driven Innovation for Growth and Well-being
Federal Trade Commission Report: Big Data: A Tool for Inclusion or Exclusion?

Industry position

The mobile industry recognises the societal benefits that can result from big data and wants to unlock the huge potential of big data analytics in a way that respects well-established privacy principles and fosters an environment of trust.

New laws are not necessary to address big data analytics and IoT. Rather, mobile operators recognise that existing privacy principles apply in these areas. Rules that restrict the legitimate use of data or metadata should be qualified and proportional to the risk of privacy harm that consumers might suffer if their data is misused. These rules should also be applied consistently across different industry sectors and types of technology.

Operators are well placed to understand the potential risks to individuals and groups from big data analytics and can implement measures to avoid or mitigate those risks.

New insights derived from the data will often give rise to new uses or 'purposes of processing' that had not been considered or identified when the data was initially collected. Accordingly, privacy frameworks must recognise this potential and make such uses possible.

Mobile operators can address these types of challenges and increase trust between industry stakeholders and consumers by:

» Building on existing privacy initiatives, such as the GSMA Mobile Privacy Principles and the Privacy Design Guidelines for Mobile Application Development.

» Finding innovative ways to provide individuals with meaningful choice, control and transparency to individuals on what data is collected and how it is used. For example, this could be addressed through user-friendly dashboards or signals from IoT devices easily discoverable by smartphones.

» Thinking carefully about the impact on individuals (and groups) of insights derived from big data and the actions or decisions that may be taken based on those insights.

» Reducing the risk of re-identification of individuals after data has been processed where this may raise privacy concerns.

» Establishing clarity on responsibilities between parties when collaborating on big data analytics projects.

» Incorporating ethical decision-making into governance models.

Equally, governments can ensure their country and citizens gain the most benefit from the potential of big data by:

» Understanding how big data analytics works and the context in which it takes place.

» Accommodating innovative approaches to transparency and consent.

» Developing and adopting practical industry guidelines and self-regulatory measures that seek to harness, rather than hinder, big data analytics.

Debate:

» ***How can mobile operators and policymakers help society realise the benefits of big data analytics in a privacy-protective manner and in compliance with applicable laws?***

» ***How can the GSMA strengthen the trust of stakeholders involved in collecting and analysing data?***

Electromagnetic fields and health

Background

Research into the safety of radio signals has been conducted for several decades and underpins human exposure limits that provide protection to all people (including children) against all established health risks.

The WHO and ITU encourage governments to adopt the radio frequency electromagnetic field (RF-EMF) exposure limits developed by the International Commission on Non-Ionizing Radiation Protection (ICNIRP). These were reviewed and updated in 2020.

New applications, such as 5G, wireless IoT and wearable devices, are designed to comply with relevant exposure limits. The international exposure guidelines are not technology-specific and apply to all mobile technologies, including 5G.

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 radio signals of mobile devices and mobile network antennas that comply with international safety recommendations.

However, research has suggested a possible increased risk of brain tumours among long-term users of mobile phones. As a result, in May 2011, the International Agency for Research on Cancer classified radio signals as a possible human carcinogen. Health authorities advise that given the scientific uncertainty and lack of supporting evidence from cancer trend data, this classification should be understood to mean that more research is needed. They also remind mobile phone users of practical measures for individuals to reduce exposure, such as using a hands-free kit or text messaging.

Mobile phones are tested for compliance with exposure limits when operating at maximum power. In use a mobile phone operates at a much lower power level.

For mobile networks, whether 2G, 3G, 4G or 5G, the typical levels in publicly accessible areas are a small fraction of the exposure limits and similar to broadcast services.

A comprehensive health-risk assessment of radio signals is being conducted by the WHO. The conclusions are expected in late 2022.

Resources:

WHO International EMF Project Website
GSMA Report: EMF Exposure Compliance Policies for Mobile Network Sites
GSMA Report: International EMF Exposure Guidelines
GSMA Website: Safety of 5G Networks
GSMA Interactive Map: 5G EMF Surveys

Industry position

National authorities should implement EMF-related policies based on established science, in line with international recommendations and technical standards.

Significant differences between national limits and international guidelines can cause confusion and increase public anxiety. Consistency is vital, and governments should:

- Base EMF-related policy on reliable information sources, including the WHO, trusted international health authorities and expert scientists.
- Set a national policy covering the siting of masts, balancing effective network roll-out with consideration of public concerns.
- Accept mobile operators' declarations of compliance with international or national radio frequency levels using technical standards from organisations such as the International Electrotechnical Commission (IEC) and the ITU.
- Actively communicate with the public and address their concerns based on the positions of the WHO.

Parents should have access to accurate information so they can decide when and whether their children should use mobile phones. The current WHO position is that international safety guidelines protect everyone in the population with a large safety factor, and that there is no scientific basis to restrict children's use of phones or the locations of base stations. We encourage governments to provide information and voluntary practical guidance to consumers and parents based on the position of the WHO.

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

The mobile industry works with national and local governments to help address public concerns about mobile communications. Adoption of evidence-based national policies for exposure limits and siting of antennas, public consultations and information can help to reassure the public.

On-going, high-quality independent 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.

Debate:

- ***Does using a mobile phone regularly or living near a base station have any health implications?***
- ***Are there benefits to adopting the updated international EMF limits for mobile networks or devices?***
- ***Should there be specific restrictions to protect children, pregnant women or other potentially vulnerable groups?***

Deeper dive: Health authorities on the science

To date, and after much research performed, no adverse health effect has been causally linked with exposure to wireless technologies. Health-related conclusions are drawn from studies performed across the entire radio spectrum but, so far, only a few studies have been carried out at the frequencies to be used by 5G.

Tissue heating is the main mechanism of interaction between radiofrequency fields and the human body. Radiofrequency exposure levels from current technologies result in negligible temperature rise in the human body.

As the frequency increases, there is less penetration into the body tissues and absorption of the energy becomes more confined to the surface of the body (skin and eye). Provided that the overall exposure remains below international guidelines, no consequences for public health are anticipated.

– WHO Question and Answer, February 2020

Most of the epidemiological research does not support an association between mobile phone use and tumours occurring in the head, which is the body part with the highest exposure to radio frequency electromagnetic fields. In studies reporting positive associations, it is difficult to exclude various forms of bias, such as recall bias in retrospective exposure assessment.

– International Agency for Research on Cancer, IARC, 2020

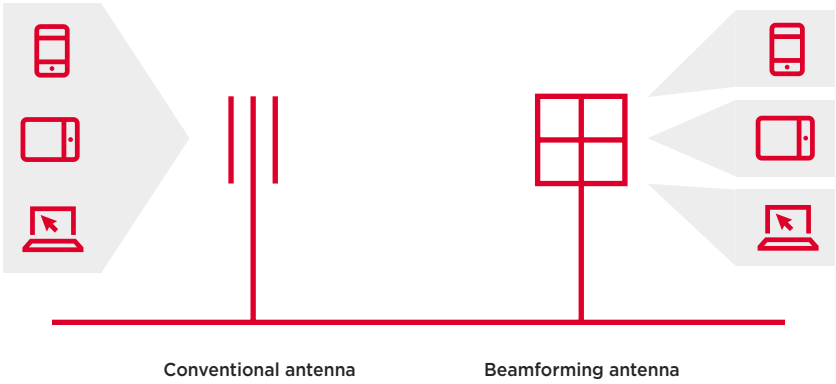
A large number of studies have been undertaken on both acute and long-term effects from RF EMF exposure typical of base stations. Research at these levels of exposure has provided no conclusive evidence of any related adverse health effects.

– International Commission on Non-Ionizing Radiation Protection (ICNIRP), accessed January 2022

Deeper dive: Advanced antenna technologies

Many of the antennas used for 5G are similar to those in use today. Advanced antenna technologies, such as beamforming, require the use of arrays of small antenna elements to optimise the delivery of radio signals to connected mobile devices. At high-band 5G frequencies these antennas can be small.

Figure 14 **Conventional and beamforming antennas**



As shown in Figure 14, a conventional base station antenna transmits a radio signal to a wide area regardless of how many users are connected while advanced beamforming antennas transmit radio signals to connected users, reducing unwanted signals.

Deeper dive: A global look at mobile network exposure limits

The WHO endorses the guidelines of the ICNIRP and encourages countries to adopt them. While many countries have adopted this recommendation, some have chosen to adopt other limits or additional measures on the siting of base stations.

A map on the GSMA website shows the approach to radio frequency (RF) exposure limits that countries have adopted for mobile communication antenna sites. Much of the world follows the ICNIRP guidelines or the similar US Federal Communications Commission (FCC) rules.

In some cases (e.g. China and Russia) RF limits have not been updated to reflect more recent scientific knowledge. In other cases, limits applicable to mobile networks may be the result of arbitrary reductions made as a political response to public concern.

Excluding countries or territories with unknown RF limits, 137 apply ICNIRP (1998 or 2020 limits), 10 follow the FCC limits from 1996 and 37 have other limits. For the 'Other' category, there are many differences between these countries in their limit values and application.

Resources:

GSMA EMF Policy Website

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 to access illegal content, ranging from pirated material that infringes intellectual property rights (IPR) to racist content or child sexual abuse material (child pornography).

Laws regarding illegal content vary considerably. Some content, such as child sexual abuse material, is considered illegal around the world, while other content, such as dialogue that calls for political reform, is illegal in some countries while in others they are protected by rights to freedom of expression.

Communications service providers, including mobile 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 based on relevant data protection, privacy and disclosure legislation. In the case of child sexual abuse content, mobile operators use terms and conditions, notice and takedown processes and reporting mechanisms to keep their services free of this material.

Resources:

GSMA Reference Document: Mobile Alliance Against Child Sexual Abuse Content Interpol Crimes Against Children
GSMA and UNICEF Report: Notice and Takedown: Company Policies and Practices to Remove Online Child Sexual Abuse Material
GSMA Guide: Hotlines: Responding to Reports of Illegal Online Content
GSMA and Child Helpline International Guides: Internet Safety Guides
International Centre for Missing and Exploited Children Report: Model Legislation and Global Review
INHOPE
WePROTECT Global Alliance Guidance Document: The Model National Response

Industry position

The mobile industry is committed to working with law enforcement agencies and appropriate authorities and 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 constitutes illegal content, the scope of which is broad 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 placing responsibility for enforcement on hotlines, law enforcement agencies and industry.

The mobile industry condemns the misuse of its services for sharing child sexual abuse content. The GSMA 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 the prevention of unauthorised distribution.

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 governments, law enforcement or industry have in the policing and removal of illegal content?***
- ***Should access to illegal content on the internet be blocked by ISPs and mobile operators?***

Deeper dive: Mobile Alliance Against Child Sexual Abuse Content

The Mobile Alliance Against Child Sexual Abuse Content was founded by an international group of mobile operators within the GSMA to obstruct the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content.

Figure 15 **Mobile Alliance procedures to stop child sexual abuse content**

Alliance members have made the commitment to:

» Implement technical mechanisms to restrict access to websites or URLs identified by an appropriate, internationally recognised agency as hosting child sexual abuse content.

» Implement notice and take-down processes to enable the removal of any child sexual abuse content posted on their own services.

» Support and promote hotlines or other mechanisms for customers to report child sexual abuse content discovered on the internet or on mobile content services.

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

The Mobile Alliance also contributes to wider efforts to eradicate online child sexual abuse content by publishing guidance and toolkits for the benefit of the entire mobile industry. For example, it has produced a guide to establishing and managing a hotline in collaboration with INHOPE, the umbrella organisation for hotlines, and a guide to implementing notice and take-down processes with UNICEF.

In the 10 years since the Mobile Alliance was founded, changes to the digital ecosystem, including the increase in online interactivity and user-generated content, have altered the nature of online child sexual exploitation and abuse. For example, hotlines are increasingly seeing self-generated content (also known as 'sexting') being shared online. Child helplines are receiving calls from young people reporting 'sexual extortion' or being blackmailed by an offender using self-produced sexual images or videos to make sexual or financial demands.

GSMA and Mobile Alliance members continue to work with their external partners to monitor emerging issues such as these and find additional ways to contribute to wider efforts to address them. For example, they are collaboratively developing guidance for child helpline counsellors on internet safety issues (including illegal content and sexual extortion) and members lead internet safety consumer education and awareness campaigns on an on-going basis.

Internet governance

Background

Internet governance involves an array of activities related to the policy and procedures of the management of the internet. It encompasses legal and regulatory issues, such as privacy, cybercrime, intellectual property rights and spam. It is also concerned with technical issues related to network management and standards, and economic issues such as taxation and internet interconnection arrangements.

Because the growth of the mobile industry is tied to the evolution of internet-enabled services and devices, decisions about the use, management and regulation of the internet affect mobile service providers and other industry players and their customers.

Internet governance requires input and collaboration from diverse stakeholders relating to their interests and expertise in technical engineering, resource management, standards and policy issues, among others. Relevant stakeholder groups will vary depending on the specific internet governance issues that are being addressed.

Resources:

Internet Governance Forum Website
Internet Society Internet Governance Website
UNESCO Internet Governance Website

"Only a concerted joint global effort by governments, businesses, the technical community and civil society will produce a governance architecture that is as generic, scalable and transnational as the internet itself. No single actor or group of actors can solve this alone."

– Vint Cerf, Chief Internet Evangelist at Google and Co-inventor of the Internet Protocol suite, February 2018

Industry position

The internet should be secure, stable, trustworthy and interoperable, and no single institution or organisation can or should manage it. The existing multistakeholder model for internet governance and decision-making should be preserved and allowed to evolve.

Given the ubiquity of the internet in today's world, any architecture designed to govern its use should be capable of addressing a range of issues and challenges relevant to different stakeholders in a manner that is more agile and flexible than traditional government and intergovernmental mechanisms.

Collaborative, diverse and inclusive decision-making models are required for stakeholders to participate in internet governance.

The decentralised development of the internet should continue, without the control of a particular business model or regulatory approach.

Some internet governance issues warrant a different approach at the local, national, regional or global level. An effective and efficient multistakeholder model ensures that stakeholders, within their respective roles, can participate in building consensus on such issues.

Technical aspects related to the management and development of internet networks and architecture should be addressed collaboratively by different stakeholder groups through relevant standards bodies, the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB) and other forums.

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

Debate:

- ***Who 'owns' the internet?***
- ***Should certain countries or organisations be allowed to have greater decision-making powers than others about the management of the internet?***
- ***How should a multistakeholder model be applied to internet governance?***

Mandated government access

Background

Mobile operators are often subject to a range of laws and/or licence conditions that require them to support law enforcement and security activities in countries where they operate. These requirements vary from country to country and have an impact on the privacy of mobile customers.

Where they exist, such laws and licence conditions typically require operators to retain data about their customers' mobile service use and disclose it, including their 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 the industry in protecting the privacy of its customers' information and their communications.

Legislation often lags behind technological developments. For example, obligations may apply only to established telecommunications operators but not to more recent market entrants, such as those providing internet-based services, including Voice over IP (VoIP), video or instant messaging.

In response to public debate concerning the extent of government access to mobile subscriber data, a number of major telecommunications providers (such as AT&T, Deutsche Telekom, Orange, Rogers, SaskTel, Sprint, T-Mobile, TekSavvy, TeliaSonera, Telstra, Telus, Verizon, Vodafone and Wind Mobile), as well as internet companies (such as Apple, Amazon, Dropbox, Facebook, Google, LinkedIn, Microsoft, Pinterest, Snapchat, Tumblr, Twitter and Yahoo!) publish 'transparency reports' that provide statistics relating to government requests for disclosure of such data.

Resources:

United Nations General Assembly Report: Guiding Principles on Business and Human Rights – Implementing the United Nations 'Protect, Respect and Remedy' Framework Sixth Form Law – Malone v. The United Kingdom Website
High Court Judgement: Data Retention and Investigatory Powers Act 2014 (DRIPA)

Industry position

Governments should ensure they have a proportionate legal framework that clearly specifies the surveillance powers available to national law enforcement and security agencies.

Any interference with the right to privacy of telecommunications customers must be in accordance with the law.

The retention and disclosure of data and the interception of communications for law enforcement or security purposes should take place only under a clear legal framework and using the proper process and authorisation specified by that framework.

There should be a legal process available to telecommunications providers to challenge requests which they believe to be outside the scope of the relevant laws.

The framework should be transparent, proportionate, justified and compatible with human rights principles, including obligations under applicable international human rights conventions, such as the International Convention on Civil and Political Rights. Given the expanding range of communications services, the legal framework should be technology-neutral.

Governments should provide appropriate limitations of liability or indemnify telecommunications providers against legal claims brought in respect of compliance with requests and obligations for the retention, disclosure and interception of communications and data.

The costs of complying with all laws covering the interception of communications and the retention and disclosure of data should be borne by governments. Such costs and the basis for their calculation should be agreed in advance.

The GSMA and its members are supportive of initiatives that seek to increase government transparency and the publication by government of statistics related to requests for access to customer data.

Debate:

- ***What is the correct legal framework to achieve a balance between a government's obligation to ensure its law enforcement and security agencies can protect citizens and the rights of those citizens to privacy?***
- ***Should all providers of communications services be subject to the same interception, retention and disclosure laws on a technology-neutral basis?***
- ***Would greater transparency about the number and nature of requests governments make assist the debate, improve government accountability and bolster consumer confidence?***

Deeper dive: Trending towards transparency

There is an important global debate on the scope, necessity and legitimacy of the legal powers government authorities use to access the communications of private individuals. ICT firms are increasingly reporting the demands of governments for communications data where it is legal to do so. These reports have revealed the degree to which government intelligence and law enforcement agencies rely on such information.

Many of the largest communications and internet content providers (including AT&T, Deutsche Telekom, Telenor, Verizon, Vodafone, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter and Yahoo!) publish periodic transparency reports.

Typically, these reports include how many of these requests resulted in the disclosure of customer information. They reveal the frequency of such requests, as well as some detail about the kind of information accessed. This can include customer account information, the interception of communications and metadata, which can reveal an individual's location, interests or relationships. Mobile operators often have no option but to comply with such requests, but they are increasingly pressing for greater transparency about the nature and scale of government access.

Questions have also arisen about the role of telecommunications network and service providers in relation to such access. For example, misunderstandings can arise about the extent to which mobile operators have the technical capacity to intercept communications. Intercepting standard phone calls or SMS messages to and from specific users is technically possible, and lawful interception requirements and capabilities have been described in global mobile standards for decades.

However, communications between users on an internet-based platform, known as an over-the-top (OTT) service, is generally beyond the reach of mobile operators. OTT messaging applications are usually encrypted and messages are not stored by operators, nor are decryption keys made available to them. This leaves operators unable to access or provide the content of messages, even by lawful request. Both internet companies and mobile operators may find themselves in a difficult position, bound to meet their obligations to provide lawful access while also assuring their customers that they protect their personal information.

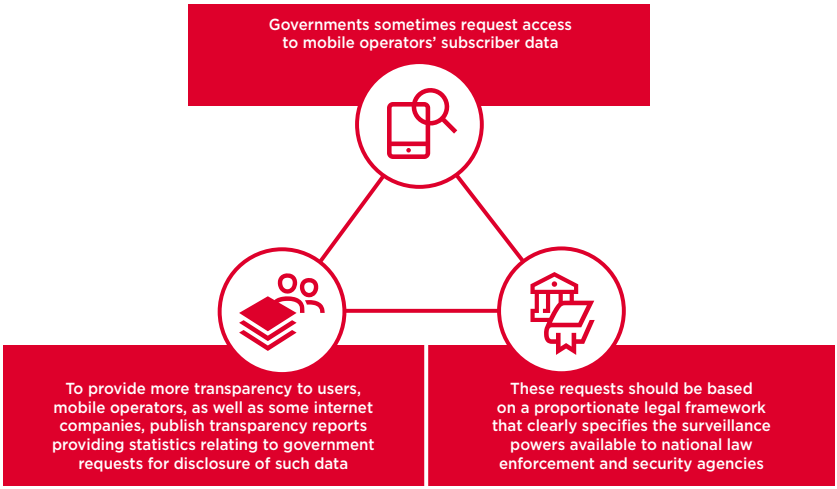
To further support their commitment to transparency, some operators have joined forces with internet companies and other stakeholders in initiatives such as the Global Network Initiative (GNI). The GNI brings together telecommunications operators, major internet companies, leading academics, civil society organisations and investors to advance privacy and freedom of expression in the ICT sector. In March 2017, seven operators – Millicom, Nokia, Orange, Telefónica, Telenor Group, Telia Company and Vodafone – joined an expanded GNI after having promoted transparency through the Telecommunications Industry Dialogue. These companies committed to the GNI

Principles on Freedom of Expression and Privacy, which provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of these human rights globally.

Civil society organisations have contributed to the advancement of these issues by trying to provide trustworthy measures of transparency. Ranking Digital Rights (RDR) publishes an annual report on telecoms' and internet companies' disclosed commitments, policies and practices that affect users' privacy and freedom of expression. The RDR calls for governments to allow encryption and publish their own transparency reports to make it clear what information they demanded from companies and why.

The debate can be heated between those who argue that law enforcement agencies require broad access to fight crime and those who challenge the level of government inquiry into private lives and strive to maintain citizens' rights to privacy in the digital age. GSMA members maintain that transparency reporting brings valid information to the public and policymakers, raising key questions about the balance between government access and privacy.

Figure 16 **Government access – encouraging transparency**



Case study: National regulatory approaches to government access

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

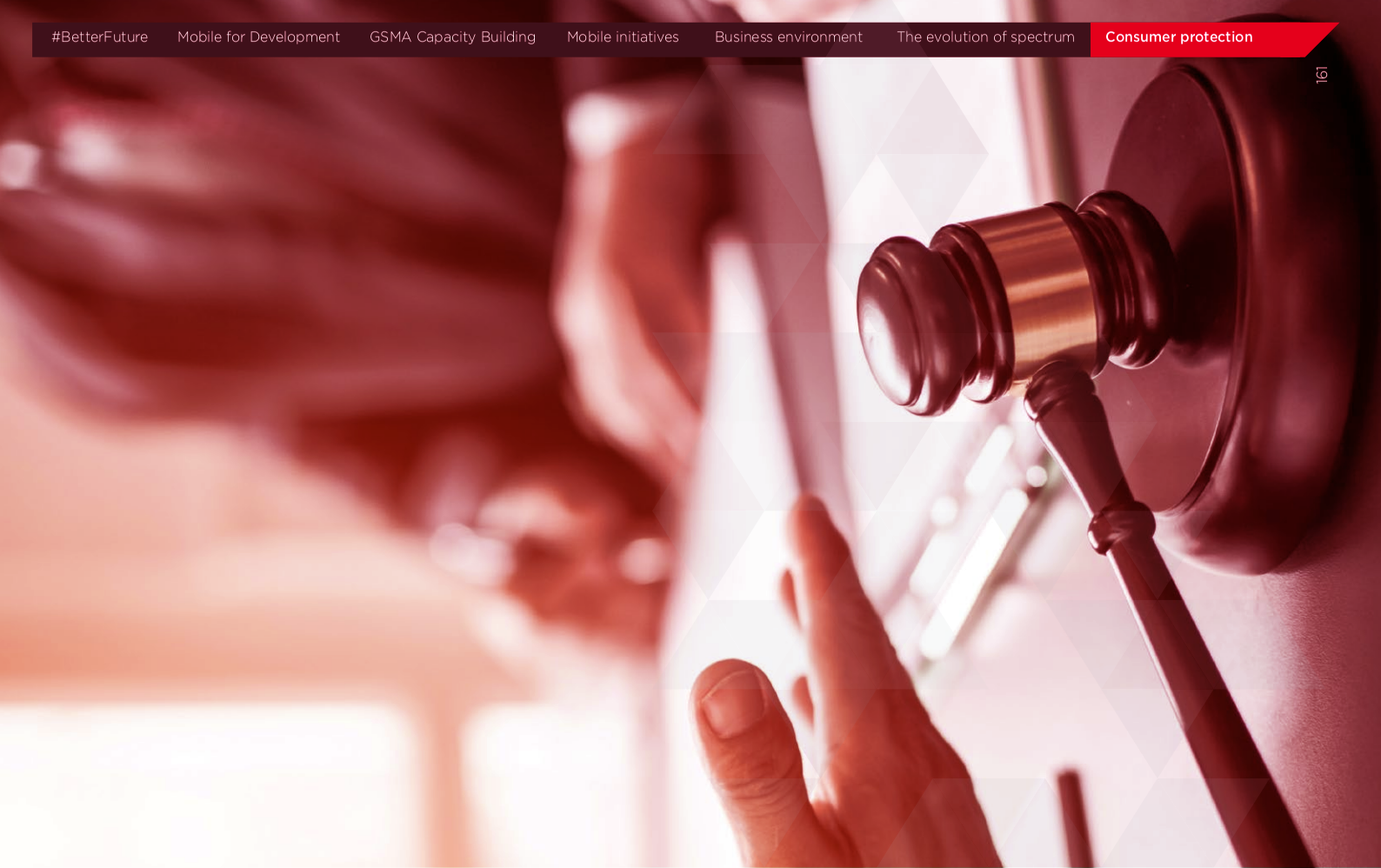
In the UK, communications service providers are required to separately retain a range of account and communications data and must ensure the data can be disclosed in a timely manner to UK law enforcement agencies, the security services and a number of prescribed public authorities under the UK Regulation of Investigatory Powers Act (RIPA). Prescribed authorities can also seek a warrant from the Secretary of State to intercept communications. The two main objectives of RIPA are to regulate the investigatory powers of the state and to set the legitimate expectations for citizens' privacy. As RIPA is subject to oversight by the Surveillance Commissioner and the Interception Commissioner, citizens can seek redress for alleged unlawful access to their data or communications, and service providers operating in the UK can raise concerns about the validity of requests.

In April 2014, the European Court of Justice ruled that the EU Data Retention Directive is 'invalid' because it violated two basic rights: respect for private life and protection of personal data. The European Commission has emphasised that the decision of whether to introduce national data-retention laws is a national decision and consequently, the UK and several other EU countries are reviewing their data-retention laws, which required communications service providers to store communications data for up to two years.

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

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

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



Mandated service restriction orders

Background

From time to time, mobile operators receive orders from government authorities to restrict services on their networks. These service restriction orders (SROs) require operators to shut down or restrict access to their mobile network, network service or Over The Top (OTT) service. Orders include blocking particular apps or content, restricting data bandwidth and degrading the quality of SMS or voice services. In some cases, operators would risk criminal sanctions or the loss of their licence if they disclosed that they had been issued with an SRO.

SROs can have serious consequences. For example, national security can be undermined if powers are misused, and public safety can be endangered if emergency services and citizens are unable to communicate with one another. Freedom of expression, freedom of assembly, freedom to conduct business and other human rights can also be affected.

Individuals and businesses can also be affected by an SRO, unable to pay friends, suppliers or salaries. This can have a knock-on effect on credit and investment plans, ultimately damaging a country's reputation for managing the economy and foreign investment and discouraging donor countries from providing funds or other resources.

MNOs also suffer. Not only do they sustain financial losses from the suspension of services and damage to their reputation, but their local staff can also face pressure from authorities and possibly even public retaliation.

Resources:

Australian Government Draft Guidelines on Website Blocking
Global Network Initiative and the Telecommunications Industry Dialogue Joint Statement: Service Restrictions
Telia Company Form for Assessment and Escalation of SROs

Industry position

The GSMA discourages the use of SROs. Governments should only resort to SROs in exceptional and pre-defined circumstances, and only if absolutely necessary and proportionate to achieve a specified and legitimate aim that is consistent with internationally recognised human rights and relevant laws.

To aid transparency, governments should only issue SROs to operators in writing, citing the legal basis and with a clear audit trail to the person authorising the order. They should inform citizens that the service restriction has been ordered by the government and has been approved by a judicial or other authority in accordance with administrative procedures laid down in law. They should allow operators to investigate the impacts on their networks and customers and to communicate freely with their customers about the order. If it would undermine national security to do so at the time when the service is restricted, citizens should be informed as soon as possible after the event.

Governments should seek to avoid or mitigate the potentially harmful effects of SROs by minimising the number of demands, the geographic scope, the number of potentially affected individuals and businesses, the functional scope and the duration of the restriction.

For example, rather than block an entire network or social media platform, it may be possible for the SRO to target particular content or users. In any event, the SRO should always specify an end date. Independent oversight mechanisms should be established to ensure these principles are observed.

Operators can play an important role by raising awareness among government officials of the potential impact of SROs. They can also be prepared to work swiftly and efficiently to determine the legitimacy of the SRO once it has been received. This will help establish whether it has been approved by a judicial authority, whether it is valid and binding and whether there is opportunity for appeal, working with the government to limit the scope and impact of the order. Procedures can include guidance on how local personnel are to deal with SROs and the use of standardised forms to quickly assess and escalate SROs to senior company representatives.

All decisions should first and foremost be made with the safety and security of the operators' customers, networks and staff in mind, and with the aim of being able to restore services as quickly as possible.

Debate:

- *What factors and alternatives should governments consider before planning an SRO?*
- *What tools and methods can be used to avoid the need for an SRO or to avoid negative impacts if an SRO is the only option?*

Mandatory registration of prepaid SIMs

Background

In a number of countries, customers of prepaid or pay-as-you-go (PAYG) services can anonymously activate their subscriber identity module (SIM) card simply by purchasing credit, as formal user registration is not required. Some 150 governments around the world[21] have mandated prepaid SIM registration, citing a perceived but unproven link between the introduction of such policies and the reduction of criminal and anti-social behaviour. Mandated prepaid SIM registration is most prevalent in Africa, where 90 per cent of UN-recognised states have such laws.

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

SIM registration can, however, allow many consumers to access value-added mobile and digital services that would not otherwise be available to them as unregistered users, including identity-linked services such as mobile money, e-health and e-government services.

For a SIM registration policy to create positive outcomes for consumers, it must be implemented in a pragmatic way that takes local market conditions into account, such as the ability of mobile operators to verify customer IDs. If registration requirements are too onerous for a customer to meet, mandating a SIM registration policy may lead to implementation challenges and unforeseen consequences. For example, it could unintentionally exclude vulnerable and socially disadvantaged consumers or refugees who lack the required IDs. It might also lead to the emergence of an underground market for fraudulently registered or stolen SIM cards, driven by the desire of some mobile users, including criminals, to remain anonymous.

Resources:

GSMA Mandatory Registration of Prepaid SIMs website
GSMA Report: Access to Mobile Services and Proof of Identity
GSMA Policy Note: Enabling Access to Mobile Services for the Forcibly Displaced
GSMA Report: Mandatory Registration of Prepaid SIM Cards: Addressing Challenges through Best Practice
GSMA Report: Regulatory and Policy Trends Impacting Digital Identity and the Role of Mobile

21. GSMA. (2021). Access to Mobile Services and Proof of Identity.

Industry position

While registration of prepaid SIM card users can deliver valuable benefits to citizens, governments should not mandate it.

To date, there has been no empirical evidence that mandatory SIM registration directly leads to a reduction in crime. Where a decision to mandate the registration of prepaid SIM users has been made, we recommend that governments take into account global best practices and allow registration mechanisms that are flexible, proportionate and relevant to the specific market, including the level of official ID penetration in that market and the timing of any national identity roll-out plans.

If these conditions are met, the SIM registration exercise is more likely to be effective and lead to more accurate customer databases. Furthermore, a robust customer verification and authentication system can enable mobile operators to facilitate the creation of digital identity solutions, empowering customers to access a variety of mobile and non-mobile services.

We urge governments considering the introduction or revision of mandatory SIM-registration to take the following steps prior to finalising their plans:

- Consult, collaborate and communicate with mobile operators before, during and after the implementation exercise.
- Balance national security demands against the protection of citizens' rights, particularly where governments mandate SIM registration for security reasons.
- Set realistic timescales for designing, testing and implementing registration processes.
- Provide certainty and clarity on registration requirements before any implementation.
- Allow and/or encourage the storage of electronic records and design registration processes that are administratively 'light'.
- Allow and/or encourage the SIM-registered customer to access other value-added mobile and digital services.
- Support mobile operators in the implementation of SIM-registration programmes by contributing to joint communication activities and to their operational costs.

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?*

Misinformation and disinformation

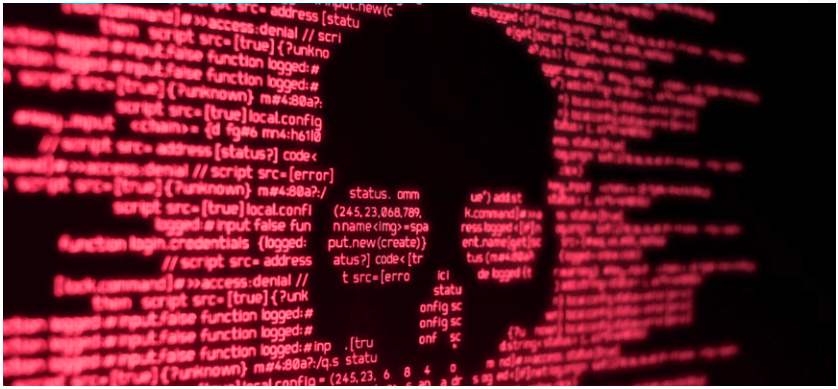
Background

It is important to distinguish between misinformation and disinformation. Misinformation is information that is false but not created with the intent to cause harm. Disinformation is information that is false and deliberately created to harm a person, social group, organisation or country.

Mobile operators do not typically host content, but they can nevertheless be affected by false information. In particular, misinformation linking 5G and the COVID-19 pandemic has had direct consequences for the industry, such as attacks on telecommunications equipment and staff.

Through its work with the mobile industry, the GSMA provides access to factual information, including independent expert reports on EMF and health.

In some countries, governments have used service restriction orders (SROs) to require operators to shut down or restrict access to their mobile network or service or an Over The Top (OTT) service. Orders can include blocking particular apps or content, restricting data bandwidth and degrading the quality of SMS or voice services. This can have consequences for customers and society in general.



Resources:

GSMA Report: Mobile Privacy Principles
GSMA EMF and Health Website
GSMA Report: Exploring Online Misinformation and Disinformation in Asia Pacific
GSMA Report: Safety, Privacy and Security across the Mobile Ecosystem
EU Code of Practice on Disinformation
WHO FAQ: Radiation: 5G Mobile Networks and Health
WHO Mythbusters: 5G Mobile Networks DO NOT Spread COVID-19

Industry position

False information can have a harmful impact on society. It can erode public confidence and distort perceptions of independently verifiable facts, leading to a lack of public trust in democratic processes and in institutions. It can also create or deepen tensions in society by exploiting individual or collective vulnerabilities.

Governments and policymakers should explore appropriate countermeasures to false online information. The EU Code of Practice on Disinformation, signed by online platforms, is an example of organisations collaborating to create an accountability mechanism and opportunities to share information and best practice.

Awareness campaigns can also be used to point citizens to trustworthy sources of information, equip them with tools to use technology safely and provide a mechanism to report websites containing false or harmful information.

Mobile operators continue to communicate accurate information on their networks and services to their customers.

While governments and law enforcement agencies have a legitimate mandate to protect citizens, this sometimes leads them to use powers that require mobile operators to block or restrict communication services. Internet shutdowns should be avoided or used only in very exceptional and predefined circumstances.

Debate:

- *Who determines whether information is true or false?*
- *What are the most effective mechanisms to deal with misinformation and disinformation?*

Mobile devices: counterfeit

Background

A counterfeit mobile device explicitly infringes the trademark or design of an original or authentic branded product, even where there are slight variations to the established brand name.

Due to their illicit nature, these mobile devices are typically shipped and sold on shadow or underground markets globally by organised criminal networks. It is estimated that almost one in five mobile devices may be counterfeit[22]. This has far-reaching negative impacts. Consumers risk lower quality, safety, security, environmental health and privacy assurances. Governments forego taxes and duties and must contend with increased crime. Industry players are also affected, as it can harm their trademarks and brands.

Some countries are considering introducing national lists of homologated (i.e. approved) devices to combat counterfeiting, smuggling and tax evasion. The purpose of homologated lists is to indicate which devices are permitted access to mobile networks. Operators add device-blocking capabilities to their local networks and connect with the national homologated list to ensure only permitted devices are allowed network access.

However, counterfeit mobile devices are not easy to identify and block, given that many have International Mobile Equipment Identity (IMEI) numbers that appear legitimate. It is now common for counterfeiters to hijack IMEI number ranges allocated to legitimate device manufacturers for use in their products, which makes it more difficult to differentiate between authentic and counterfeit products.

Industry position

The mobile industry supports the need for legal and product integrity in the device market and is increasingly concerned about the negative impact of counterfeit devices on consumer welfare and society in general.

Although mobile operators and legitimate vendors cannot stop the production and distribution of counterfeit devices, multistakeholder collaboration can help combat the issue at the source. National law enforcement and customs agencies should take measures to stop the production and exportation of counterfeit devices in their jurisdictions. Information on crime patterns and specific criminal activity relating to counterfeit devices must be provided by national agencies to appropriate international bodies, such as Interpol and the World Customs Organization, to facilitate action by relevant agencies in other jurisdictions.

The GSMA has made its device information and device status services available for customs agencies and other industry stakeholders to verify the authenticity of mobile device

Resources:

GSMA IMEI Services: The Global Source of IMEI Data
GSMA Device Check Platform
EUIPO-ITU Report: The Economic Cost of IPR Infringement in the Smartphones Sector
Spot a Fake Phone Website

22: According to figures from OECD, 2017

identities online. National customs agencies are advised to use these services as part of a rigorous set of measures to monitor the importation of mobile devices.

The GSMA encourages operators to deploy systems like Equipment Identity Registers (EIRs) and to connect to GSMA systems like EIR with access to the GSMA Device Database. Using the GSMA global Type Allocation Code (TAC) list of all legitimate device identity number ranges, operators can block devices with invalid IMEIs.

National authorities should study which factors, such as import duties and taxation levels, contribute to local demand for counterfeit devices. The potential of reducing tax levels on devices to narrow the price gap between counterfeit/smuggled and legitimate devices should be carefully considered, as it could make the underground market a less lucrative place to trade.

Implementing national lists of homologated devices can be successful if they are linked to the GSMA TAC list. National import verification systems and national device homologation systems should also be linked to national lists of approved devices. Some implementations propose that customers register their details and devices centrally. The GSMA does not support central customer registrations because they are unnecessary – the subscriber identities associated with each device can be established by operators themselves.

Where national authorities are considering introducing a system to block non-homologated devices, they should consider offering amnesty to consumers who already own non-compliant devices. Blocking huge quantities of devices would not only be a major loss for consumers, but would also have significant social, economic and security impacts. It is recommended that the funding model for such systems should not place a burden on consumers and mobile operators, since they are not the cause of the underlying issue. National systems should also not be applied to roamers who might be denied service without cause.

Debate:

» ***How can governments and other stakeholders best address the issue of counterfeit mobile devices?***

Mobile devices: theft

Background

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

The GSMA has been leading industry initiatives to block stolen mobile devices based on a shared database of the unique identifiers of devices reported lost or stolen. Using the IMEI of mobile devices, the GSMA Device Registry maintains a central list, known as the GSMA Block List, of devices reported lost or stolen by mobile customers. The GSMA Device Registry is available to mobile operators around the world to ensure stolen devices transported to other countries are also denied network access.

The effectiveness of blocking stolen devices on individual network EIRs depends on the secure implementation of the IMEI in all mobile devices. Leading device manufacturers are encouraged to support a range of measures to strengthen IMEI security in accordance with GSMA-defined security requirements.

Industry position

The mobile industry has led numerous initiatives and made great strides in the global fight against mobile device theft.

Although the problem of device theft is not of the industry's creation, the industry is part of the solution. When lost or stolen mobile devices are rendered useless they have significantly reduced value, removing the incentive for thieves to target them.

The GSMA encourages operators to participate in its Device Registry Programme to report and block the IMEIs of devices flagged as stolen on the global Block List. Typically, operators deploy EIRs on their networks to deny connectivity to flagged devices and share identifiers of devices from their own local network's block list to ensure devices stolen from their customers can be blocked on the networks of other participants. These block list solutions have been in place on some networks for many years.

To enable a wider range of stakeholders to combat device crime, the GSMA provides services that allow eligible parties, such as law enforcement, device traders and insurers, to check the status of devices against the GSMA Block List and, in some cases, to also flag stolen devices.

Resources:

GSMA IMEI Services: The Global Source of IMEI Data
GSMA Device Registry
GSMA IMEI Security Technical Design Principles
GSMA Report: IMEI Security Weakness Reporting and Correction Process
GSMA Reference Document: Anti-Theft Device Feature Requirements GSMA Mobile Phone Theft: Consumer Advice

IMEI blocking, when combined with other multistakeholder measures, can be the cornerstone of a highly effective anti-theft campaign.

Consumers that have had their devices stolen are particularly vulnerable to their personal data being used to commit a range of additional crimes. Industry, law enforcement agencies and regulators are recommended to provide anti-theft consumer education material on their websites with advice and measures appropriate to their market.

The concept of a 'kill switch' – a mechanism that disables a stolen phone remotely – has been developed for a range of devices. The GSMA supports device-based anti-theft features and has defined feature requirements for a globally applicable solution. These high-level requirements have set a benchmark for anti-theft functionality while allowing the industry to innovate.

The deployment of persistent endpoint security solutions on mobile devices can also help render devices useless and unattractive to criminals by preventing those devices from working on non-mobile networks such as Wi-Fi where EIR blocking would otherwise be ineffective.

National authorities have a significant role to play in combating criminal activity. It is critical that they engage constructively with the industry to ensure the distribution of mobile devices through unauthorised channels is monitored and that action is taken against those involved in the theft or illegal distribution of stolen devices.

A coherent cross-border information-sharing approach involving all relevant stakeholders makes national measures more effective. The GSMA advocates the sharing of stolen device data internationally for blocking and status-checking purposes, which can be facilitated by the GSMA Device Registry and Device Check services. Only if regulation allows stolen device information to be shared across all countries will this deterrent have a global impact.

In markets with a national homologated list, lost and stolen device information can be exchanged between mobile operators through the GSMA Device Registry. Alternatively, if a national device block list system is already in place, and complies with GSMA requirements, it may be approved to use the GSMA Device Registry to exchange block list information.

Debate:

- ***What can industry do to prevent mobile phone theft?***
- ***What are the policy implications of this rising trend?***

Mobile network and device security

Background

Security attacks can impact all technology, including mobile devices. Mobile operators use encryption technologies to deter criminals from eavesdropping and intercepting traffic.

The barriers to compromising mobile security are high and research into possible vulnerabilities has generally been technically quite complex. While no security technology is guaranteed to be unbreakable, practical attacks on mobile services are rare, as they tend to require considerable resources, including specialised equipment, computer processing power and a high level of technical expertise beyond the capability of most people.

Reports of eavesdropping are not uncommon, but such attacks have not taken place on a wide scale, and LTE and 5G networks are considerably better protected against eavesdropping risks than GSM networks. Moreover, 5G technology boasts a host of new security capabilities that further enhance protection levels.

Industry position

The protection and privacy of customer communications are 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 GSMA leads a range of industry initiatives to make operators aware of the risks and mitigation options available to protect their networks and customers and its work is acknowledged by regulators around the world as being sufficient to eliminate the need to formally regulate.

» The GSMA works with a wide group of experts to facilitate an appropriate response to threats. We play a key role in coordinating the industry response to security vulnerability research through its Coordinated Vulnerability Disclosure (CVD) programme.

» The GSMA's Telecommunication Information Sharing and Analysis Centre (T-ISAC) collects and disseminates information and advice on security incidents within the mobile community in a trusted and anonymised way. The GSMA has also conducted a comprehensive threat

Resources:

GSMA Security Accreditation Scheme Website
GSMA Network Equipment Security Assurance Scheme
GSMA Security Advice for Mobile Device Users Website
GSMA Coordinated Vulnerability Disclosure Website
GSMA T-ISAC Website

analysis involving industry experts from across the ecosystem, regulators as well as public sources such as 3GPP, the European Union Agency for Cybersecurity (ENISA) and the National Institute of Standards and Technology (NIST) and mapped these threats to appropriate and effective security controls. This analysis has been collated into a 5G Cybersecurity Knowledge Base providing useful guidance on a range of 5G security risks and mitigation measures.

» The GSMA's Fraud and Security Group acts as a centre of expertise to drive the industry's management of fraud and security matters. The group seeks to maintain or increase the protection of mobile operator technology and infrastructure, and customer identity, security and privacy, so that the industry's reputation stays strong and mobile operators remain trusted partners in the ecosystem.

» The GSMA's 5G Cybersecurity Knowledge Base makes available the combined knowledge of the 5G ecosystem to increase trust in 5G networks and make the interconnected world as secure as possible.

» The GSMA supports global security standards for emerging services and acknowledges the role that SIM-based secure elements have played in protecting customers and mobile services because the SIM card has proven itself to be resilient to attack. The Embedded Universal Integrated Circuit Card (eUICC) approach used in eSIM solutions that has been defined by the GSMA and has been rolled out by industry inherits the best security properties from the SIM and is designed to build on the protection levels achieved in the past.

» The GSMA constantly monitors the activities of hacker groups, as well as researchers, innovators and a range of industry stakeholders, to improve the security of communications networks. Our ability to learn and adapt can be seen in the security improvements implemented from one generation of mobile technology to the next.

Debate:

» ***How secure are mobile voice and data technologies and what is being done to mitigate the risks?***
» ***Do emerging technologies and services create new opportunities for criminals?***
» ***What will the 5G security landscape look like?***

Number resource misuse and fraud

Background

Many countries have serious concerns about number resource misuse or calls that never reach the destination indicated by the international country code. These calls are instead terminated prematurely, through carrier and/or content provider collusion, to revenue-generating content services without the knowledge of the ITU-T assigned number-range holder.

This abuse puts such calls outside any national regulatory controls on premium-rate and revenue-share call arrangements and is a key contributing factor to International Revenue Share Fraud (IRSF) perpetrated against telephone networks and their customers. Perpetrators of IRSF are motivated to generate incoming traffic to their own services with no intention of paying the originating network for the calls. They then receive payment quickly, long before other parties, within the settlement process. Misuse also affects legitimate telephony traffic, as high-risk number ranges can be blocked as a side effect.

Industry position

Number resource misuse has a significant economic impact on many countries, so multistakeholder collaboration is key.

The telecommunications fraud carried out as a consequence of number resource misuse is one of the topics being addressed by the GSMA Fraud and Security Group, a global conduit for best practice with respect to fraud and security management for mobile operators. The Fraud and Security Group's main focus is to drive industry management of mobile fraud and security matters to protect operators and consumers and safeguard the mobile industry's trusted reputation.

The Fraud and Security Group supports EU guidelines under which national regulators can instruct communications providers to withhold payment to downstream traffic partners in cases of suspected fraud and misuse.

The group believes that national regulators can help communications providers reduce the risk of number resource misuse by enforcing stricter management of national numbering resources. Specifically, regulators can:

» Ensure national numbering plans are easily available, accurate and comprehensive.

» Implement stricter controls over the assignment of national number ranges to applicants and ensure the ranges are used for the purpose for which they have been assigned.

» Implement stricter controls over leasing of number ranges by number-range assignees to third parties.

The Fraud and Security Group shares abused number ranges among its members and with other fraud management industry bodies. It has also worked with leading international transit carriers to reduce the risk of fraud that arises as a result of number resource misuse, and with law enforcement agencies to support criminal investigations in this area.

Resources:

ITU-T Notification of Possible Misuse of E.164 Resources Website

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.
- Use the High-Risk Number List available from the GSMA Fraud Intelligence Service, 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 (BOIC-exHC) function for new or high-risk subscriptions.

Debate:

- ***How can regulators, number-range holders and other industry players collaborate to address this type of misuse and fraud?***

Signal inhibitors (jammers)

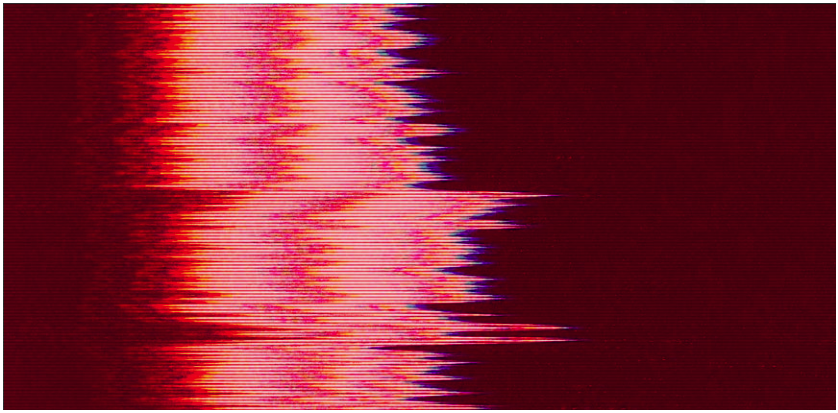
Background

Signal inhibitors, also known as jammers, are devices that generate interference or otherwise intentionally disrupt communications services. In the case of mobile services, they interfere with communication between the mobile terminal and the base station. Their use by private individuals is banned in countries such as Australia, the UK and US.

In some regions, such as Latin America, signal inhibitors are used to prevent the illegal use of mobile phones in specific locations, such as prisons. However, blocking the signal does not address the root cause of the problem: wireless devices illegally ending up in the hands of inmates who then use them for illegal purposes.

Moreover, signal inhibitors do not prevent mobile devices from connecting to Wi-Fi networks because they do not affect the frequency bands used by Wi-Fi routers. As a result, signal inhibitors do not block people from using Over The Top (OTT) voice applications to make calls to phone networks.

Mobile operators provide coverage and capacity by investing heavily in the installation of radio base stations. However, the indiscriminate use of signal inhibitors compromises these investments by causing extensive disruption to the operation of mobile networks, reducing coverage and leading to the deterioration of service for consumers.



Resources:

GSMA Common Position Proposal on Signal Inhibitors (Jammers) in Latin America
GSMA Report: Signal-Blocking Solutions: Use of Jammers in Prisons
GSMA Report: Safety, Privacy and Security Across the Mobile Ecosystem

Industry position

In some Latin American countries, such as Colombia, El Salvador, Guatemala and Honduras, governments are promoting the deployment of signal inhibitors to limit the use of mobile services in prisons. The GSMA and its members are committed to working with governments to use technology to help keep mobile phones out of sensitive areas, and to cooperating on efforts to detect, track and prevent the use of smuggled devices.

It is vital that a long-term, practical solution is found that does not have a negative impact on legitimate users, nor affect the substantial investments that mobile operators have made to improve their coverage.

The nature of radio signals makes it virtually impossible to ensure that the interference generated by inhibitors is confined, for example, within the walls of a building. Consequently, the interference caused by signal inhibitors affects citizens, services and public safety. It restricts network coverage and has a negative effect on the quality of services delivered to mobile users. Inhibitors also cause problems for other critical services that rely on mobile communications. For example, during an emergency they could limit the ability of mobile users to contact emergency services via numbers such as 999, 911 or 112, and they can interfere with the operation of mobile-connected alarms or personal health devices.

The industry's position is that signal inhibitors should only be used as a last resort and only deployed in coordination with operators. This coordination must continue for the total duration of the deployment of the devices, from installation through to deactivation, to ensure that interference is minimised in adjacent areas and legitimate mobile phone users are not affected.

Furthermore, to protect the public interest and safeguard the delivery of mobile services, regulatory authorities should ban the use of signal inhibitors by private entities and establish sanctions for private entities that use or commercialise them without permission from relevant authorities. The import and sale of inhibitors or jammers must be restricted to those considered qualified and authorised to do so and their operation must be authorised by the national telecommunications regulator.

Nevertheless, strengthening security to prevent wireless devices being smuggled into sensitive areas such as prisons is the most effective measure against the illegal use of mobile devices in these areas, as it would not affect the rights of legitimate users of mobile services.

Debate:

- ***Should governments or private organisations be allowed to use signal inhibitors that interfere with the provision of mobile voice and data services to consumers?***
- ***Should the marketing and sale of signal inhibitors to private individuals and organisations be prohibited?***

Appendix

GSMA Intelligence

GSMA Intelligence is an extensive and growing resource for GSMA members, associate members and other organisations interested in understanding the mobile industry. Through industry data collection and aggregation, market research and analysis, GSMA Intelligence provides a valuable view of the mobile industry, and the wider mobile ecosystem, around the globe.

Global coverage

GSMA Intelligence publishes data and insights spanning 240 markets and 900 mobile network operators. Comprising more than 30 million individual data points, GSMA Intelligence combines historical and forecast data from the beginnings of the industry in 1979 with forecasts out to 2030. 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 to more than 7,000 network deployments to date. White papers and reports from across the GSMA and weekly bulletins are also available as part of the service.

Powerful data tools

Information in GSMA Intelligence is made easy to use by a range of data selection tools: multifaceted search, rankings, filters, dashboards, a real-time data and news feed, as well as the ability to export data into Excel and add graphs and charts to presentations.

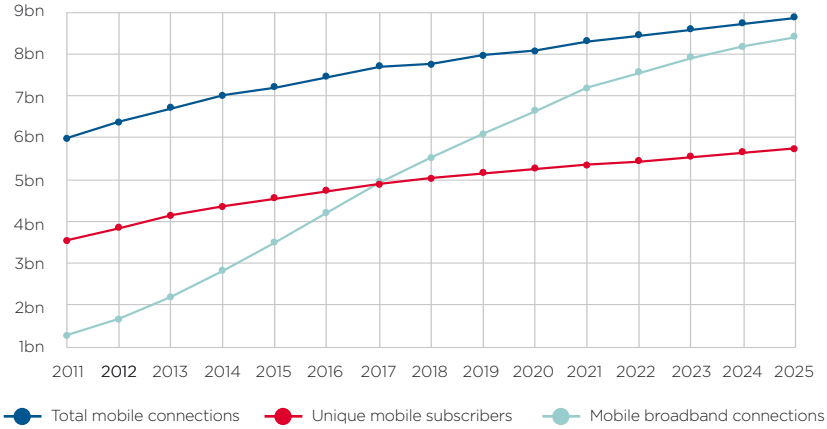
The global unique subscriber base grew by 1.7 per cent in the previous 12 months. This growth is forecast to continue at a similar rate until 2025. Growth is far from uniform around the world and is largely driven by LMICs, which are forecast to add 360 million subscribers over the next six years, compared to only 28 million new additions in high-income markets over the same period.

Unique subscriber penetration rates vary significantly across regions. Europe has the highest penetration rate on average, followed by North America and the Commonwealth of Independent States (CIS). Sub-Saharan Africa had the lowest penetration rate in 2021 at 46 per cent of the population, despite having the fastest subscriber growth of any region over the past decade.

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

Figure 17 **Unique subscriber penetration by region**

Figure 18 **Global connection trends**

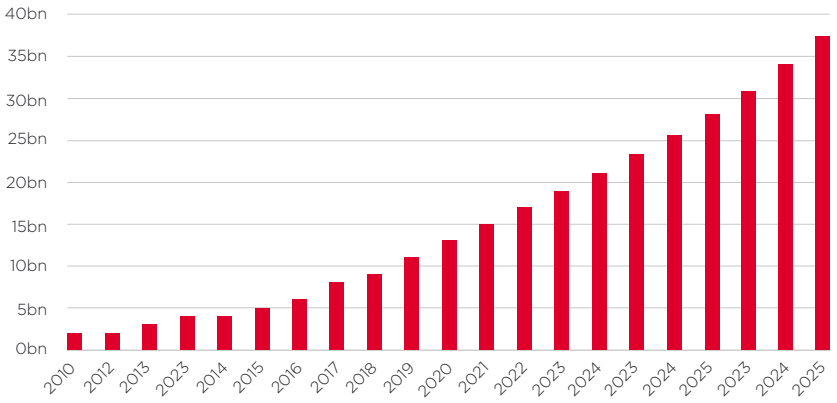


GSMA Intelligence forecasts that between 2022 and 2025, mobile operators will grow annual revenues by 1.1 per cent CAGR to reach $1.14 trillion. Slowing subscriber growth, coupled with declining levels of ARPU, are the main factors driving this trend.

Between 2022 and 2025, mobile operators around the world will spend $745 billion on CapEx, compared to $788 billion over the preceding four years. While 5G is already available across most of the world's largest economies, spending on the technology will continue as operators expand the coverage and capacity of their networks. GSMA Intelligence forecasts that the total number of IoT connections (cellular and non-cellular) globally will reach 23.4 billion in 2025, and rise to 37.5 billion by 2030.

While IoT is rapidly becoming a mainstream technology in consumer markets (for consumer electronics and smart home devices), enterprise IoT will be the largest source of connections growth in the future.

Figure 19 **Total IoT connections, 2010 – 2025**



The Internet of Things defined

GSMA Intelligence defines IoT devices as those capable of two-way data transmission (excluding passive sensors and radio frequency identification, or RFID tags). It includes connections using multiple communication methods, such as cellular and short-range connectivity. It excludes PCs, laptops, tablets, e-readers, data terminals and smartphones.

Most IoT devices, typically in indoor environments, will be connected by unlicensed radio technologies designed for short-range connectivity. These include technologies such as Wi-Fi, Z-Wave and ZigBee. IoT devices that require mobility, lower latency and ultra-reliability will primarily be connected by cellular networks using licensed spectrum. Cellular networks address the need for more secure, managed connectivity, allowing devices to connect directly to the cloud (as opposed to a gateway). Managed connectivity will be one of the key drivers of growth. Licenced LPWA networks enable a slew of IoT devices that require longer battery life and lower data throughputs to be connected. Currently, there are nearly 150 licensed LPWA networks around the world. GSMA Intelligence forecasts that by 2025, licensed cellular networks will serve 4.1 billion IoT connections globally or 17 per cent of all IoT connections.

GSMA
2nd Floor
The Walbrook Building
25 Walbrook
London
EC4N 8AF

Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601