GSMA

Mobile Policy Handbook

An insider's guide to the issues

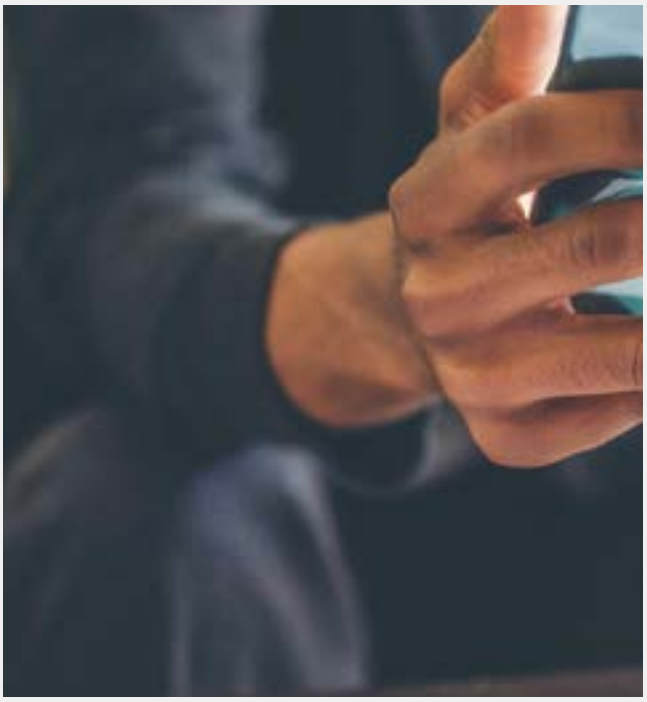
February 2024

GSMA

The GSMA is a global organisation which is 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 **gsma.com.**

Follow the GSMA on X: @**GSMA**



About this handbook

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. Acknowledging the shared goals of attracting digital investment, encouraging innovation and building digital trust, we are committed to helping governments and regulators achieve positive outcomes for the digital economy and society through effective, forward-looking 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 global mobile industry positions under one cover, the handbook is an informative primer, a signpost for good practice and an index of resources for those who want to maximise the value of digital connectivity in their own market.

This ninth edition of the *Mobile Policy Handbook* is intentionally leaner, with renewed focus on the essential topics and the collective view of mobile network operators worldwide. Cover to cover, new positions have been added and long-standing topics have been refreshed with timely background information, up-to-date statistics and more recent resources that help readers go deeper.

Please be aware that the online version of this resource at **gsma.com/publicpolicy/mobilepolicyhandbook** may include more recent updates or additions.

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

Contents

Connecting the world, investing in the future

The global digital revolution has changed the way people everywhere live, work and play. Internet-enabled services and solutions are generating immeasurable benefits and the pace of technological innovation continues to accelerate. Underlying it all is digital connectivity, including mobile telecommunications.

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.

Without the networks that securely and reliably transport ever-increasing volumes of data, the world as we know it would be pure science fiction. In reality, digital connectivity is everywhere. By the end of 2022, more than 5.5 billion people worldwide subscribed to a mobile phone service, with average monthly data consumption surging to 11.3Gb per user and networks supporting 2.5 billion Internet of Things (IoT) connections.[1]

For most people today, digital connectivity is a vital, enabling and entertaining element of daily life. This was never clearer than during the COVID-19 restrictions of 2020–2022. People who were connected could rely on the internet to stay in touch with friends and family, access education and health services and work remotely. It was also a reminder to policymakers that not everyone is connected, whether by choice or circumstance, and that closing the digital divide still matters.

Bringing new digital services to life

5G is a crucial next step for mobile technology because it can handle far greater volumes of data, enable a massive IoT infrastructure and support an array of services that require fast, dependable, low-latency connectivity. To expand and evolve their networks, mobile operators will invest $1.5 trillion in capital between 2023 and 2030, 90% of which will be for 5G.[2]

In 2023, 5G launched in approximately 30 new markets. Many were in Africa and Asia, making 5G a truly global phenomenon. As 5G adoption scales up, operators must realise a return on the investment and mobile operators will increasingly highlight the link between mobile devices, 5G and new digital services while expanding their 5G fixed wireless access (FWA) offerings to new areas.

The 2023 World Radiocommunication Conference (WRC-23) was a critical moment in identifying new, internationally harmonised spectrum bands and enabling countries to confidently assign mobile spectrum to mobile operators for 5G deployments. These investments will enable 5G to proliferate and deliver on the industry's future promise.

Mobile operators are integrating transformative solutions in their networks and adjusting business models to expand services and pursue commercial opportunities. To make service provision more efficient and flexible, they continue to invest in network virtualisation and transition to cloud-based, software-driven network management. To optimise network functions and improve customer care, they are integrating artificial intelligence (AI) tools in many parts of their business. To offer connectivity services more efficiently to developers and cloud providers in an API-driven world, they are building the GSMA Open Gateway.

1 GSMA, *The State of Mobile Internet Connectivity 2023*
2 GSMA, *The Mobile Economy 2023*

Embodying responsible leadership

It is widely accepted that understanding and responding to social, environmental and ethical issues is good for business, and the mobile industry embodies responsible, sustainable business practice and trusted leadership. Mobile operators are actively engaged in a range of initiatives supported by the GSMA, including:

- **Net-zero commitments**. By committing to net-zero targets, mobile operators are taking responsibility for their emissions, including their indirect emissions up and down their value chains.
- **SDGs**. Every year, the GSMA reports on the mobile industry's collective contribution towards achieving the UN Sustainable Development Goals (SDGs) and calls for the policy actions needed to achieve the 2030 Agenda.
- **Closing the digital divide**. As network coverage connects more than 95% of people around the world, mobile operators remain focused on closing the 'usage gap', which refers to the 1.5 billion adults globally who are not connected due to a lack of digital skills, financial resources or locally adapted services, even though mobile broadband service is available where they live.

Good practice in telecoms policy and regulation

None of these efforts can be fully realised without supportive policy and regulatory frameworks. Governments and regulatory authorities create the conditions under which mobile operators can meet growing demand, pursue new innovations, contribute to socio-economic development and achieve environmental sustainability.

The industry positions in this handbook suggest what can be done – and what should not be done – across many policy areas that affect the business of mobile operators and the welfare of consumers. These positions are grouped into four categories:

- **Business environment**, including topics such as market competition, taxation and net neutrality.
- **Spectrum management and licensing**, including spectrum planning, auctions, sharing and more.
- **Consumer protection**, including balanced and proportionate regulation for data privacy, public safety and network security.
- **Environmental sustainability**, including energy efficiency, sustainable supply chains and enhancing the sustainability of other economic sectors through mobile connectivity.

When governments adopt a policy and regulatory framework for mobile telecoms that adheres to established good practice, the entire digital economy becomes stronger, generating better and broader outcomes for businesses and consumers.

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

Resources

The Mobile Economy 2023, GSMA

Mobile Net Zero: State of the Industry on Climate Action 2023, GSMA

2023 Mobile Industry Impact Report: Sustainable Development Goals, GSMA

The State of Mobile Internet Connectivity 2023, GSMA

GSMA Capacity Building programme

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 10,000 regulatory professionals from more than 175 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 that 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, the digital divide and how to leverage mobile technology to achieve SDG targets.

The in-house policy experts who develop and teach the courses have backgrounds in telecoms, 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 and this 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 (UKTA).

Courses are suitable for professionals at any stage of their career. They are available both face-to-face and online, meaning policymakers and regulators have maximum flexibility in how they study. The in-person courses are between one and three days long, while the online courses last between two and five weeks.

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

Courses:

- 5G: The Path to the Next Generation
- Addressing the Digital Divide
- Big Data Analytics and Artificial Intelligence for Impact
- Bridging the Mobile Gender Gap
- Children's Rights and Connectivity
- Climate Change and the Mobile Industry
- Competition Policy in the Digital Age
- Internet of Things
- Leveraging Mobile to Achieve SDG Targets
- Mobile Money for Financial Inclusion
- Personal Data in the Context of Mobile Networks
- Principles of Mobile Privacy and Security
- Radio Signals and Health
- Spectrum Management for Mobile Telecommunications
- The Evolution of Radio Access Networks: Disaggregation, Open RAN and 6G
- The Importance of Sustainability and ESG to the Mobile Industry
- The Role of Mobile in Humanitarian Action

How we deliver our training

On site

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

Online

All GSMA courses are available online, giving students control over their own learning. Through the online platform, students can study from anywhere in the world, progress at their own pace and schedule coursework around work and family life.

Via local partners

The GSMA also delivers courses through a range of strategic partnerships with academic institutions, development organisations, regulatory bodies and training specialists. This gives us the flexibility to deliver courses at a location near you.

01 Business environment

Mobile operators provide 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 the emergence of internet platforms and services.

In most countries, however, mobile operators are still subject to rules and obligations that 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.

Resetting policy and regulation to drive the digital economy

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. By updating the regulatory framework, policymakers can ensure that government and industry are aligned and working to foster an inclusive digital society for all.

Figure 1 identifies four areas of policy action related to network investment, regulation, promoting the digital economy and demonstrating digital leadership.[3]

3 GSMA (2017), *Embracing the Digital Revolution: Policies for Building the Digital Economy*

Business environment

The evolution of spectrum

Consumer protection

Environmental sustainability

Figure 1: Policy levers to promote an inclusive digital economy[4]

Encourage network investment

Implement a broadband policy with clear goals

Support infrastructure deployment

Focus on spectrum allocation and use, not auction revenues

Modernise regulation

Adopt functionality-based, technology-neutral regulation

Favour ex-post approaches over ex-ante prescriptive regulation

Apply regulations consistently across the digital ecosystem

Promote 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

4 Ibid

The following pages cover a range of policy topics affecting mobile operators, laying out key points of debate and formally agreed industry positions.
As the mobile industry deploys 5G more extensively in the coming years, the need for pro-investment policies and modern regulatory regimes has never been greater.

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.

These networks have been made possible by technological advances that have reduced barriers to network deployment and management and that have 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 spectra, 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 geographical, commercial and logistical connectivity challenges that can often be unique, 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?

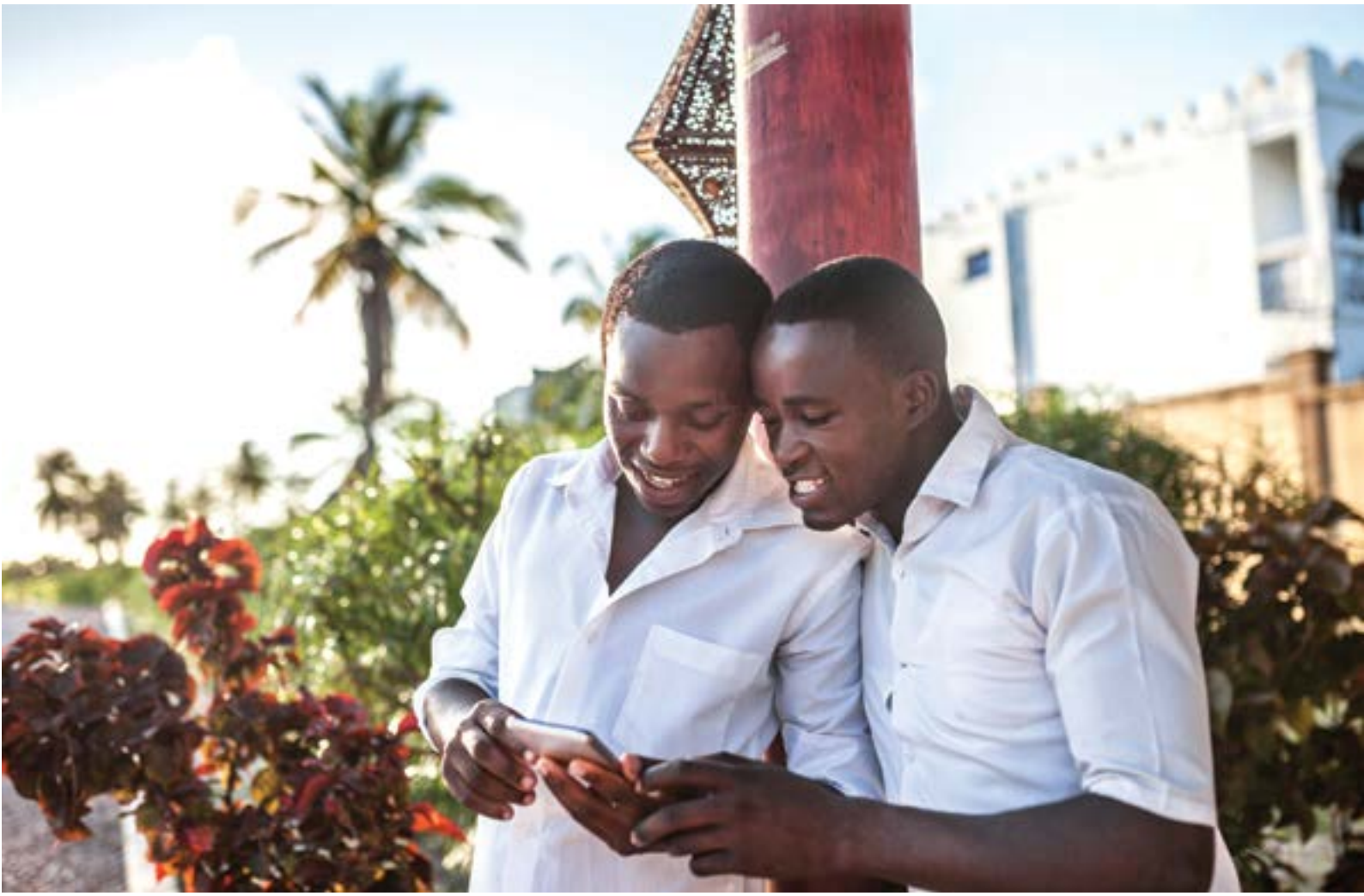
How should community networks be supported and regulated to ensure high-quality, local connectivity while maintaining a level playing field with mobile operators?

Industry position

Community networks can complement the efforts of mobile operators to expand coverage because they are an opportunity to deliver the transformative benefits of connectivity to locations that are not commercially viable. By doing so, they can drive the use of information and communication technology (ICT), 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 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 spectra 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 rollouts and worse performance.

Resources

Wireless Networking in the Developing World, The WNDW Project, February 2013

Competition

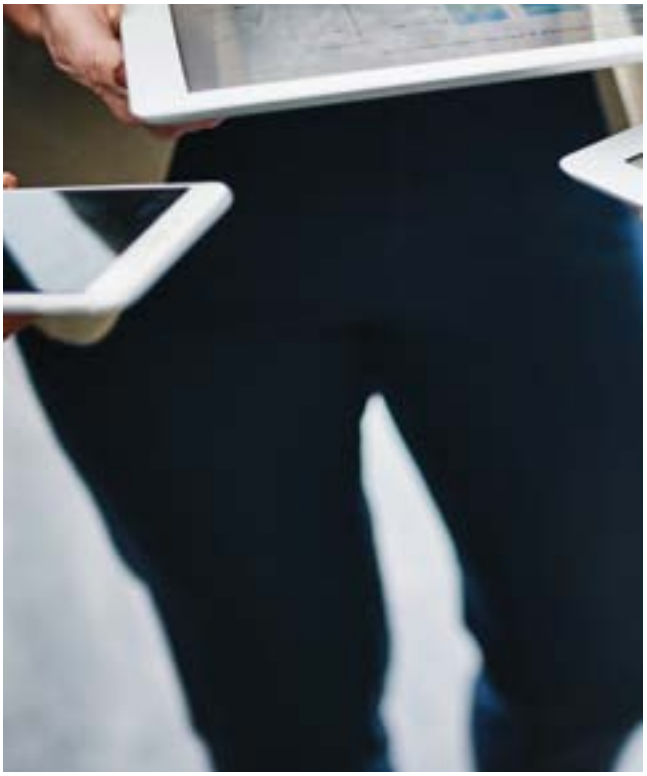
Background

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 digital economy and explosive growth in smartphone adoption have brought innovation and disruption to traditional mobile communications services. These changes have also had an impact on existing policy frameworks and challenged competition policy.

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, so far, 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?

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-related ones.

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, those 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 can also be improved and updated to tackle the issues arising in digital markets more effectively, as some authorities around the world are demonstrating.

Resources

GSMA Competition Policy website

The Data Value Chain, GSMA, June 2018

Competition Policy in the Digital Age, GSMA, October 2015

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 and businesses with improved offerings. For example, while many operators continue to invest in their 4G networks, they are also investing in 5G network deployments.

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 – and mobile data in particular – has grown steadily, with most users getting far 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 the 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.

Debate

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

Industry position

When assessing mobile mergers, policymakers should consider the full range of benefits of mergers, including price effects, innovation, investments and the use of spectrum over the short and long 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 to 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, whether 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 mobile operators could, in some cases, deter investment and lead to the underuse or misuse of resources.

Resources

Competition Dynamics in Mobile Markets in Europe, GSMA, November 2022

Assessing the Impact of Market Structure on Innovation and Quality in Central America, GSMA, May 2018

Assessing the Impact of Mobile Consolidation on Innovation and Quality: An Evaluation of the Hutchison/Orange Merger in Austria, GSMA, July 2017

Assessing the Case for In-country Mobile Consolidation in Emerging Markets, GSMA, February 2015

Global title leasing

Background

A global title (GT) is an address used for routing signalling messages on telecommunications networks. National authorities allocate numbering resources to communications providers, which reserve and use part of those numbers for use as GTs. In mobile networks, GTs enable information to be exchanged within and between networks so that mobile services work regardless of whether users are in their home network or roaming.

The practice of leasing GTs (by a 'GT lessor' to a 'GT lessee') has enabled additional entities (GT lessees) to gain access to the global SS7 network and to exchange signalling messages using GTs associated with the GT lessor. This reduces routing transparency and accountability, disguising the activities of GT lessees and making it difficult for mobile operators to know who sent the signalling traffic entering their networks. The lack of transparency and absence of controls and oversight associated with GT leasing is of concern to mobile operators and their customers due to the risks it introduces, which can include traffic interception, location tracking and fraud.

Debate

How can regulators ensure that recipients of national numbering resources use them in ways that do not introduce security or fraud risks to other networks or their customers?

How can legitimate and innovative mobile services be supported without continued use of GT leasing?

Industry position

GT leasing has evolved through the emergence of commercial relationships built up over time without any industry standardisation, specifications or recommendations. As a result, there is no agreed framework governing the relationships between GT lessors and the networks to which they are interconnected. Not all parties engaged in GT leasing have considered the impact of GT leasing on the networks receiving the traffic or the subscribers of those networks.

In response to these shortcomings, GSMA members have developed a GT leasing reference document (FS.52) that describes GT leasing motivations, benefits, issues and concerns. The document also contains a code of conduct containing requirements and guidelines intended to minimise the risks associated with GT leasing.

GT lessors and transit carriers involved in GT leasing arrangements are being invited to voluntarily declare to their partners that they adhere to the GT Leasing Code of Conduct as evidence of their commitment to routing transparency and to reduce the risks for mobile operators and their customers. Operators and carriers that do not lease GTs are also being encouraged to publicly declare their support for the Code of Conduct and request compliance from their suppliers and partners.

Resources

GSMA Global Title Leasing Code of Conduct, GSMA, 2023

Mobile Privacy Principles, GSMA, February 2016

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 antennae, avoiding unnecessary duplication. It 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 mobile operators based on their commercial needs.

Debate

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

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

Industry position

Governments should have a regulatory framework that allows voluntary 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 that are necessary to allow them to compete on quality of service and coverage.

Infrastructure-sharing agreements should be governed by commercial law and, as such, be 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

Unlocking Rural Coverage: Enablers for Commercially Sustainable Mobile Network Expansion, GSMA, July 2016

Intellectual property rights: patents

Background

The mobile ecosystem has been a major driver of economic progress and welfare. Countries around the world continue to benefit from improvements in productivity and efficiency brought about by the uptake of mobile products and services.[5]

Without the immense efforts of the mobile industry, many of the adopted technologies in 2G, 3G, 4G and beyond 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. The public has become heavily reliant on mobile telecommunications technology and the ability of mobile operators to deliver such services.

However, in the past few years, there have been radical changes in the licensing of telecommunications technology (the prime use of patent portfolios in telecommunications). Initially, patents were used to preserve a company's 'freedom to operate' (the ability to bring 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?

5 GSMA (2023), *The Mobile Economy 2023*

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 purchase patents (rather than developing and licensing technology) to be asserted against manufacturers and mobile operators already using the technology.

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

- The complexity of mobile operator networks
- The scale of investments needed to build them
- The level of revenues they generate
- 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 minor, will have a severe negative effect on people's lives.
- The importance of maintaining the integrity of mobile telecommunications services and ensuring continuous investment and adoption of new technologies in the telecommunications market.
- 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).

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 mobile operator enjoying significant market power, regulators have developed various regulations and the most notable is 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 a productive and appropriate activity for regulators?

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

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

Industry position

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

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. Therefore, extraterritorial intervention is not appropriate.

Resources

The Impact of Recent Cuts in Mobile Termination Rates Across Europe, Frontier Economics for Vodafone Group, May 2012

The Setting of Mobile Termination Rates: Best Practice in Cost Modelling, GSMA, October 2008

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 mobile 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 and the number and mix of subscribers is constantly changing, 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 puts equal demand on a network. For example, voice traffic is time-sensitive and 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.

Debate

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

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

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

Industry position

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 how operators handle 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.

Resources
GSMA Net Neutrality website

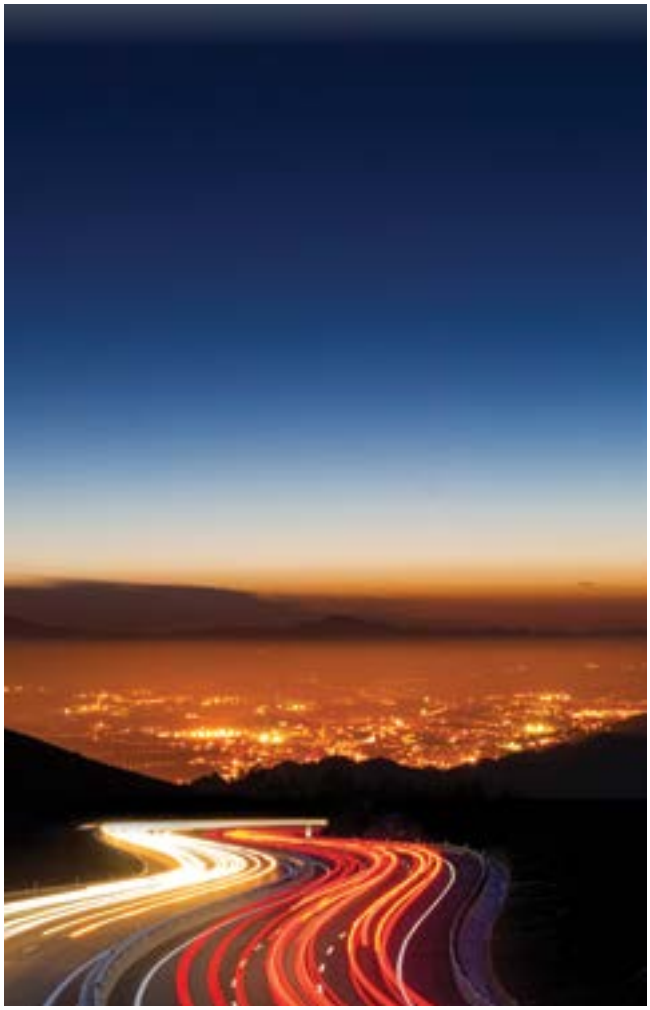
Passive infrastructure providers

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 mobile 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 and particularly so in relation to independent tower companies.



Debate

What benefits do independent tower companies offer to mobile operators?

Should passive infrastructure sharing ever be mandated by a regulatory authority?

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

Industry position

Licensed mobile operators should be able to share passive infrastructure with other licensed mobile 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 the mobile industry to expand coverage cost-effectively and rapidly while retaining competitive incentives. Regulation of passive infrastructure-sharing should be permissive but 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 that applies 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 (for example, 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 mobile 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 the construction of 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.

Resources

Infrastructure Sharing: An Overview, GSMA, June 2019

Public-private partnerships

Background

A public-private partnership (PPP) is a legal arrangement between two or more private-sector 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 would otherwise be risky investments with limited commercial potential. Governments view PPPs as a way to drive investment in areas without coverage 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.[6]

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
- Last mile: radio access networks and wired local loops

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?

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[7] or provide the infrastructure to deploy commercially viable networks.[8]

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[9] because 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.

6 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 24 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.*
7 '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.*
8 The ACE submarine cable is a good example of infrastructure that has enabled faster and cheaper internet connectivity across 24 countries in Africa.
9 European Commission (2023), *Guidelines on State Aid for Broadband Networks*

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.[10] As a second step, governments should consider giving mobile operators the same preferential conditions that 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 (SWN) 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).

Resources
Guidelines on State Aid for Broadband Networks, European Commission, 2023

10 GSMA (2016), *Unlocking Rural Coverage: Enablers for Commercially Sustainable*

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 because these normal fluctuations result in customers experiencing different levels of service quality.

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 users. Mobile throughput can vary dramatically over time, and throughput is not the only product attribute that influences consumer choice.

Debate

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

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

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

Industry position

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

The quality of service that mobile consumers experience depends on many factors and some of these are beyond the control of mobile 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 because 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 service quality, they should engage in dialogue with the industry to find solutions that strike the right balance of transparency and quality of service.

Resources

The Quality of Mobile Services in Latin America, GSMA, February 2015

Single wholesale networks

Background

Single wholesale networks (SWNs), also known as single-distributor, government-initiated monopolies or wholesale open access networks (WOANs), were implemented by some countries in the mid- to late-2010s. Considered by policymakers as an alternative to competitive mobile networks for the delivery of mobile broadband services in 4G or 5G, SWNs have become less popular.

Supporters of SWNs argued that they addressed certain concerns better than traditional network competition. These concerns generally included lack of coverage or inadequate competition in rural areas, inefficient use of radio spectrum or fears that the private sector lacked incentives to maximise coverage or investment. However, SWNs have proven to be unsuccessful in solving any of these problems and have largely been abandoned for competition-based approaches.

Government-initiated network monopolies require mobile operators and others to rely on wholesale services from the SWN as they serve and compete for retail customers. While there are variations in the SWN proposals discussed and implemented by different governments, mobile operators are limited to providing broadband in one technology (4G or 5G) solely via the SWN in most cases.

Debate

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

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

Industry position

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

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 mobile 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, 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 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.

Resources

Policy Trends in the Aftermath of Single Wholesale Networks, GSMA, 2023

Assessing the Case for Single Wholesale Networks in Mobile Communications, Frontier Economics for the GSMA, September 2014

Taxation

Background

Mobile telecommunications have a positive impact on economic and social development, creating jobs, increasing productivity and improving the lives of citizens. Despite these beneficial outcomes, many countries impose mobile-specific taxes on consumers and operators. These include special communication taxes, such as excise duties on mobile handsets and airtime usage, and revenue-share levies on mobile operators. Some countries have applied a surcharge on international inbound call termination (SIIT), which can increase international call prices and effectively act as a tax on citizens of other countries. These taxes have placed a disproportionate tax burden on the mobile sector, which can prevent countries from reaping the full benefits of mobile technology.

Debate

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

Industry position

Governments should reduce or remove mobile-specific taxes because the social impact and 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.
- Dynamic incentives for operators should not be affected – taxation should not disincentivise efficient investment or competition in the 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 spillovers 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 to consumer adoption and use of mobile broadband. Lowering the tax burden on the sector increases mobile uptake and use, creating a multiplier effect across the wider economy.

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

Resources

GSMA Mobile Taxation Research and Resources

Mobile Tax Policy and Digital Development: A Study of Markets in Sub-Saharan Africa, GSMA, October 2023

Rethinking Mobile Taxation to Improve Connectivity, GSMA, February 2019

Universal service funds

Background

A policy goal of many governments, universal service refers to telecommunications service that is available, accessible and affordable for everyone.

Several countries have established universal service funds (USFs) to extend coverage to 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.[11] Studies by the GSMA and the International Telecommunication Union (ITU) show that disbursement rates remain very low around the world and many funds have been unable to distribute any of the levies collected.

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

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 employ to enable the private sector to expand connectivity?

How relevant are USFs in mature markets?

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 expanding mobile connectivity. Importantly, governments can help by removing sector-specific taxes, stimulating demand and developing infrastructure.

Mobile Network Expansion

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 mobile industry, should be competitive and technology-neutral, and should target projects with the greatest possible impact. USFs should have:

- 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.
- An independent fund structure to avoid political interference.
- Effective administration that avoids 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.
- Regular consultation with mobile operators to ensure investments in coverage are targeted efficiently, include operational expenditure subsidies where necessary and avoid duplication of infrastructure.

If USFs cannot be managed efficiently within a reasonable time frame, a plan should be implemented to phase them out.

Resources

Survey of Universal Service Funds, Key Findings, Ladcomm Corporation for the GSMA, April 2013

The Impact of Universal Service Funds on Fixed-Broadband Deployment and Internet Adoption in Asia and the Pacific, UN ESCAP, 2016

02 The evolution of spectrum

Effective spectrum policies are necessary to encourage the investment required to meet increased demand for data services and enhance the quality and range of services offered. On a larger scale, these policies promote socio-economic benefits, address the digital divide and help reduce carbon emissions in all parts of the world.

To maximise this impact, long-term planning and short-term action are required in several areas. This includes licensing enough spectrum resources through planning and roadmap development, avoiding fragmentation and, importantly, guaranteeing technology neutrality in spectrum assignments.

Spectrum pricing also has a significant impact. Governments seeking to maximise state revenues from spectrum 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 and Vision 2030

Background

Mobile networks 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 that 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.

5G supports significantly faster mobile broadband speeds and heavier data usage than previous generations of mobile technology, while also enabling the full potential of IoT. From connected cars and smart cities to the industrial internet and fibre-like fixed wireless access (FWA), 5G allows more devices to access more data than ever before. The efficiency of 5G is essential to preserving today's most popular mobile applications, such as on-demand video, in an environment of high-user demand.

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

- **Enhanced mobile broadband**, including peak download speeds of at least 20Gbps and a reliable 100Mbps user experience data rate in dense urban areas.
- **Ultra-reliable and low latency communications**, including 1ms latency and very high availability, reliability and security to support services such as virtual reality (VR) and connected vehicles.
- **Massive machine-type communications**, including the ability to support at least one million IoT connections per square kilometre with long battery life and extensive wide area coverage.
- **Fixed wireless access**, including the ability to offer fibre-like speeds to homes and businesses in rural and urban areas — in developed and developing markets.

The speed and availability of 5G services depend on mobile operators having access to spectrum in low, mid- and high bands to build cost-effective networks. Robust licensing and timely availability of spectrum is also vital to the success of 5G deployment. With these in place, 5G can transform digital economies across the globe, help close the broadband usage gap and support digital inclusion. 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.

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

Debate

The GSMA recognises that an average total of 2 GHz of mid-band spectrum needs to be made available to licensed mobile. How can regulators meet the spectrum demand for 5G capacity and which harmonised bands can be used?

Industry position

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

As data traffic continues to increase, more users switch to 5G for mobile and FWA and new, innovative use cases take off, more spectrum across low, mid- and high bands will be needed.

On average, 2 GHz of mid-band spectrum per country will be needed between 2025 and 2030. Mid-band spectrum has been the main driver of 5G launches so far and is expected to help realise most of the socio-economic benefits of 5G in the next decade. Meeting spectrum needs in this range is vital to the future of 5G and requires policymakers to formulate a clear spectrum roadmap.

An average of 5 GHz of high-band spectrum will be needed per market by 2030. It complements low- and mid-band spectrum implementations in dense urban areas and provides fibre-like connectivity through FWA. It also helps ensure secure, reliable and low-latency networks in manufacturing plants or high-density locations, such as sports and music venues and travel hubs.

Low-band spectrum needs for 5G are greater than the actual capacity available below 1 GHz. Expanding spectrum in this range as far as possible is vital to giving rural communities equitable access to mobile services available in urban areas meeting digital inclusion goals. Current proposals in the 600 MHz band will allow for between 2x35 and 2x40 MHz of additional low-band capacity. Expanding low-band spectrum by this amount can improve rural download speeds by 30 to 50 per cent.

Resources

Vision 2030: Low-Band Spectrum for 5G, GSMA, June 2022

Vision 2030: mmWave Spectrum Needs, GSMA, June 2022

5G Spectrum Public Policy Position, GSMA, June 2022

Vision 2030: Insights for Mid-Band Spectrum Needs, GSMA, July 2021

5G Spectrum Guide – Everything You Need to Know

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 due to economies of scale
- A wider range of devices supported by a larger international market
- Roaming or the ability to use a mobile device abroad
- Fewer cross-border interference issues

Efforts to harmonise bands for mobile have taken different forms.

First steps towards the harmonisation of any band happens at a World Radiocommunication Conference (WRC). Mobile allocation for a particular frequency band, and additional International Mobile Telecommunications (IMT) identification, have always been sought at WRCs to harmonise mobile use.

The WRC process is still a useful way to support harmonisation. At WRC-15, for example, agreement was reached on three 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. At WRC-23, further harmonisation of the 3.5 GHz range occurred while the 6 GHz band was harmonised for the first time.

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 at 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 WRC-23 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 are charting their own path, making inter-regional harmonisation and industry guidance on spectrum use vital to the spectrum development process.

Debate

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

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 on which bands are best used, as equipment will only be developed in bands used by early-adopter nations. However, WRC-23 did manage a long-term view on some spectrum with the identification of the 6 GHz for mobile use.

At 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 useable, with costly consequences for consumers.

Resources

The GSMA at WRC-23

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 significantly 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 terms and the assignment of new bands for mobile broadband services.

Providing for flexible spectrum use by limiting licence conditions enables spectrum to be redeployed as technology and market conditions change, bringing down the cost-of-service provision. However, spectrum licences have sometimes contained terms and conditions that go beyond those necessary to guarantee co-existence among users.

Debate

Spectrum licensing is at the heart of mobile services. What measures can policymakers implement to guarantee long-term investment and certainty?

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.

Access to spectrum is essential for the supply of mobile services. The way spectrum is assigned and managed has an impact on competition.

Recommendations for licence terms and conditions:

- Authorities should limit conditions on the use of spectrum to those necessary to guarantee co-existence.
- Spectrum licences should be technology- and service-neutral.
- Governments with particular policy objectives should consider regulation that supports the commercial provision of widespread and affordable access before imposing conditions.
- When conditions are imposed, any related costs should be deducted from spectrum costs.
- Mobile licences should have a minimum 20-year term to provide sufficient certainty to support mobile network investment, which has long payback periods, as well as presumption of renewal.

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, February 2022

Approaches to assigning spectrum

Background
Licensed spectrum is necessary for mobile services to provide quality service and customer value. This, in turn, facilitates the investments needed to deploy mobile networks widely.

The licensing of spectrum bands for mobile services supports international harmonisation, which delivers lower-cost devices and equipment through economies of scale. Dynamic spectrum access techniques enable specific spectrum bands to be shared between multiple uses by avoiding signals being transmitted at the same time. However, exclusive licensing has been central to the success of mobile and any spectrum sharing mechanisms should be considered as a complementary possibility.

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 planned carefully. 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 multi-round 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, combinatorial 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
- Adequate market competition
- 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. Seeking to maximise auction revenues can have significant costs for society, especially the digital economy, if competition 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.

Administrative assignments

Administrative assignments are most effective when market demand is lower. Like spectrum auctions, 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 vague and subjective criteria, or a lack of transparency, increases the risk of favouritism and corruption as well as the potential for the outcome to be challenged in the courts. A trade-off may be needed between policy objectives and the licence fee. Even where the objective is clear, estimating the appropriate price can be challenging.

Regulatory objectives that may be considered part of an administrative assignment 'beauty contest' include coverage, service quality and a variety of social and economic goals.

A challenge with administrative assignments is the risk that successful applicants will be unable to fulfil their offers, particularly if market or technology forecasts prove inaccurate. Licensing authorities should set out the penalties that will be imposed if commitments are not met in advance.

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 approach to use?

Industry position

Efficient spectrum assignments are necessary to realise the full economic and societal value of mobile.

Auctions are the main approach to assigning the right to use a particular spectrum band, but administrative assignments (e.g. beauty contests) can also be used where demand is expected to be lower than the supply of spectrum. Sometimes, a hybrid approach is used whereby the licensing authority initially selects a shortlist of bidders based on administrative criteria and then holds an auction to assign the licence among the shortlisted candidates.

There is no single best way to assign spectrum. Instead, the merits of each approach should be assessed on a case-by-case basis. Auctions remain the most common approach globally. They work best when there is excess demand for spectrum and they help to select the mobile operators most likely to put their spectrum assignment to best use for the benefit of society. Administrative assignments, on the other hand, may be suitable in areas where there is less demand for spectrum and may allow authorities to compare the range of policy objectives offered by candidates.

Whatever approach is chosen, it must be implemented with care. This includes identifying issues through public consultation and weighing the trade-offs of different 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.

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, February 2022

Auction Best Practice, GSMA, September 2021

Spectrum licence renewal

Background

Managing spectrum renewals effectively is a vital part of any country's spectrum management strategy. Uncertainty over future rights to use the spectrum may lead to mobile operators ceasing investment in developing their networks and competing less to grow their customer base until the uncertainty is resolved. Regulators serve consumers best by creating a transparent, predictable and coherent approach to spectrum licence renewal.

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, in addition to investment in new services, can potentially affect mobile services for millions of consumers.

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?

Industry position

The right approach to licence renewals is an important part of a successful spectrum management strategy. Authorities should aim to minimise uncertainty by creating a presumption of renewal unless there has been a breach of licence conditions, a fundamental reallocation of spectrum to a new service is required, or an overriding policy need arises.

Recommendations for 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 market context. Auctions tend to be the most common approach.
- When choosing the assignment approach, licensing authorities should prioritise the objectives of promoting efficient use of spectrum 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 focused on future certainty.
- A decision not to automatically renew a spectrum licence should only be made under certain circumstances, such as for a serious breach of conditions or if spectrum is left idle.
- Licensing authorities should work in close partnership with stakeholders to enable a timely, fair and successful licensing process.

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, February 2022

Spectrum sharing, leasing and trading

Background

Ever-increasing data traffic means mobile services must have access to ever-increasing spectrum to meet demand. Since it has become increasingly difficult to clear new frequency bands for future mobile use, better spectrum management is needed instead to both improve the efficiency of spectrum use and ensure viable use in less economically viable areas.

At the same time, there is a growing appetite 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.

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?

Industry position

Allowing spectrum to be shared, leased or traded among mobile operators can ensure spectrum continues to be used efficiently over time. It encourages efficiency by allowing spectrum rights to be transferred to those who will make better use of them.

By helping to reduce the spectrum shortages some mobile operators face while also ensuring valuable spectrum does not lie fallow, spectrum sharing supports more intensive spectrum use, higher service quality, and lower service provision costs.

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

Voluntary leasing and trading also reduce risks for mobile operators, who can sell or lease unused spectrum while acquiring new capacity as they grow. The ability to trade and lease licences can ensure that spectrum is used efficiently without any need for government-imposed charges.

Recommendations for spectrum sharing, leasing and trading:

- Licensing authorities should allow voluntary spectrum sharing, leasing and trading among mobile operators and facilitate such mechanisms through clearly defined spectrum rights, long licence terms and limited administrative costs.
- In advance of a formal spectrum secondary market framework being 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, facilitate sharing, leasing and trading.
- Competition issues should be assessed based on sharing, leasing and trading agreements. Certain safe harbours can be established where the spectrum represents a small share of market capacity or where a market share is below a certain threshold.

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, February 2022

Technology neutrality

Background

Technology-neutral spectrum licensing is widely recognised as best practice when assigning spectrum to mobile operators. It enables operators to refarm spectrum used for GSM (2G) or 3G to 4G and 5G at a pace driven by market demand. This allows spectrum to be used more efficiently, which should always be the overarching goal of spectrum management for all regulators and governments. It also maximises the technical efficiency. As a result, users benefit from better mobile broadband coverage, higher data speeds and lower mobile data prices than they would otherwise.

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?

Industry position

To get technology neutrality right, there are a few things to keep in mind:

- Attempts to extract additional revenue have misfired and held back the introduction of new mobile technologies.
- While a renewal process provides an opportunity to reissue spectrum licences as neutral, regulators should not delay the introduction while waiting for existing licences to expire.
- When assigning new spectrum, regulators should do so in a technology-neutral manner or, at the very least, not restrict the introduction of next-generation technologies, such as 5G.

The decision to allow, and actively support, technology neutrality is being made easier by technological advancements. For example, the options for managing refarmed bands have improved by leaps and bounds.

The most important development is the ability to ‘gracefully refarm’ bands so they are used simultaneously for several technologies, including 4G and 5G. This allows newer technologies to be introduced in line with growing mobile broadband demand while also supporting legacy users. For regulators, this means they no longer need to worry that refarming will leave legacy users unserved.

Resources

Technology-Neutral Spectrum and Legacy Network Sunsets, December 2023

Spectrum pricing

Background

The primary goal of charging a fee for spectrum is to award spectrum to those who will use it most efficiently to deliver maximum benefits for society. In this way, a well-designed auction will assign spectrum to those who value it most, providing an incentive for them to use it efficiently through investment in widespread, high-quality mobile networks. However, charging for spectrum can also provide substantial state revenues and lead governments to artificially inflate spectrum prices at the expense of efficient spectrum use and the wider economy.

Extremely high-priced auctions are typically the result of national policy decisions, such as setting excessive reserve prices, making an insufficient amount of spectrum available for auction and a lack of clarity on future releases or the renewal process for expiring licences. Such factors can create uncertainty or artificial scarcity of spectrum and encourage mobile operators to bid above their true valuation of the licences on offer.

Debate

More and more telecoms 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 relevant levels of government?

Industry position

Spectrum is a valuable asset, but a long-term vision is needed to maximise this 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.

Recommendations for spectrum pricing and fees:

- Spectrum prices should promote, and not undermine, the optimal use of spectrum for the benefit of society.
- High spectrum fees reduce the funds available for investment and will negatively impact the quality, speed and reach of mobile broadband services.
- Licensing authorities should set auction reserve prices conservatively to allow the market to determine a fair price and to reduce the risk of leaving spectrum unassigned.
- Authorities should be particularly careful not to set renewal fees that remove returns on earlier investments. Renewal fees should only recoup administrative costs.
- Costs related to conditions or obligations attached to the licence should be deducted from spectrum fees.

Resources

Spectrum Pricing Helps Boost Mobile Services, November 2022

Spectrum for industries

Background

The development of new mobile technologies alongside the cloud, big data and machine learning are transforming the connectivity requirements of private mobile networks, also referred to as 'networks for vertical industries'. These range from creating smart utility grids and automating manufacturing to delivering goods by drones and supporting advanced public safety and transport networks. Connected enterprises need to be agile and open to the challenges and opportunities of this era of digitalisation that 5G is delivering.

Policymakers play a vital role by managing the spectrum that underpins these developments, and great care needs to be taken to ensure private mobile network requirements are fully supported without harming other wireless users. Private networks are an integral part of 5G, enabling industrial applications, logistics hubs, local campus networks and many more functions. However, private networks do not imply private spectrum. Asymmetric carve-outs are an aggressive regulatory tool that has an economic cost and, with best-practice licensing, can be avoided.

Debate

As governments turn their attention to supporting high-speed network rollouts, 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?

Industry position

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

Spectrum set-asides can lead to insufficient spectrum being available for mobile operators to use and meet all their 5G requirements and capabilities. Scarcity also encourages higher prices to be paid for spectrum, which is strongly linked to less network investment, slower rollouts, 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 following considerations should inform spectrum policy decisions related to private networks:

- Commercial mobile operators support the needs of a wide variety of private mobile networks and have added capabilities with 5G.
- Spectrum leasing or, when carefully planned, other types of spectrum sharing can be viable options for supporting industry 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 rollouts, worse performance and reduced coverage.
- Policymakers should consider the coexistence challenges when different use cases need to be supported in the same mobile band.

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, February 2022

Spectrum Policy Trends 2023, GSMA, February 2023

03 Consumer protection

As mobile services have become more economically and socially important, particularly 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 reduce 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 multistakeholder fora
- Educating consumers and businesses in the safe use of mobile technologies and applications
- Commissioning research that offers real-world insight and evidence

The following pages 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.

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 their 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
- Opportunities to play and be creative

Increasingly, mobile devices are playing a role in formal education and informal learning. For people in low- and middle-income countries (LMICs) and rural areas, as well as areas where certain groups – 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 to benefit from mobile technologies safely and securely.

The mobile industry has taken active steps to support the safe and responsible use of mobile services by children. The GSMA plays a leading role in voluntary industry initiatives, including education and awareness.

Debate

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

How can all stakeholders navigate the tensions between different child rights in the digital world?

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, its mobile operator members and a range of other organisations, including 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 the ITU's Child Online Protection programme, and actively engages with governments and regulators seeking 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 because they represent the first generation to have grown up in a connected, always-on world. They are also future consumers and innovators who will deliver the next wave of innovation in mobile.

Resources

Guidelines for Industry on Online Child Protection, UNICEF, 2020

Tools for Companies in the ICT Sector, UNICEF

Enhancing Children's Lives Through Mobile, GSMA, 2019

Internet Safety Guides, GSMA and Child Helpline International, 2017

Research Results, Global Kids Online

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.[12]

Cross-border flows of personal data are currently regulated by several international, regional and national instruments and laws that are 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 the Asia-Pacific Economic Cooperation (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 increasingly implementing data localisation rules (also known as 'data sovereignty') that impose local storage requirements or use of local technology.[13] Such localisation requirements can be found in a variety of sector- and subject-specific rules. The restrictive measures are sometimes imposed by countries based on the belief that supervisory authorities can more easily control and scrutinise data that is stored locally.[14] This can be counterproductive from a data security perspective if the storage of data runs the risk of creating 'honey pots' where data stored in a single place with no backup can attract cyberattacks.

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 of frameworks and fora include the Global Cross Border Data Rules (CBPR) Forum, 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 (BCR).

11 UN ESCAP (2017), *The Impact of Universal Service Funds on Fixed-Broadband Deployment and Internet Adoption in Asia and the Pacific*
12 International Chamber of Commerce (2016), *Trade in the Digital Economy: A Primer on Global Data Flows for Policymakers*; ECIPE (2014), *The Cost of Data Localisation: A Friendly Fire on Economic Recovery*
13 Chander, A. and Le, U. (2015), 'Data Nationalism', *Emory Law Journal*, 64(3); Hill, J.F. (2014), 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders', The Hague Institute for Global Justice, Conference on the Future of Cyber Governance

Debate

How can industry, legislators, regulators and civil society engage effectively to develop policy that supports cross-border flows of data?

How can data protection safeguards adequately address the legitimate concerns of governments that seek to impose localisation requirements?

Industry position

Cross-border data flows 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 that 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 CBPR and the EU BCR, 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 the convergence of different approaches to privacy while also promoting appropriate standards of data protection and allowing accountable companies to build scalable and consistent data privacy programmes.

Requirements for companies to use local data storage or technology create unnecessary duplication and 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.

Resources

Promoting Transparency, Choice and Trust in the Digital Society, GSMA privacy website

Cross Border Data Flows: The Impact of Data Localisation on IoT, GSMA, January 2021

Mobile Privacy Principles, GSMA, February 2016

Smart Data Privacy Laws, GSMA, June 2019

Cybersecurity

Background

The internet and mobile connectivity have become ever more pervasive, making it vital to ensure that people can use increasingly essential services reliably, 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 also incorporating new features and enhancing existing security capabilities to minimise the potential for fraud, identity theft and other possible threats. This includes encryption, integrity checking and user identity validation. 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,[15] 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 and the confidentiality, integrity and availability ('CIA triad') of information.

The mobile industry has a long history of providing secure products and services to customers[16]:

- **Protecting network infrastructure and devices**
  Mobile 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' being applied across the value chain. The GSMA itself plays a central role in coordinating activities 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 together provide a security assurance framework to facilitate security improvements across the mobile industry.

- **Protecting public safety**
  Mobile networks are considered critical national infrastructure in many jurisdictions, and the services they support play a key role in protecting the public. The laws and regulations applicable to mobile operators, including telecoms licence conditions, often require them to take on additional responsibilities and assist law enforcement agencies.

14 European Commission (2017), *Communication on Building a European Data Economy*
15 ENISA (2016), *Definition of Cybersecurity: Gaps and Overlaps in Standardisation*

- **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. Mobile 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.

Debate

In the context of 5G implementation and the expanding web of IoT devices, services and AI, 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?

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.

Different types of cyberthreats have the potential to undermine the integrity of networks through unauthorised interception of networks. This can be through hardware and software in the mobile value chain, as well as through the use of social engineering where employees and mobile users are deceived into providing information. The mobile industry has been responding to these threats primarily by building more sophisticated security, training employees and conducting awareness-raising campaigns for customers. A holistic approach is important, with security and privacy embedded in the culture and early stages of product and service development.

While the GSMA provides guidance on a range of mobile security risks and mitigation measures,[17] the mobile industry looks to governments and law enforcement agencies to ensure there are appropriate legal frameworks, resources and processes in place to deter and prosecute criminal behaviour. Cybersecurity is not restricted by borders and requires national and international cooperation, such as those reflected in the Convention on Cybercrime, known as the Budapest Convention,[18] and the African Union Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention.[19]

Resources

Mobile Telecommunications Security Landscape 2023, GSMA, February 2023

Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, November 2022

Cybersecurity: A Governance Framework for Mobile Money Providers, GSMA, September 2019

Cybersecurity and Mobile Money: Prioritising Consumer Trust and Awareness, GSMA, July 2021

16 GSMA (2017), *Safety, Privacy and Security Across the Mobile Ecosystem: Key Issues and Policy Implications*
17 GSMA Mobile Cybersecurity Knowledge Base
18 Council of Europe Convention on Cybercrime

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 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 mobile 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 increase the risk of consumers unwittingly providing easy access to their personal information, leaving them exposed to unwanted or undesirable outcomes such as identity theft and fraud.

Debate

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

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, regardless of service or device, a consistent level of security must be provided.

Mobile operators believe that customer confidence and trust are only possible when users feel their privacy is appropriately protected.

Safeguards should include 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 specific types of data. For example,

legislation must deal with the risk to an individual arising from a range of data types and contexts, rather than focusing on individual data types.

The mobile industry should ensure privacy risks are considered when designing new apps and services and develop solutions that provide consumers with simple ways to understand their privacy choices and control their data.

The GSMA is committed to working with stakeholders from across the mobile industry to develop a consistent approach to privacy protection and promote trust in mobile services.

Resources

Promoting Transparency, Choice and Trust in the Digital Society, GSMA privacy website

Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, November 2022

5G and Data Privacy, GSMA, July 2020

Smart Data Privacy Laws, GSMA, June 2019

Protecting Privacy and Data in the Internet of Things, GSMA, February 2019

Mobile Privacy Principles, GSMA, February 2016

Data privacy and responsible AI

Background

The roll-out of 5G and the Internet of Things (IoT) is enabling organisations to process more real-world data in real time. The use of artificial intelligence (AI) systems, including generative AI (GenAI), supports data analysis on a significant scale and in an autonomous way, resulting in faster decision-making and the design of effective new solutions for economies and society at large. In the telecoms industry, AI and advanced data analytics are used, among other things, to optimise and automate networks, avoid service outages, reduce power consumption and CO_2 emissions, increase security and prevent fraud.

Mobile operators also provide AI capabilities to third parties on a commercial basis, such as delivering AI as a platform capability or employing AI to process mobile network data analytics for governments, traffic planning authorities, energy providers and other commercial organisations.

Recent and rapid advances in AI are also presenting challenges which, if not properly addressed, can exacerbate issues such as breaches of privacy, the spread of misinformation and disinformation and security risks. Some international bodies have worked to create a framework for AI development, including UNESCO's Recommendation on the Ethics of Artificial Intelligence, and the EU's AI Act which aims to address the risks generated by specific uses of AI.

The mobile industry has developed the *AI Ethics Playbook* and a related self-assessment questionnaire, both of which are practical tools to help organisations consider how to ethically design, develop and deploy AI systems. The playbook explains how AI systems should be responsibly designed, developed and deployed in accordance with the principles of fairness, human agency and oversight, privacy and security, safety and robustness, transparency and explainability and accountability, and with full consideration of the potential environmental impact.

Debate

How can the mobile industry and legislators help society realise the benefits of AI in a responsible way that protects privacy and complies with applicable laws?

How can the mobile industry help increase trust in AI among its stakeholders and society at large?

Are new laws and regulations required for AI?

Industry position

As the adoption of AI accelerates, it is vital that systems are designed, developed and deployed responsibly while upholding an individual's right to privacy and protecting personal data. Governments and regulators can help create a flourishing environment by ensuring that laws and regulations are not onerous, and that they support innovation, provide certainty and build trust.

As providers of mobile infrastructure, mobile operators encourage governments to consider the implications of legislation for the industry, including the potential impact on technology uptake and future economic efficiency gains through the use of AI systems. A risk-based approach should be taken when developing AI laws and regulations to ensure appropriate safeguards are in place while promoting innovation and competition. Ideally, these should be standardised and applied internationally and consistently to enable AI solutions to benefit from economies of scale.

Governments should facilitate and fund further research and development and investment in AI and mobile data-related solutions in both the public and private sectors. To foster an environment that attracts AI talent, it is important that governments invest in capacity building to ensure policymakers and regulators are guided by best practice and in digital skills to help citizens and industry keep pace with rapidly evolving AI technology.

The mobile industry recognises the potential societal benefits of AI and seeks to unlock its potential in a way that respects well-established privacy-by-design principles. Mobile operators are committed to the responsible use of AI in their operations, customer interactions and external products and services to protect customers and employees and ensure that AI operates fairly and reliably.

Resources

The Mobile Industry and AI, GSMA, February 2023

The AI Ethics Playbook: Implementing Ethical Principles into Everyday Business, GSMA, February 2022

AI Ethics Assessment, GSMA

Mobile Privacy and Big Data Analytics, GSMA, February 2017

Privacy Design Guidelines for Mobile Application Development, GSMA, February 2012

Data-Driven Innovation: Big Data for Growth and Well-Being, OECD, October 2015

Electromagnetic fields and health

Background

Research into the safety of radio signals has been conducted for several decades and underpins the 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, including 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 (IARC) 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 device or text messaging.

Mobile phones are tested for compliance with exposure limits when operating at maximum power. A mobile phone typically 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 2024.

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?

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.

Ongoing, 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.

Resources

The International EMF Project website, WHO

EMF Exposure Compliance Policies for Mobile Network Sites, GSMA, October 2021

International EMF Exposure Guidelines, GSMA, October 2021

Safety of 5G Networks, GSMA website

5G EMF Surveys, GSMA interactive map

Illegal content

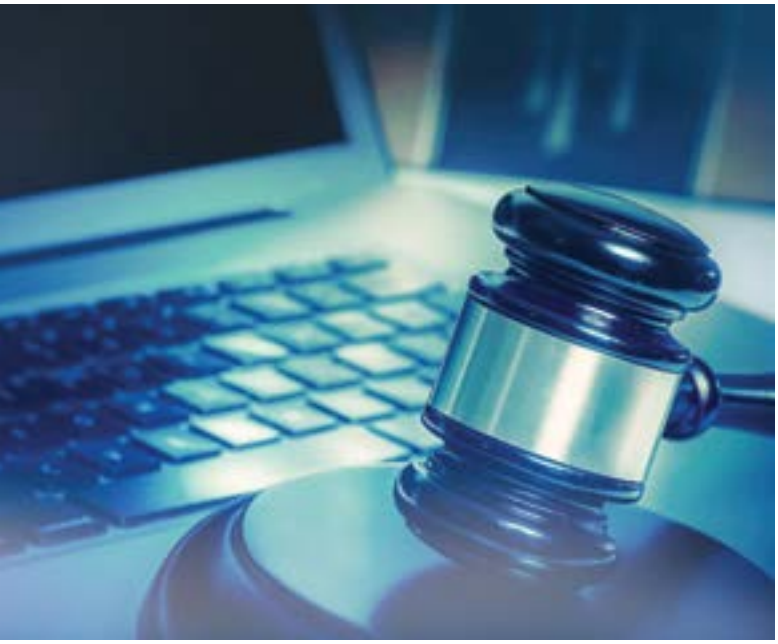
Background

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 but is protected by rights to freedom of expression in others.

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 takedown' processes to remove or disable access to the illegal content as soon as they are notified of its existence by the appropriate legal authority).

Mobile operators are typically alerted to illegal content by national hotline organisations or law enforcement agencies. When content is reported, operators follow procedures 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.



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?

Industry position

The mobile industry is committed to working with law enforcement agencies and appropriate authorities, and to having robust processes in place that enable the swift removal or disabling of confirmed instances of illegal content hosted on their services.

ISPs, including mobile operators, are not qualified to decide what 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 to Combat Digital Child Sexual Exploitation 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.

Resources

Combatting Online Child Sexual Abuse Content website, GSMA Mobile Alliance Against Child Sexual Abuse Content

Notice and Takedown: Company Policies and Practices to Remove Online Child Sexual Abuse Material, GSMA and UNICEF, May 2016

Hotlines: Responding to Reports of Illegal Online Content, GSMA, July 2016

Child Sexual Abuse Material: Model Legislation and Global Review, Tenth Edition, International Centre for Missing and Exploited Children, 2023

INHOPE website

The Model National Response website, WePROTECT Global Alliance

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.

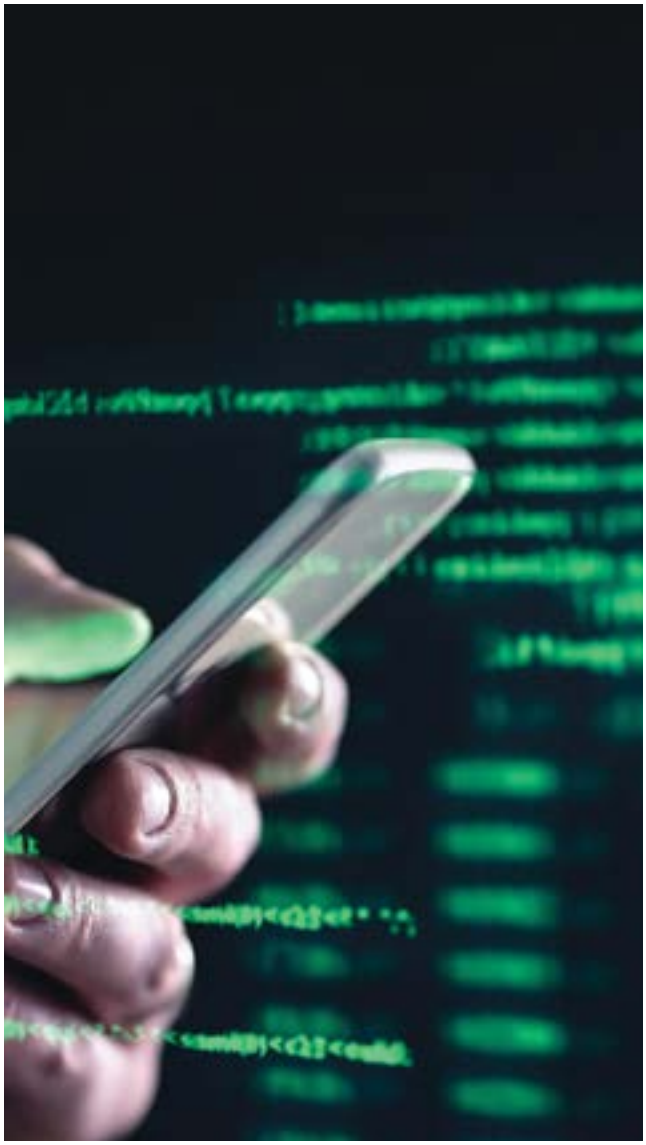
Internet governance requires input and collaboration from diverse stakeholders relating to their interests and expertise in technical engineering, resource management, standards and policy issues, among others. Relevant stakeholder groups will vary depending on the specific internet governance issues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

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?



> "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 today, any architecture designed to govern its use should be capable of addressing a range of issues and challenges 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 a 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.

Resources

Internet Governance Forum website

WSIS+20 and IGF+20 Review by the UN General Assembly (2025), Internet Governance Forum

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, Google, LinkedIn, Meta, Microsoft, Pinterest, Snapchat, Tumblr, Yahoo! and X), publish 'transparency reports' that provide statistics relating to government requests for disclosure of such data.

Debate

What is the correct legal framework to achieve a balance between a government's obligation to ensure that 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?

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 they believe to be outside the scope of 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 publication of statistics related to requests for access to customer data.

Resources

Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, Office of the High Commissioner for Human Rights, 2011

Judgment on the Data Retention and Investigatory Powers Act 2014 ('DRIPA'), UK High Court of Justice

A Question of Trust: Report of the Investigatory Powers Review (UK), David Anderson QC, June 2015

Office of the Privacy Commissioner of Canada website

Mandatory registration of prepaid SIMs

Background

In several 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. At the end of 2020, 72% of mobile subscriptions were prepaid[20] and 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 African countries, where SIM registration is required to identify the user.

Some governments, including the Czech Republic, UK and USA, have decided against mandating registration for 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

19 African Union Convention on Cyber Security and Personal Data Protection
20 GSMA Intelligence, prepaid penetration (prepaid connections, Q3, 2020)

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.

Debate

To what extent do the benefits of mandatory prepaid SIM registration outweigh the costs and risks?

What factors should governments consider before mandating such a policy?

Industry position

While registration of prepaid SIM card users can have valuable benefits for 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 consider global best practices and allow registration mechanisms that are flexible, proportionate and relevant to the market, including the level of official ID penetration 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 that are considering the introduction or revision of mandatory SIM registration to take the following steps before 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 their operational costs.

Resources

Access to Mobile Services and Proof of Identity, GSMA, April 2021

Enabling Access to Mobile Services for the Forcibly Displaced, GSMA, September 2017

Regulatory and Policy Trends Impacting Digital Identity and the Role of Mobile, GSMA, October 2016

Mandatory Registration of Prepaid SIM Cards: Addressing Challenges through Best Practice, GSMA, April 2016

Mandated service restriction orders (network shutdowns)

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, mobile 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, and can become 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.

Debate

What factors and alternatives should governments consider before planning an SRO?

What tools and methods can be used to avoid the need for an SRO or to avoid negative impacts if an SRO is the only option?

Industry position

The GSMA discourages the use of SROs. Governments should only resort to SROs in exceptional and pre-defined circumstances, and only if absolutely necessary and proportionate to achieve a specified and legitimate aim that is consistent with internationally recognised human rights and relevant laws.

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 SRO. If it would undermine national security to do so at the time 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 of the potential impact of SROs among government officials. 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 to establish whether it has been approved by a judicial authority, whether it is valid and binding and whether there is any opportunity for an 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.

First and foremost, all decisions should be made with the safety and security of the mobile operator's customers, networks and staff in mind, and with the aim of restoring services as quickly as possible.

Resources

Guidelines for the Lawful Disruption of Access to Online Services, Australian Government, July 2017

Joint Statement on Network and Service Shutdowns, Global Network Initiative and the Telecommunications Industry Dialogue, July 2016

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 and shared to harm a person, social group, organisation or country. Another commonly used term is malinformation, which is true information shared intentionally to cause harm.

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.

The European Commission is regulating misinformation and disinformation through the Digital Services Act (DSA),[22] which came into force in November 2022, following the Commission's concerns regarding the growing influence of online platforms in political discussions, disinformation campaigns, fake news dissemination in the lead-up to elections and the societal impact of hate speech.

21 GSMA (2021), *Access to Mobile Services and Proof of Identity 2021*

Debate

Who determines whether information is true or false?

What are the most effective mechanisms to deal with misinformation and disinformation?

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 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.

Resources

Exploring Online Misinformation and Disinformation in Asia Pacific, GSMA, July 2021

Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, November 2022

2022 Code of Practice on Disinformation, European Commission

EMF and Health website, GSMA

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 in shadow or underground markets by organised criminal networks. It is estimated that almost one in five mobile devices may be counterfeit.[23] This has far-reaching negative impacts. Consumers risk lower quality, safety, security, environmental health and privacy assurances. Governments forgo taxes and duties and must contend with increased crime. Industry players are also affected, as it can harm the trademarks and brands of legitimate device manufacturers and the substandard performance of counterfeit devices can have implications for mobile operators.

Some countries have introduced national lists of homologated (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. Mobile 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 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.

Debate

How can governments and other stakeholders best address the issue of counterfeit mobile devices?

Industry position

The mobile industry supports the need for legal and product integrity in the mobile 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 (WCO), to encourage and facilitate action by relevant agencies in other jurisdictions.

The GSMA makes its device information and device status services available for customs agencies and other industry stakeholders to verify the authenticity of mobile device 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 mobile operators to deploy systems like the Equipment Identity Register (EIR) and to connect to GSMA systems such as the GSMA Device Database.

22 European Commission website, *Tackling online disinformation*

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 to reduce 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 mobile 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.

Resources

Preventing Device Crime website, GSMA Device Information Services

GSMA IMEI Database website

The Economic Cost of IPR Infringement in the Smartphones Sector, EUIPO and ITU, February 2017

Spot a Fake Phone website

Mobile devices: theft

Background

Policymakers in many countries are concerned about the incidence of mobile device theft, particularly when organised crime becomes involved in the trafficking 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 accessible to mobile operators around the world to ensure that stolen devices transported to other countries can be 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 and reliability in accordance with GSMA-defined security requirements.

Debate

What can industry do to prevent mobile phone theft?

What are the policy implications of this rising trend?

Industry position

The mobile industry has led numerous initiatives and developed a range of enablers in the global fight against mobile device theft.

Although the problem of device theft is not of the industry's creation, the industry recognises it is part of the solution. When lost or stolen mobile devices are rendered useless, they have significantly less value, removing the incentive for thieves to target them.

The GSMA encourages mobile operators to participate in its Device Registry service 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 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.

IMEI blocking, when combined with other multistakeholder measures, can be the cornerstone of a highly effective anti-theft campaign.

Consumers who have had their devices stolen can be 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 markets.

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 and encourages 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.

Resources

Preventing Device Crime website, GSMA Device Information Services

IMEI Security Technical Design Principles, GSMA, August 2016

IMEI Security Weakness Reporting and Correction Process, GSMA, November 2016

Anti-Theft Device Feature Requirements, GSMA, May 2016

Security Advice for Mobile Device Users website, GSMA

Mobile network and device security

Background

Security attacks can affect 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 complex. While no security technology is guaranteed to be unbreakable, practical attacks on mobile services are rare because 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 4G and 5G networks are considerably better protected against eavesdropping risks than earlier generation networks. 5G technology boasts a host of new security capabilities that further enhance protection levels.

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?

How is 5G, and all the capabilities it brings, affecting the security landscape?

Industry position

The protection and privacy of customer communications is at the forefront of mobile 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 mobile operators aware of the risks and mitigation options available to protect their networks and customers. This work, described below, is recognised by regulators around the world as sufficient to eliminate the need to formally regulate.

- The GSMA works with a large group of experts to facilitate an appropriate response to threats. It plays a key role in coordinating the industry response to security vulnerability research through its Coordinated Vulnerability Disclosure (CVD) programme.[24]

- 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 analysis involving industry experts from across the ecosystem, regulators and 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 range of security guidance publications, including the GSMA Baseline Security Controls, which helps mobile operators understand and develop their security posture.

23 According to figures from OECD, 2017

- The GSMA's Fraud and Security Group acts as a centre of expertise for the industry's management of fraud and security matters. The group seeks to maintain or increase the protection of mobile operator technology and infrastructure, as well as customer identity, security and privacy, to ensure the industry maintains a strong reputation and mobile operators remain trusted partners in the ecosystem.
- The GSMA Mobile Cybersecurity Knowledge Base makes the combined knowledge of the 5G ecosystem available 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, as SIM cards have proven to be resilient to attack. The Embedded Universal Integrated Circuit Card (UICC) approach that has been defined by the GSMA and rolled out by industry inherits the best security properties of the SIM and is designed to build on the protection levels achieved in the past.
- The GSMA constantly monitors the activities of hacker groups, researchers, innovators and a range of industry stakeholders to improve the security of communications networks. The ability of the GSMA to learn and adapt can be seen in the security improvements that have been implemented from one generation of mobile technology to the next.

Resources

GSMA Mobile Cybersecurity Knowledge Base, GSMA

FS.31 Baseline Security Controls, GSMA

GSMA Mobile Telecommunications Security Landscape, GSMA, February 2023

Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, November 2022

GSMA T-ISAC website

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 the USA.

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 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 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 forcing a deteriorated service for consumers.

Debate

Should governments or private organisations be allowed to use signal inhibitors that interfere with the provision of mobile voice and data services to consumers?

Should the marketing and sale of signal inhibitors to private individuals and organisations be prohibited?

Industry position

In some Latin American countries, such as Colombia, El Salvador, Guatemala and Honduras, governments are promoting the deployment of signal inhibitors to limit the use of mobile services in prisons. The GSMA and its members are committed to working with governments to use technology 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 to find a long-term, practical solution that does not have a negative impact on legitimate users or 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.

Signal inhibitors should only be used as a last resort and only deployed in coordination with mobile operators. This coordination must continue for the duration of the deployment of the devices, from installation 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 create 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 from being smuggled into sensitive areas such as prisons is the most effective measure against the illegal use of mobile devices in these areas, and this would not affect the rights of legitimate users of mobile services.

Resources

Common Position Proposal on Signal Inhibitors (Jammers) in Latin America, GSMA, November 2014

Signal Inhibitor Solutions: Use of Jammers in Prisons, GSMA, December 2018

Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, November 2022

04 Environmental sustainability

The latest science warns that the impacts of climate change are greater and more far-reaching than previously understood, and that the window of opportunity to remain within the Paris Agreement's 1.5°C temperature goal is quickly narrowing. The mobile industry recognises the importance and urgency of tackling the climate crisis, which is why mobile operators are taking steps to mitigate their own impacts while deploying digital solutions to reduce emissions and enhance resilience in other sectors and society.

To understand how the mobile industry is progressing, mobile operators and suppliers are encouraged to disclose their climate impacts, risks and opportunities to the Carbon Disclosure Project (CDP) every year. Operators are setting emissions reduction targets – with best practice aligned with the ICT sector pathway to net-zero GHG emissions by 2050 or earlier – and reducing their emissions by improving energy-efficiency, purchasing and using renewable energy and electrifying heat and fleet vehicles. They are also working with other sectors to decarbonise by using smart, connected technologies and to change behaviours to improve efficiency and enable a low-carbon economy.

To put the world on a sustainable path requires the collective will and participation of everyone, not just one sector. Governments and regulatory authorities are key players in setting new policies and stimulating innovation for a world at risk.

The following topics offer a snapshot of the key aspects of climate action that touch the mobile sector and the industry's perspective on how governments can, and must, take swift and meaningful action:

- To prioritise a just transition to economy-wide net-zero emissions by 2050 at the latest.
- To lay out national policies and plans that enable these targets to be achieved.
- To create and protect resilient green jobs and provide education, reskilling and retraining opportunities for the workforce, in dialogue with business and other stakeholders.

Energy efficiency

Background

As mobile use and demand for widespread connectivity grow, so too does demand for data accessed through network infrastructure. Heavier data traffic drives up electricity use across networks, placing energy efficiency high on the agenda of mobile operators for both financial and environmental reasons.

Through innovation, the industry has boosted the efficiency of every new generation of mobile technology and 5G is the most energy efficient yet. The roll-out of 5G and densification of towers mean that, in the short term, mobile networks are expected to consume more electricity to support the increase in data traffic. This increase can be mitigated by retiring older, less energy-efficient 2G and 3G networks, by switching from copper to fibre for fixed networks and by deploying energy-efficient features of 5G, such as AI-optimised sleep modes.

The industry is working on several fronts:

- Improving the efficiency of new networks with 5G specification by calling for a 90% reduction in the energy used to transfer each unit of data.[25]
- Switching off and removing legacy network equipment as soon as it becomes feasible to support migration to newer, more energy-efficient equipment.
- Running efficiency programmes to identify energy hotspots and deploy measures to reduce energy consumption – for example, through temperature optimisation, free cooling at cell sites and power-saving features such as AI, selective switch-off and generator battery hybrids.
- Encouraging mobile operators to earn the ISO 50001 certificate, which is the global standard for energy management systems in organisations.
- Sharing and encouraging alignment with energy best practice across the industry to highlight operators' energy-efficiency measures.
- Making fleets more energy-efficient by investing in more fuel-efficient and lower carbon vehicles and by improving access to electric vehicle charging stations to facilitate the transition.

Debate

How can innovation in mobile technology support national energy-efficiency improvements?

How can the mobile industry and governments work together to retire inefficient legacy equipment?

24 GSMA Coordinated Vulnerability Disclosure (CVD) programme

Industry position

Policies that support and incentivise the transition to more energy-efficient networks and mobile industry practices are an important part of achieving carbon reduction goals.

The mobile industry calls on governments to:

- Support the roll-out of newer, more energy-efficient networks such as 5G, where it is feasible, including through efficient spectrum policy.
- Enable older, less energy-efficient legacy equipment to be retired in regions where this is feasible and circumstances dictate market readiness for deployment.
- Provide incentives for businesses to deploy energy-efficiency measures – for example, through reduced taxation for upgrading equipment, regulatory treatment and preference in public procurement.
- Support research and development for innovative, energy-efficient technologies – for example, for network equipment, data centres and buildings.

Resources

5G Energy Efficiencies: Green is the New Black, GSMA Intelligence, 2020

Going Green: Benchmarking the Energy Efficiency of Mobile, 2021

The 5G Guide: A Reference for Operators, GSMA, 2019

Renewable electricity

Background

The fastest way for mobile operators to reduce carbon emissions is by using, purchasing and investing in renewable energy to power their operations. Many operators around the world are already doing this and have targets in place to source all of their electricity requirements from renewable sources. [26]

However, there are challenges in sourcing renewables in many markets. For some markets, this is due to a lack of sourcing options due to centralised market control, while for others this is due to a lack of appropriate financial and legal structures to support investment in renewables. High costs are a barrier in some countries, while others lack access to sufficient renewable energy resources. For some, it is a combination of these and other factors.[27]

The mobile industry recognises the urgent need to decarbonise electricity. The industry supports the phase-out of fossil fuel use and production and the ramp-up of clean and renewable sources of energy generation to increase renewable capacity. The following actions are being taken:

- Developing targets and demonstrating progress to source 100% renewables for networks, data centres, buildings and infrastructure, including towers managed by towercos and energy service companies (ESCOs).
- Publicly declaring renewable energy commitments – for example, through the RE100 initiative – and sending strong demand signals to the marketplace and to policymakers.
- Investing in new renewable capacity – for example, by installing on-site renewable energy and pursuing power purchase agreements (PPAs) with new power generation facilities.
- Engaging with policymakers to highlight the challenges of developing and accessing renewables and advocating for solutions.

25 GSMA (2019), *The 5G Guide: A Reference for Operators*
26 GSMA (2023), *Mobile Net Zero: State of the Industry on Climate Action 2023*

Debate

How can the mobile industry commit to investment in additional renewable electricity generation?

How can PPPs accelerate the transition to renewable energy?

Industry position

Governments play a crucial role in decarbonising the electricity supply by supporting investment, innovation and regulation designed to phase out fossil fuel use and production and ramp up renewable capacity.

The mobile industry calls on governments to:

- Implement policies, regulations, market design and permitting that help to accelerate the deployment of renewable energy generation and expansion of electricity networks, including corporate purchases of renewable energy.
- Address financing gaps and barriers for clean energy investments, particularly in LMICs where the cost of capital is high.
- Support innovation to further reduce costs and improve technology performance of solar, wind and other clean energy sources, as well as the use of digital technologies to maximise the benefits of variable renewables.
- Set targets and timelines to phase out fossil fuel subsidies and unabated fossil fuel generation in line with the 1.5°C target of the Paris Agreement.

Resources

Mobile Industry Position Paper: Access to Renewable Energy, GSMA, 2022

Renewable Energy for Mobile Towers: Opportunities for Low- and Middle-Income Countries, GSMA, 2020

Energy Challenges for Mobile Networks in Sub-Saharan Africa, GSMA, 2023

Sustainable supply chain

Background

One of the biggest environmental impacts of the mobile industry is the manufacturing and use of devices and equipment. Although mobile phones and network equipment account for a small proportion of overall e-waste by weight, they can have a bigger impact than other waste streams because of the rare earth minerals and metals they contain.

By moving away from linear business models of mine-manufacture-use-dispose and towards more circular business models that repair, reuse and recycle equipment, the industry can become more environmentally sustainable. This is because circular business models harness the materials in unwanted equipment for other uses rather than treating everything as waste.[28]

The benefits of a circular economy and the need for it are undeniable. While the industry is mainly adopting circular economy practices through separate initiatives, the GSMA has created a strategy that outlines opportunities to create a global and unified vision for the whole ecosystem.[29] The strategic vision is underpinned by two principles: increasing the longevity of devices and equipment, and sending zero waste to landfill.[30]

Mobile companies are actively engaging in and supporting new e-waste policies and legislation around the world and creating reverse logistics supply chains to manage the flow of equipment for recycling. Leading operators are also boosting take-back schemes for unwanted mobile phones and sending zero waste to landfill.[31]

27 GSMA (2022), *Mobile Industry Position Paper: Access to Renewable Energy*
28 Tillekeratne, D (22 April 2020), 'Understanding the mobile waste management efforts of MNOs in emerging markets', GSMA Blog
29 GSMA (2022), *Strategy Paper for Circular Economy: Network Equipment*
30 GSMA (2022), *Strategy Paper for Circular Economy: Mobile Devices*

Debate

Could investment in innovative technology reduce waste and recover precious materials, advancing more of the SDGs?

How can governments and industry collaborate to enhance the longevity of mobile devices and equipment?

Industry position

Governments can facilitate the transition to a circular economy by implementing policies that promote resource efficiency, innovation, solutions and standards.

The mobile industry calls on governments to:

- Formulate clear policies and standards to drive energy and materials efficiency and circularity.
- Include recommendations for products to be designed for circularity.
- Support innovation and create incentives for circular solutions, including the development of infrastructure for handset reuse and component and materials recycling.
- Engage with mobile operators and equipment and device manufacturers on waste and what happens at the end of a product's life.

Resources

Strategy Paper for Circular Economy: Network Equipment, GSMA, 2022

Strategy Paper for Circular Economy: Mobile Devices, GSMA, 2022

Reuse, Refurbish, Recycle website, GSMA, 2023

Enabling digital transformation

Background

Mobile and other connected digital technologies are expected to transform all parts of the economy over the next decade. With targeted policies and investment, connected digital technologies have the potential to be a key driver of low carbon development.

Digital transformation can drive low carbon development by enabling more efficient use of energy and materials, implementing more circular business models and transitioning to renewable sources of energy.

Examples include smart, connected energy grids to manage predictable but intermittent renewable energy sources, smart building energy systems to reduce electricity and gas consumption and precision agriculture technologies to reduce water, fertiliser and pesticide use.

Debate

How can governments accelerate the deployment of smart, connected technologies that will support national energy transition plans?

How can mobile operators collaborate with national and local governments to develop low-carbon solutions?

Industry position

The digital transformation of industry through the adoption of smart, connected technologies can significantly lower carbon emissions, and governments should make every effort to encourage this change across all sectors.

The mobile industry calls on governments to:

- Recognise that digital transformation can support decarbonisation. For a just transition, this should be accompanied by supporting policy measures that minimise any negative impacts on employment.
- Encourage and incentivise private and public investments in digital infrastructure and solutions that contribute to climate change mitigation or adaptation and include them in existing and future state aid programmes, such as tax reductions, regardless of the sector.
- Promote policies that favour a broader digital transformation of the economy combined with a robust digital governance framework to boost the transformation that many sectors must undertake.
- Encourage the use of smart technologies to reduce emissions – for example:
  - Reduce the energy consumption of buildings.
  - Increase renewable energy use through smart grids.
  - Improve agricultural resilience and adaptation and reduce resource consumption.
  - Advance manufacturing processes and the ecosystem around them to create more sustainable production with a lower environmental impact.

Resources

The Enablement Effect, GSMA, 2019

The Role of Digital and Mobile Enabled Solutions in Addressing Climate Change, GSMA, 2021

Appendix: Connecting the World Through Mobile

The global unique subscriber base for mobile telecommunications grew by 2.5% in the previous 12 months, reaching 5.6 billion in 2023. Growth in the unique subscriber segment is driven by LMICs across South Asia, South America and Sub-Saharan Africa. These regions are forecasted to grow by 340 million subscribers over the next six years.

The mobile internet subscriber base grew by 5.1% in the previous 12 months, fuelled by growth in developing markets in South Asia and Sub-Saharan Africa. Recent regulator and mobile operator strategies that have increased the coverage and quality of long-term evolution (LTE) have catapulted the number of mobile internet subscribers to 4.7 billion.

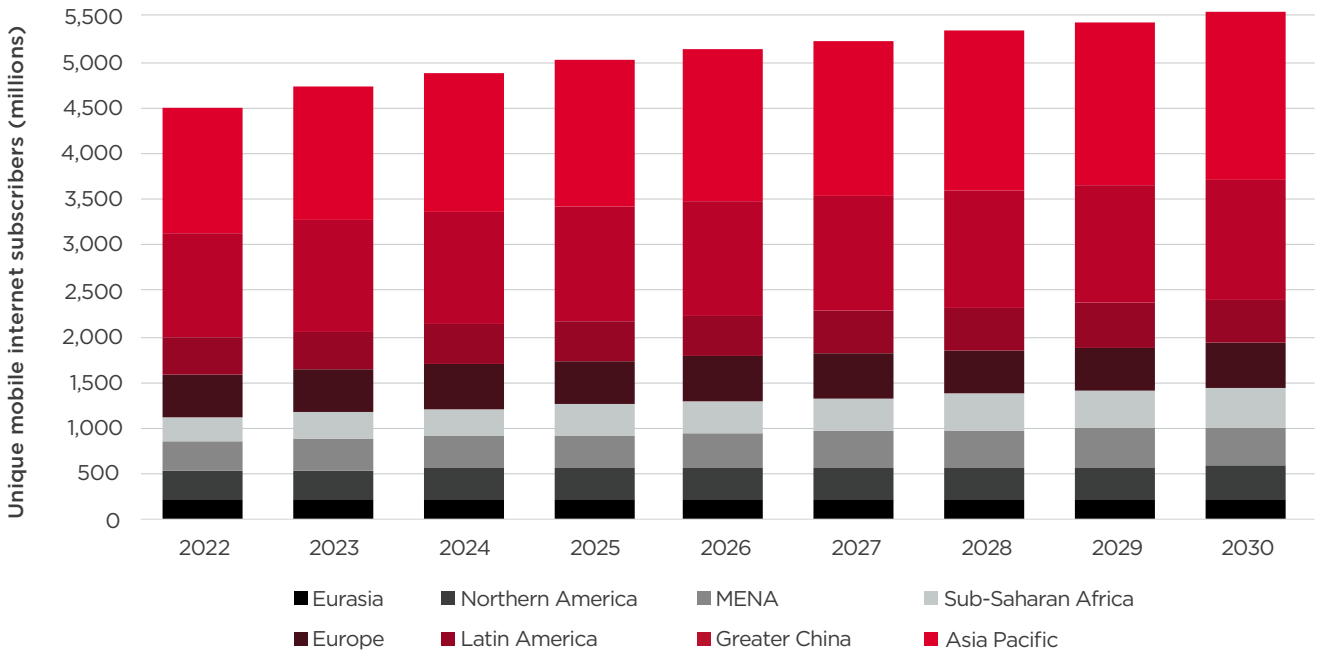
GSMA Intelligence forecasts that 5G connections will grow by more than 170% between 2023 and 2028 to reach 4.3 billion connections overall, with markets outside North America and East Asia launching more networks within the next two years.

Mobile operators planned to invest approximately 85% of capital expenditure (CapEx) in 5G in 2023 and more LMICs are shifting investments to 5G to meet consumer demand for data. The highest growth rates will be observed in Latin America, South Asia and Western Europe.

GSMA Intelligence forecasts that mobile operators will boost revenues by 1.8% CAGR between 2023 and 2030 to reach $1.3 trillion. While connections will continue to increase, a lower subscriber growth rate, coupled with declining levels of ARPU, will produce this modest increase.

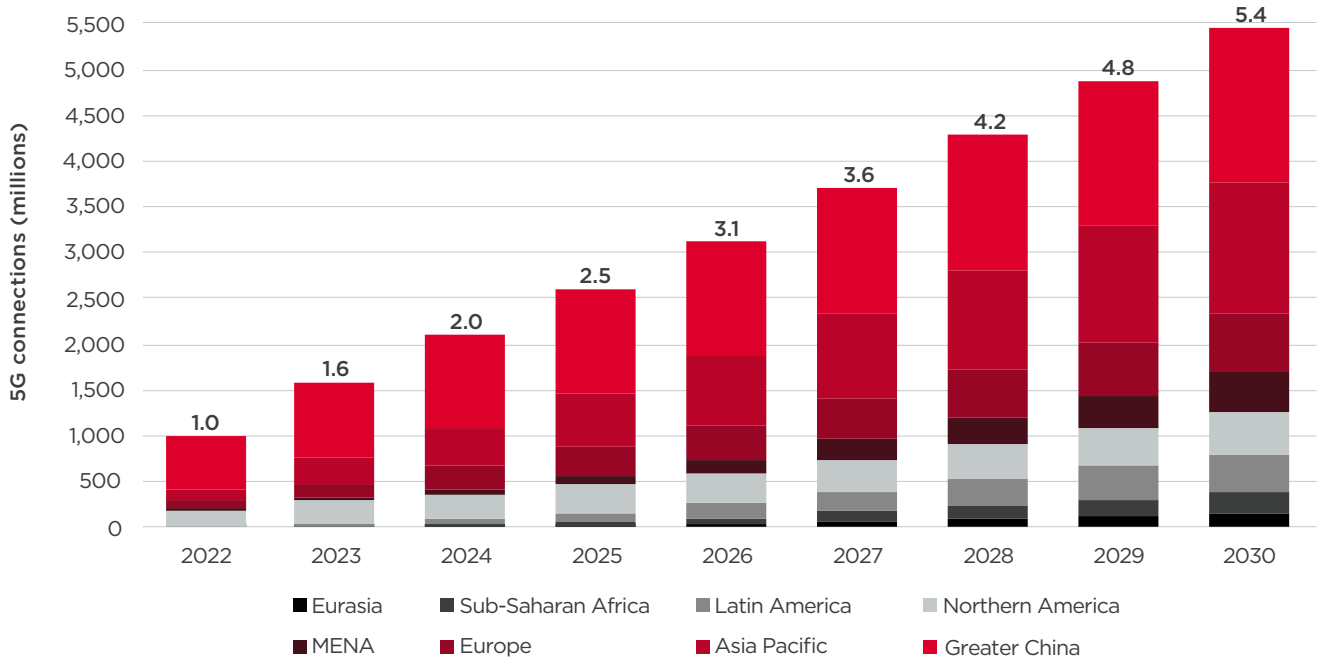
Furthermore, GSMA Intelligence forecasts that the total number of IoT connections (cellular and non-cellular) globally will reach 26.1 billion in 2025 and rise to 38.5 billion by 2030, 5.8 billion of which will be licensed cellular technologies (including 5G). While the pandemic had an adverse impact on the uptake of 5G, growth has returned in both the enterprise and consumer sectors.

Figure 2 | Unique mobile internet subscriber penetration by region



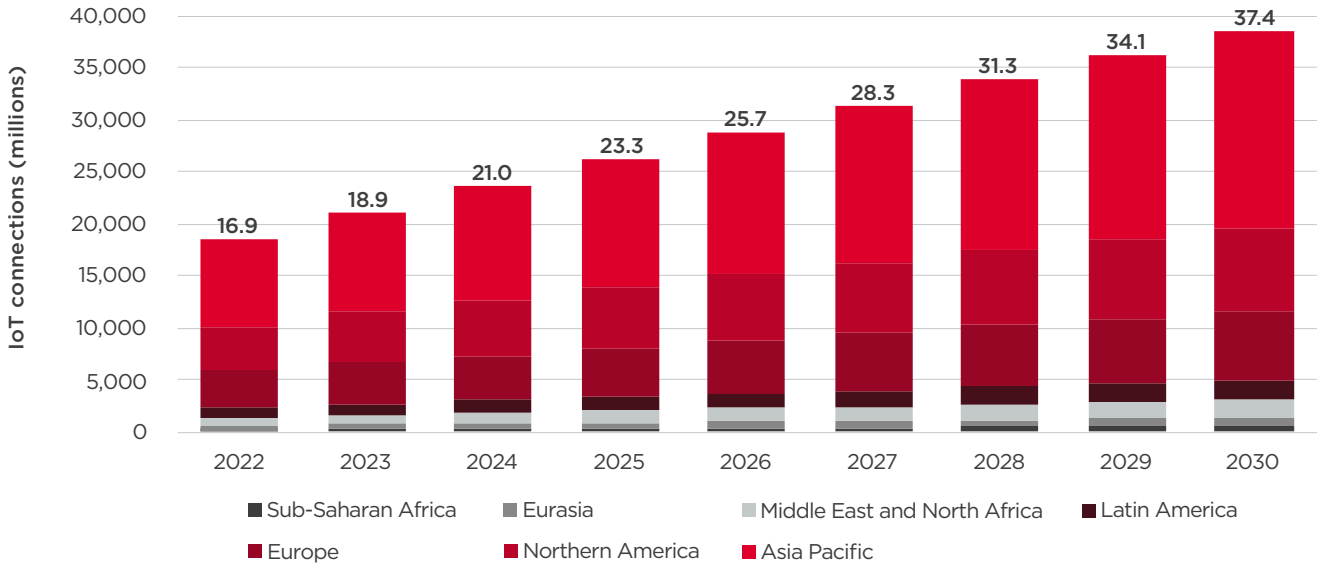
Source: GSMA Intelligence

Figure 3 | 5G connections by region (billions)



Source: GSMA Intelligence

Figure 4 | Total IoT connections by region, 2022–2030 (billions)



Source: GSMA Intelligence

GSMA Intelligence

GSMA Intelligence is the definitive source of mobile industry insights, forecasts and research used around the world for benchmarking and business planning. The analysis covers five key areas: 5G and network transformation; spectrum; IoT and the wider enterprise space; the digital consumer; and fixed and pay-TV. Covering every mobile operator, network and MVNO in every country worldwide, the team of analysts and experts use their deep understanding of markets, technologies and regulatory issues to identify and understand mobile trends and form captivating analysis on the topics shaping the mobile industry.

Global coverage

GSMA Intelligence publishes data and insights spanning 240 markets and 900 mobile and fixed network operators. Comprising more than 50 million individual data points, GSMA Intelligence combines historical and forecast data from the growth of the industry in 2000 with forecasts out to 2030. New data is added every day.

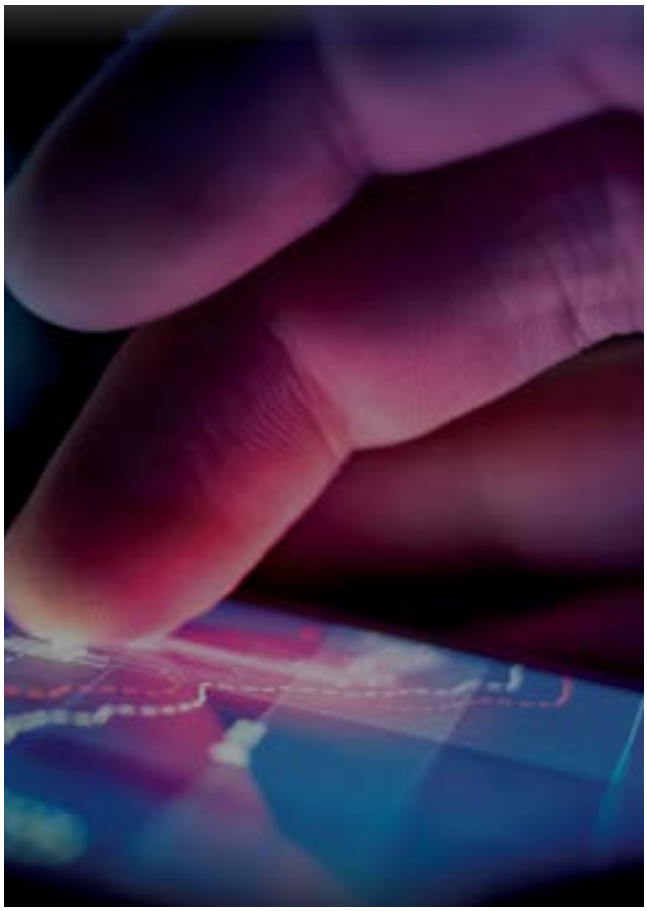
Numerous data types

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 such as multifaceted search, rankings, filters, dashboards and a real-time data and news feed, as well as the ability to export data into Excel and add graphs and charts to presentations.

gsmaintelligence.com
info@gsmaintelligence.com




F21
FOREVER 21
QFRONT
TSUTAYA
UC
oppo
アコム

GSMA™

GSMA Head Office
1 Angel Lane,
London,
EC4R 3AB,
United Kingdom
Tel: +44 (0) 20 7356 0600
Fax: +44 (0) 20 7356 0601