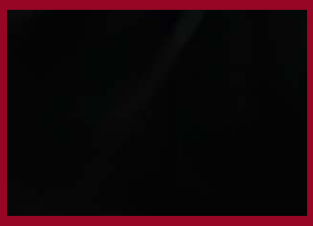
GSMA

Mobile Policy Handbook

An insider's guide to the issues



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 LinkedIn: **@GSMA**

February 2026

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.

To promote public and private sector collaboration, this handbook assembles policy topics and global mobile industry positions under one cover. This unique resource is an information 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.

In this edition, new positions have been added and others refreshed with more recent statistics and resources, to bring a deeper understanding. Please be aware that the Mobile Policy Handbook website is updated periodically between editions to ensure the latest information is reflected.

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.

Mobile networks securely and reliably transport the ever-increasing volumes of data that are necessary in today's world. By the end of 2024, 5.8 billion people worldwide subscribed to a mobile phone service, with 80% of those enjoying the benefits of a smartphone. Smartphone use is forecast to rise to 91% of connections by 2030, supported by the growing availability of financing plans and more affordable devices in Low- and Middle-Income Countries (LMICs).

For most people today, digital connectivity is a vital, productive and entertaining element of daily life, and mobile network operators constantly strive to enhance network services to enable the latest innovation in mobile applications. But the business environment for operators is one of accelerating change that creates challenges as well as opportunity.

Artificial intelligence (AI) is not only enhancing network capabilities, but is expected to generate far more network traffic across the economy. Satellite connectivity is proving to be both a complementary and competitive technology to terrestrial mobile service. Meanwhile, at a time of rising geopolitical tensions, mobile networks are acknowledged as national strategic infrastructure offering security and resilience.

Bringing new digital services to life

5G is a crucial evolution of mobile technology because it can support far greater volumes of data, enable a massive Internet of Things (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. These investments will help 5G proliferate for the benefit of all industries and consumers.

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. WRC-27 preparations are already underway with work on the likely roadmap for spectrum bands supporting future mobile technologies. The Conference will also look at a range of other issues, one of which will be connectivity between satellite and mobile handsets, known as Direct-to-Device (D2D).

As 5G adoption continues to scale up, mobile operators must realise a return on their investment, and they 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. As of mid-2025, only 18% of networks support 5G Standalone (SA), and although interest in 5G-Advanced is high, to date, few networks have launched commercially. Much of 5G's potential, therefore, remains untapped.

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 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.

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'. This 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

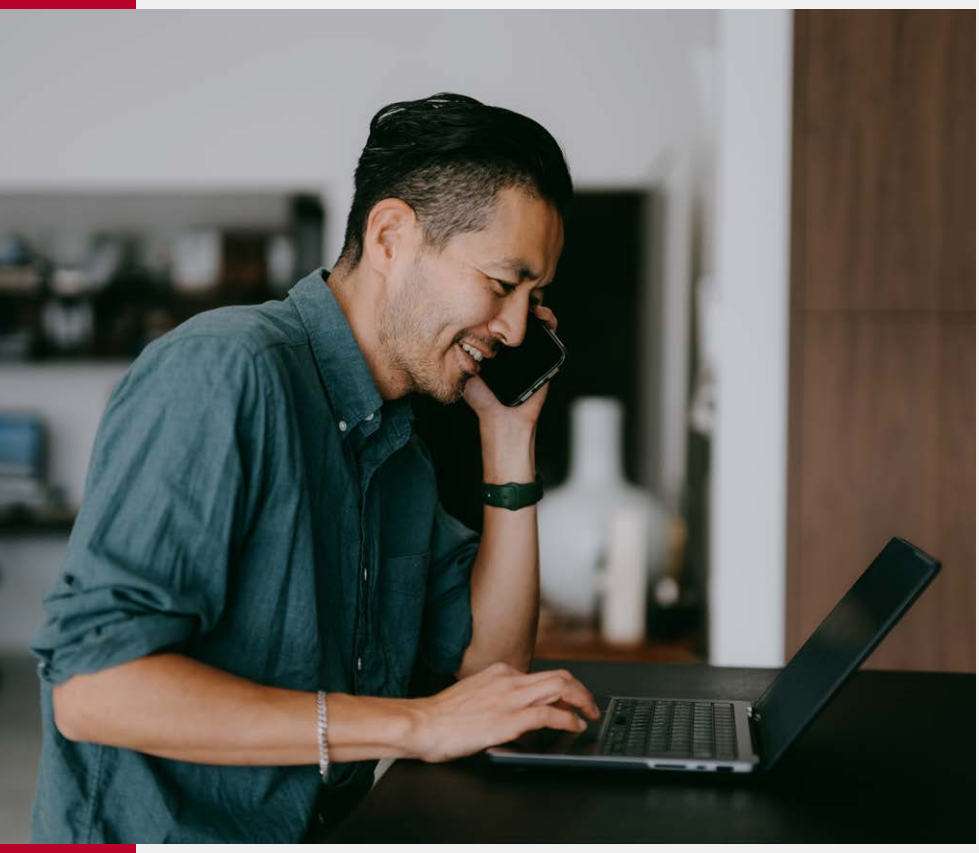
The Mobile Economy, GSMA
Mobile Net Zero: State of the Industry on Climate Action 2025, GSMA
The State of Mobile Internet Connectivity, GSMA

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 over 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, AI, competition policy, cybersecurity, the digital divide and spectrum.

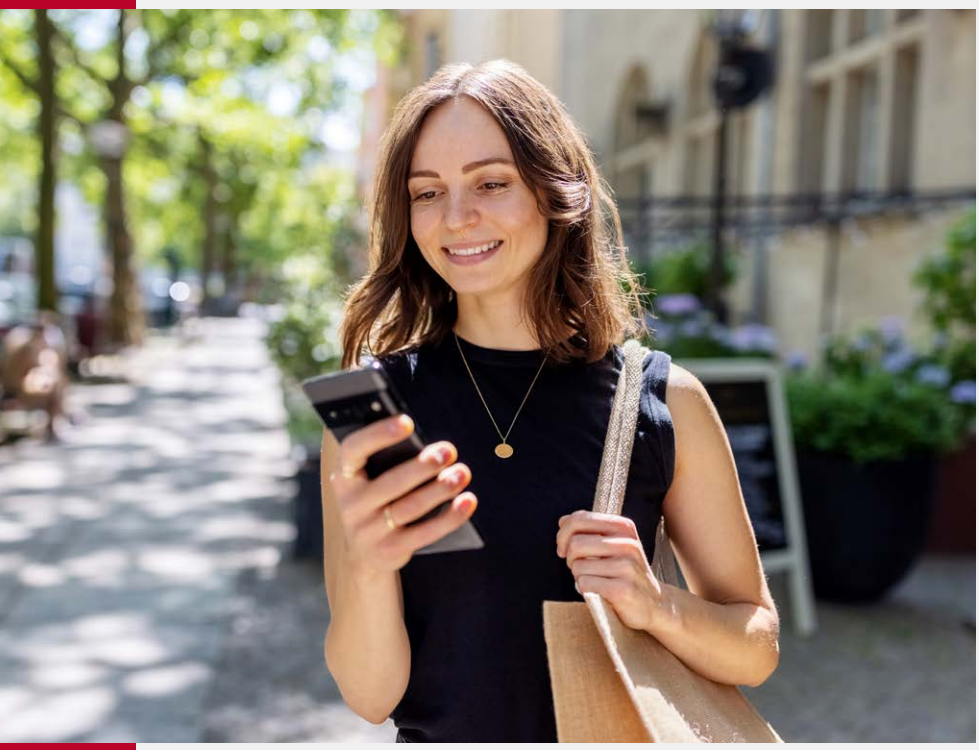
The in-house policy experts who develop and teach the courses have backgrounds in telecoms, law and financial services. Many also hold advanced academic qualifications. Through their work with the GSMA, they are in constant contact with governments and regulatory authorities around the world and this 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 certified by the United Kingdom Telecommunications Academy (UKTA) and accredited for Continuing Professional Development (CPD).

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 two 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
- An Introduction to Non-Terrestrial Networks
- Bridging the Mobile Gender Gap
- Children's Rights and Connectivity
- Cybersecurity in the Context of Mobile Telecoms
- Climate Change and the Mobile Industry
- Competition Policy in the Digital Age
- Mobile Connectivity and the AI Revolution
- Mobile Money for Financial Inclusion
- Personal Data in the Context of Mobile Networks
- Principles of Mobile Privacy and Security
- Radio Signals and Health
- Mobile Technology for Humanitarian Emergencies
- Spectrum Management for Mobile Telecommunications

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.

1 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.

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 (page 12) identifies four areas of policy action related to network investment, regulation, promoting the digital economy and demonstrating digital leadership.

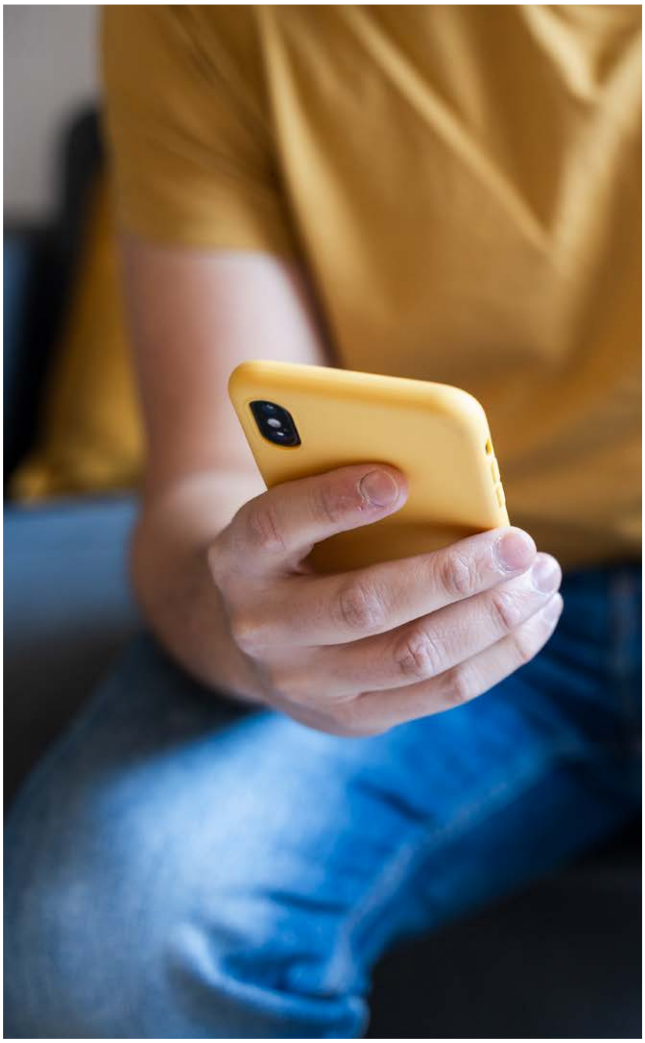


Figure 1: Policy levers to promote an inclusive digital economy

Encourage network investment

Implement a broadband policy with clear goals

Support infrastructure deployment

Focus on spectrum allocation and use, not auction revenues

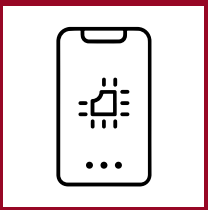
Modernise regulation

Adopt functionality-based, technology-neutral regulation

Favour ex-post approaches over ex-ante prescriptive regulation

Apply regulations consistently across the digital ecosystem

Promote 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

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.

Artificial intelligence

Background

Artificial intelligence (AI) is being integrated in products and services at an incredible pace. As the development and adoption of AI has increased, governments have become highly engaged, considering how this technology could be best used to benefit the economy and society while also managing potential risks.

The governance of AI varies, reflecting differences in government priorities, from digitalisation, to risk management, to economic growth. The EU was the first to agree on broad AI legislation focused on transparency, accountability and human rights. The United States is taking a market-driven approach through significant investment in infrastructure and public-private partnerships. China has a state-centric model with technology-specific laws enforcing strict government oversight and control. Meanwhile, countries such as Singapore are promoting international collaboration and responsible innovation through shared governance frameworks aligned with internationally agreed principles.

The telecoms sector plays a crucial role in the development and use of AI, providing high-speed, low-latency connectivity between users, data centres and cloud services – all of which are essential for a reliable AI ecosystem.

Telecoms operators also capture high-quality, localised network metadata and customer behaviour data that can be used to design and train AI products and services for enhanced public services, to increase industrial capacity and for AI research and development.

Operators themselves use AI in many aspects of their business, including for network and traffic optimisation, security (such as fraud and scam detection), energy efficiency and edge-computing integration. As use cases are still emerging it is important innovation isn't stifled by overly burdensome or technologically outdated regulation.

To leverage AI for the welfare of people and the planet, it is crucial that AI be designed, developed and deployed with ethical considerations in mind and respecting the rights of consumers, including their right to data privacy. To this end, the mobile industry has adopted principles for responsible AI (RAI): fairness, human agency and oversight, privacy and security, safety and robustness, transparency and explainability, sustainability and accountability. These are in line with internationally agreed principles such as those developed by the OECD and UNESCO. To support operators in realising these principles, the GSMA has developed a range of practical tools, offering clear steps to implement RAI across their organisations.

Debate

How can legislators, regulators and the AI ecosystem, including MNOs, engage effectively to support and contribute to the AI transformation?

What governance framework strikes the right balance between ethical and responsible development and use of AI, while fostering innovation and technological development?

What kinds of policies can foster a thriving AI ecosystem while ensuring responsible use of power and preventing abuse of dominance?

Resources

The Mobile Industry and AI, GSMA, 2023
AI for Impact website, GSMA
The GSMA Responsible AI Maturity Roadmap
Distributed inference: how AI can turbocharge the edge, GSMA Intelligence, 2025

Industry position

As the development and adoption of AI accelerate, policymakers, regulators and industry must work together to realise the benefits in a responsible and sustainable way.

It is important that governments facilitate investment in the AI ecosystem, including the infrastructure that enables it, such as telecoms networks, to maximise opportunities for society and the economy.

Governments should prioritise research and development and incentivise partnerships across the AI ecosystem to ensure innovation and future competitiveness. They should also foster an environment that attracts and cultivates AI talent, while expanding digital skills programmes to help citizens and industry keep pace with rapidly evolving AI technology. Governments can also adopt AI to enhance public services, such as infrastructure planning, health care and disaster response.

Creating a clear and consistent policy environment that encourages the development and use of AI is vital. Using shared governance frameworks based on internationally agreed principles for AI can support the global harmonisation of rules. Policymakers should work with industry, including through collaborative governance mechanisms such as time-limited regulatory sandboxes, to allow new ideas and emerging technologies to be tested. To ensure that regulation keeps pace with technological advances, investment in institutional capacity building is recommended to equip policymakers and regulators with up-to-date knowledge and global best practices. This will shape more informed and evidence-based policy responses.

By pursuing these actions, policymakers and regulators can help create an environment in which AI innovation thrives, delivering long-term social and economic benefits while ensuring the technology is used responsibly and ethically.

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, 2018

Efficient mobile market structures

Background

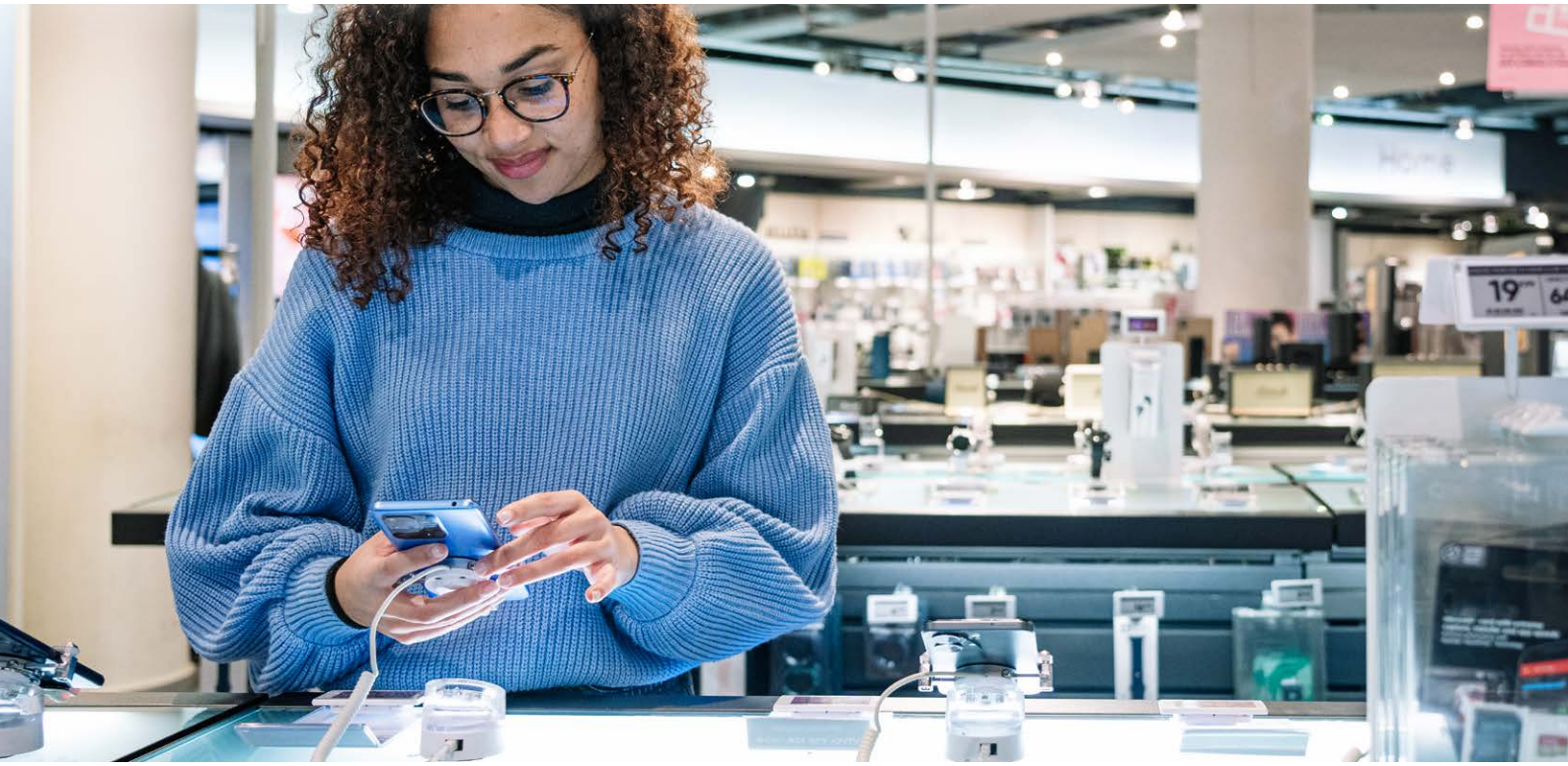
From the outset, mobile markets have been characterised by a vibrant, competitive market structure that drives investment and innovation.

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

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

Electromagnetic fields and health

Background

Research into the safety of radio signals has been conducted for several decades and informed the human exposure limits that have been set to protect all people from established health risks.

The World Health Organization (WHO) and International Telecommunication Union (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 and future wireless technologies.

There is strong consensus among expert groups and public health agencies, including the WHO, that there are no established health risks from exposure to the radio signals of mobile devices and mobile network antennas that comply with international safety recommendations. A comprehensive health risk assessment of radio signals is being conducted by the WHO.

However, some early research suggested a possible increased risk of brain tumours among long-term users of mobile phones. As a result, 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 that if they are concerned, they can reduce their exposure by 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.

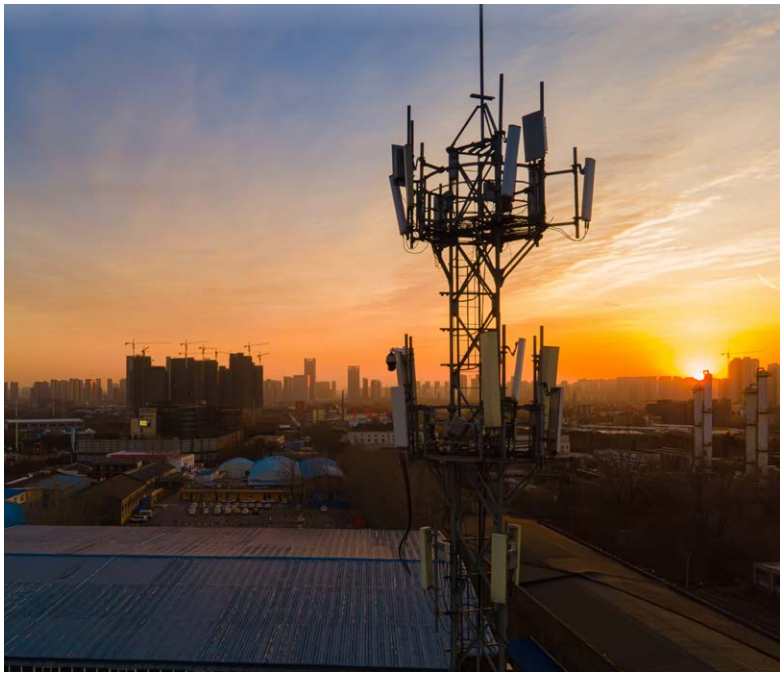
For mobile networks, whether 2G, 3G, 4G or 5G, typical levels in publicly accessible areas are a small fraction of the exposure limits and similar to broadcast services.

Debate

Does using a mobile phone regularly, or living near a base station have adverse 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 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 on the siting of masts, balancing effective network roll-out with consideration of public concerns.
- Accept mobile operators' declarations of compliance with international or national EMF limits based on the technical standards of 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.

The current WHO position is that international safety guidelines protect everyone in the population with a high safety factor, and that there is no scientific basis to restrict children's use of phones, or the locations of base stations. The GSMA encourages 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 address public concerns about mobile communications. Adoption of evidence-based national policies on 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, 2021
International EMF Exposure Guidelines, GSMA, 2021
Safety of 5G Networks website, GSMA
5G EMF Surveys, GSMA interactive map
Mobile Technology Evolution, 2025, GSMA

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.

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 can limit 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 (PPPs)

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.

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 or provide the infrastructure to deploy commercially viable networks.

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 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.

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 GSMA (2016), Unlocking Rural Coverage: Enablers for Commercially Sustainable Mobile Network Expansion. As 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

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 that 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

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 profit.
- 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 Taxation website

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. 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?

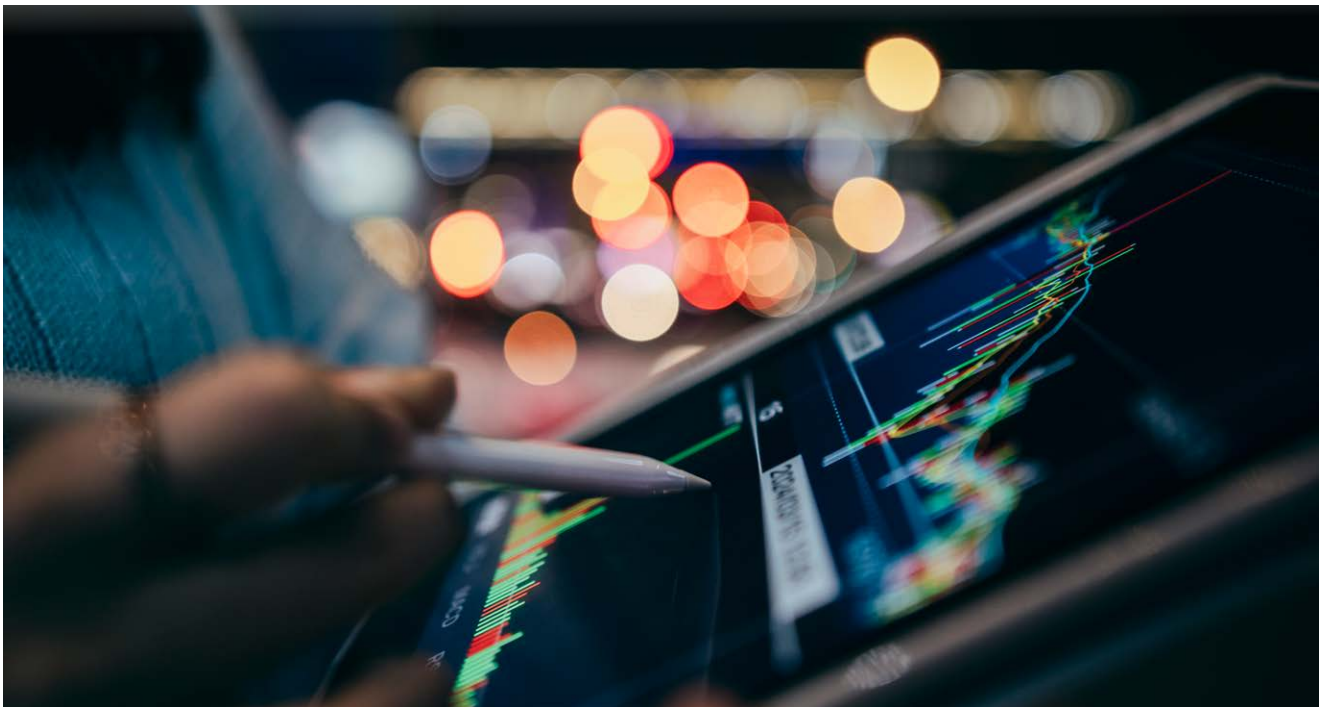
What alternative strategies can governments employ to enable the private sector to expand connectivity?

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.



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

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

Universal Service Funds in Africa, 2023

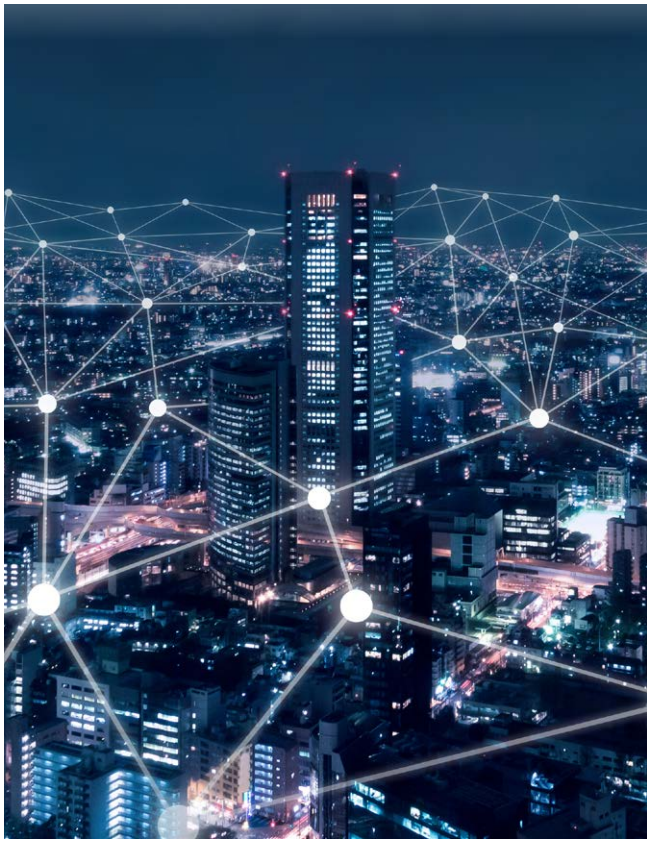
2 The evolution of spectrum

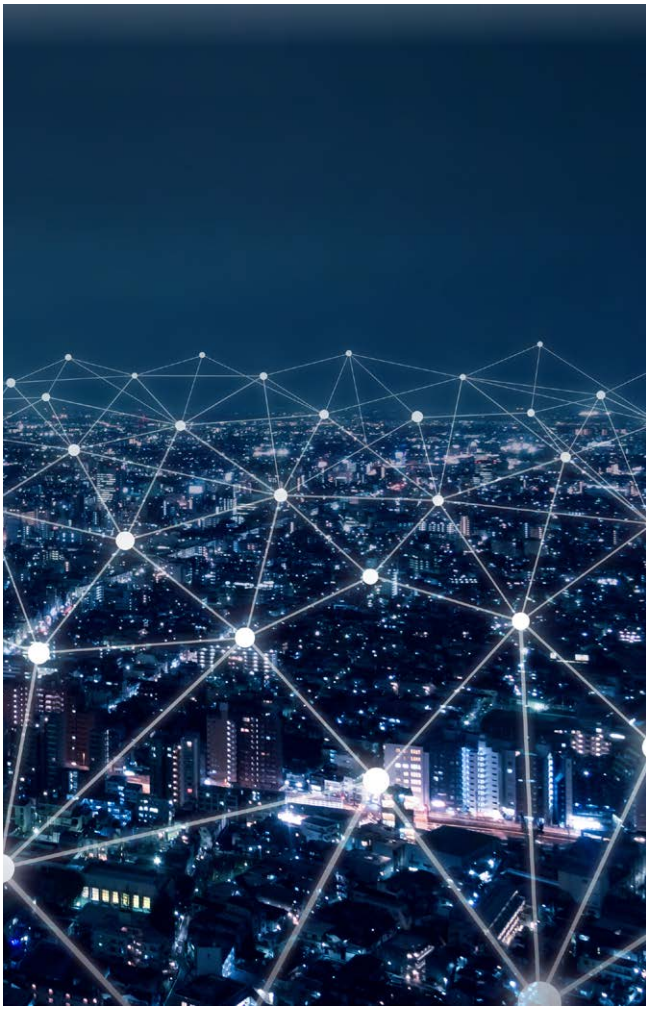
Effective spectrum policies encourage the investment required to enhance the quality and range of mobile services. Efficient use of spectrum can help reduce carbon emissions while simultaneously generating economic benefits for society and narrowing the digital divide.

To maximise this impact, long-term planning and short-term action are required in several areas. Adherence to international standards and regulatory best practices can create an environment that fosters innovation in mobile services, long-term commercial investment and healthy competition.

Governments should ensure there is sufficient licensed spectrum through planning and roadmap development, avoiding fragmentation and, importantly, guaranteeing technology neutrality in spectrum assignments. These policies can help ensure access to sufficient capacity, provide predictability and avoid costly restrictions on spectrum use.

Policies on spectrum pricing have a significant impact as lower spectrum prices are linked to faster download speeds and better coverage. Government pricing mechanisms should aim to enable broadband development, not to maximise profits, as this could deter investors and undermine competition in communications markets.





Mobile spectrum needs

Background

Governments can support mobile development by having a long-term vision of the spectrum access that mobile operators will receive.

Mobile networks operate across an evolving range of technologies, from 2G to 5G and, in the future, 6G. Growing demand for data has required wider spectrum channels, with channel sizes increasing four to five times every generation. While 2G voice applications used small tranches of spectrum to deliver voice and SMS, 5G usage requires 100 MHz data channels. 6G, which will provide capacity for mass-market augmented reality (AR), intensive AI use and other new applications, will use 200–400 MHz channels.

New generations of technology are always designed to use the spectrum of previous generations, but more bandwidth in wider channels is required alongside increased data. 2G and 3G are used in fewer and fewer markets, and these network sunsets allow spectrum to be refarmed for more efficient technologies, such as 5G.

5G supports higher network capacity and faster mobile broadband speeds than previous generations – essential to meet high-user demand for today's data-heavy mobile applications, such as on-demand video. 6G will build on 5G and the next phase in its evolution, 5G-Advanced.

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

- Enhanced mobile broadband (eMBB)
- Ultra-reliable and low latency communications (URLLC)
- Massive machine-type communications (MMTC)
- Fixed Wireless Access (FWA)

Mobile services depend on access to spectrum to build cost-effective networks. Robust licensing and timely availability of spectrum is also vital to the success of mobile deployment. With these in place, mobile 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 bands, regional and global harmonisation (the uniform allocation of radio frequency bands under common technical and regulatory conditions) have created economies of scale that have made mobile services and handsets more affordable.

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

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

As spectrum needs for licensed mobile in wider channels increase, how can regulators meet spectrum demand for mobile capacity and which harmonised bands can be used?

Industry position

Mobile technologies require harmonised mobile spectrum. Governments should carefully consider spectrum demands 10 years into the future. As data traffic continues to increase and new, innovative use cases take off, more spectrum across the low-, mid- and high-bands will be needed.

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. Meeting spectrum needs in this range is vital to the future of mobile and requires policymakers to formulate a clear spectrum roadmap. An average of 2–3 GHz of mid-band spectrum will be required in the 2035–2040 period to meet demand in high-population density locations around the world. 200-400 MHz channels will be required for 6G.

An average of 5 GHz of high-band spectrum will be needed in mature 5G markets by 2030, while countries just starting their 5G journey should seek 3.5 GHz of high-band this decade. High-band spectrum complements low- and mid-band 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 (below 1 GHz) is vital to giving rural communities equitable access to comparable urban mobile services, and expanding its capacity as far as possible can advance digital inclusion. Countries that have assigned a greater amount of low-band spectrum have also achieved higher speeds in rural areas. Furthermore, each 50 MHz of sub-1 GHz spectrum is associated with a 7 percentage point (pp) increase in 4G coverage and a 11 pp increase in 5G coverage, with a more pronounced impact than higher bands

Resources

Spectrum and Rural Connectivity, GSMA, 2026
Vision 2040: Spectrum for the future of mobile connectivity, GSMA, 2025
Vision 2030: Low-Band Spectrum for 5G, GSMA, 2022
Vision 2030: mmWave Spectrum Needs, GSMA, 2022
5G Spectrum Public Policy Paper, GSMA, 2025
Vision 2030: Insights for Mid-band Spectrum Needs, GSMA, 2021

Spectrum harmonisation

Background

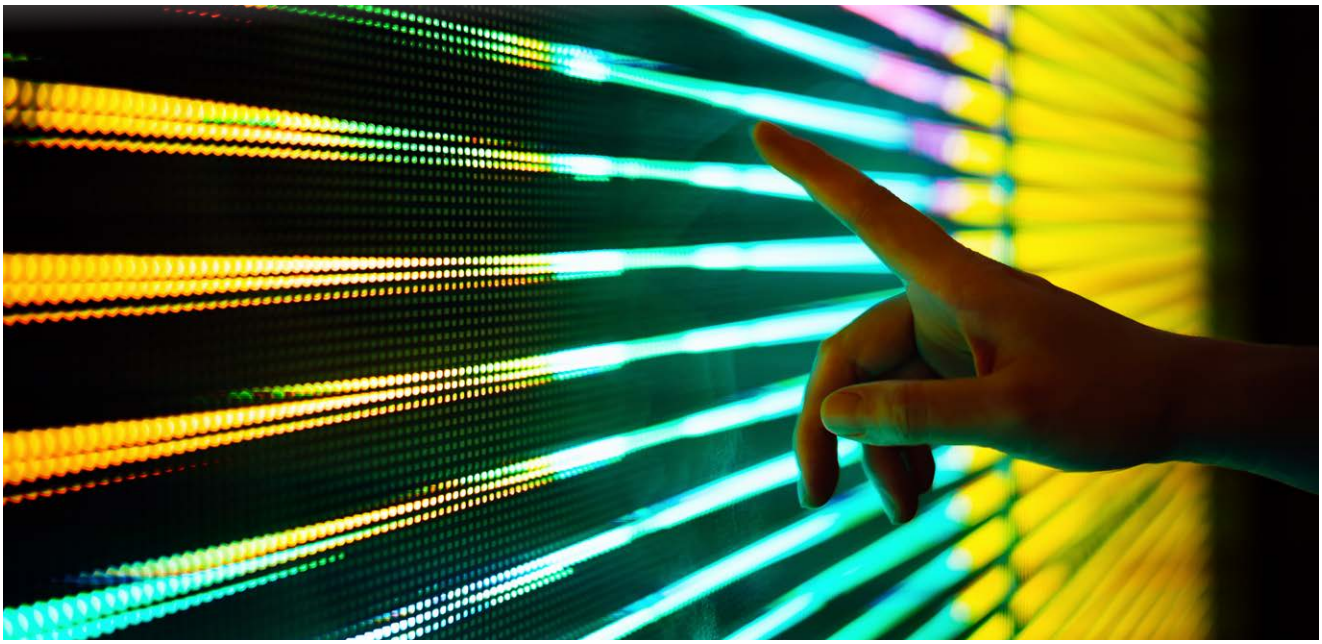
Spectrum harmonisation is the uniform allocation of radio frequency bands under common technical and regulatory conditions, across regional blocs or globally. Adherence to internationally identified spectrum bands has many advantages:

- 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. The first step in 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 instrumental to the success of harmonisation. At WRC-23, for example, agreement was reached on harmonising the 3.6–3.8 GHz and 6 GHz bands. In 2019, mmWave bands were discussed and the harmonised use of 26 GHz, 40 GHz and 66 GHz was agreed.

However, countries develop their communications systems at different rates, and negotiations at the International Telecommunication Union (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 was clear at 5G launches when the portion of the 3.5 GHz range harmonised at WRCs proved insufficient for most countries. Today, as much as 700 MHz is available in this spectrum band in some countries. WRC-27 may advance harmonisation of the 6 GHz band, but it remains to be seen whether the use of this band will outstrip agreements at the ITU.



The road to WRC-27

The WRC-27 cycle includes looking at some new spectrum for mobile: 4.4–4.8 GHz, 7.125–8.4 GHz, and 14.8–15.35 GHz. These bands will enable the new generation of mobile connectivity in the 2030s.

In addition to possible new mobile bands, the WRC-27 agenda will consider studies on other radio services, including satellite direct-to-device (D2D) connectivity between satellites and mobile devices to supplement terrestrial network coverage.

Debate

What planning tools, spectrum needs forecasts or technology analyses 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 several cycles. 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, multi-regional harmonisation has been broadly achieved by loose consensus based on equipment availability. However, this approach risks leaving later-adopting 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 band for mobile use.

At minimum, the 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

WRC-27 and WRC-23 website, GSMA
Mobile evolution: spectrum for 6G, GSMA, 2025

Spectrum licensing

Background

Spectrum licensing terms affect investment in networks and the delivery of high-quality mobile services. The amount of spectrum made available, and the conditions under which it is licensed, drive the cost and quality of mobile services for end users.

Mobile is a capital-intensive industry requiring significant investment in infrastructure. Positive spectrum licensing policies, supported by a stable, predictable and transparent regulatory regime, can encourage investment in mobile. Such policies include roadmaps that outline the release of new spectrum in harmonised mobile bands, licences that carry a presumption of renewal at the end of their initial terms and the right terms and conditions for the use of any assigned spectrum (which are limited to guaranteeing coexistence among users). The use of technology-neutral spectrum should be encouraged through licences that enable spectrum to be redeployed as technology and market conditions change.

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 investments so that mobile access is expanded, capacity increased and the range of services enhanced.

Recommendations on licence terms and conditions:

- Spectrum licences should be technology-and service-neutral (see below).
- Governments should adopt regulation that encourages the commercial provision of widespread and affordable access rather than imposing licence conditions.
- Authorities should limit conditions on the use of spectrum to those necessary, to guarantee coexistence.
- 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, and a presumption of renewal at the end of the term.

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, 2022

Spectrum Licensing website, GSMA

Approaches to assigning spectrum

Background

Licensed spectrum is necessary for mobile services to provide quality service and customer value. It facilitates the investments needed to deploy mobile networks widely.

The licensing of spectrum bands for mobile services should follow international harmonisation, which delivers lower-cost devices and equipment through economies of scale. Exclusive licensing has been central to the success of mobile, and any spectrum-sharing mechanisms should be considered only as a complementary possibility.

Auctions

Auctions are an efficient way to assign spectrum when there is competition for scarce spectrum and when demand is expected to exceed supply. Careful planning is needed, as excessively high reserve prices may result in unsold spectrum or less investment.

There are several auction designs to choose from, each with its own strengths and limitations. The best choice depends on market conditions and the objectives of governments and regulators, but above all, it is the conditions of the auction (reserve prices and obligations through terms and conditions) rather than the methodology that determines success.

For governments, which set the wider policy objectives for spectrum, considerations could 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 assignment process.

For regulators, which are charged with ongoing spectrum management, 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, where no competitive bidding process is held, 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 are sometimes considered part of an administrative assignment – a so-called "beauty contest" – include coverage, service quality and a variety of social and economic goals.

Administrative assignments carry 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 in advance the penalties that will be imposed if commitments are not met.

Debate

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 assignment is necessary to realise the full economic and social value of mobile. Auctions are the main approach to assigning the right to use a particular spectrum band, but administrative assignments (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 selects a shortlist of bidders based on administrative criteria and then holds an auction to assign the licence.

Auctions work best when there is excess demand for spectrum and they help select mobile operators most likely to use their spectrum assignment for the greatest 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.

Whichever approach is taken, 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, 2022
Auction Best Practice, GSMA, 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 mobile operators to cease investment in network development and to compete less to grow their customer base. 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, and each market needs to be considered independently with industry stakeholders involved at every stage of the decision-making process. As licensees make significant investments in spectrum, a presumption of renewal encourages continued investment. Failure to manage the process effectively, in addition to investment in new services, can potentially affect mobile services for millions of consumers.

Presumption of renewal

The presumption of renewal provides a stable environment for mobile operators by offering certainty on future investment in the sector. This tool minimises customer service disruption, as operators are not forced to reconfigure their networks or exit the market due to spectrum loss. When combined with spectrum trading, it can also support efficient long-term spectrum use.

To maintain market confidence and continuity, it is advised to minimise uncertainty by creating a presumption of renewal, except when there are serious breaches or prolonged spectrum inactivity.

Re-auctioning should be avoided as it can discourage long-term investments and cause disruption for users and existing businesses, especially if current operators lose critical spectrum holdings. Furthermore, high auction prices can undermine investment potential due to increased licence costs.

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. The only exceptions to this are where 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.

Fees for spectrum renewal should not be tied to historical spectrum prices, as the underlying value of spectrum has declined over time. Renewal fees contribute to the overall cost burden of spectrum, which may have a negative effect on affordability and access. A well-designed spectrum trading framework provides incentives for market efficiency without imposing additional financial pressure on operators.

To promote efficient use and maintain service standards, regulators could consider granting spectrum renewals in exchange for investment commitments to improve coverage or service quality. Alternatively, an administrative review process may be a more cost-effective approach to ensuring spectrum remains in productive use, balancing regulatory oversight with economic efficiency.

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, 2022
Global Spectrum Pricing, GSMA, 2025
The year of spectrum renewals, GSMA, 2025

Spectrum sharing, leasing and trading

Background

Growing data traffic leads to a greater spectrum requirement for mobile services. These increased requirements can be supported by spectrum management policies that improve the efficiency of spectrum use and ensure it is properly implemented, even in areas where coverage is required but there is no commercial benefit. However, completely clearing new frequency bands for future mobile use has become increasingly difficult.

Spectrum sharing, on the other hand, allows mobile operators to access the same frequency bands under certain conditions, improving overall spectrum efficiency. When two operators share spectrum, they agree to use a licensed band jointly, often to reduce costs and extend coverage, particularly in less populated or rural areas. Effective operator-to-operator sharing supports network expansion, reduces duplication of infrastructure and promotes better use of scarce spectrum resources without compromising competition.

Spectrum leasing involves a licence holder temporarily transferring usage rights to another party without relinquishing ownership. This gives operators the flexibility to manage capacity needs and expand services in specific areas or time frames. Leasing arrangements must be regulated to ensure transparency and protect competition.

Spectrum trading refers to the permanent transfer of spectrum usage rights between entities, usually through a market-based mechanism. Trading helps ensure spectrum is used by those who value it most and can use it efficiently, which encourages investment and innovation. Clear rules, regulatory approval and a transparent process are essential elements of effective spectrum trading.

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

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

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

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

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

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, 2022
Harnessing Spectrum Diversity, GSMA, 2025

Recommendations on spectrum sharing, leasing and trading:

- Licensing authorities should allow voluntary spectrum sharing, leasing and trading among mobile operators and facilitate these mechanisms through clearly defined spectrum rights, long licence terms and limited administrative costs.
- Authorities should only be notified of the agreements taking place so that it is clear who holds spectrum usage rights. Notification enables authorities to assess whether a proposed trade would pose any risks to competition.
- Before a formal spectrum secondary market framework is established, authorities should be prepared to assess proposals for sharing, leasing and trading subject to consultation, and consider risks to competition or of interference.
- Transparent and well-timed licence renewal processes, and information on spectrum availability, pricing and conditions, will facilitate sharing, leasing and trading.
- Competition issues should be assessed based on the specific circumstances of each sharing, leasing and trading agreement.
- Long licence terms allow the buyer or lessee of the rights to invest in using the spectrum.
- Licensed and unlicensed spectrum can have complementary roles in connectivity. Licensed spectrum is typically used to cover wide areas and reach a high number of users, while unlicensed use can support local solutions.

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 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 regulators and governments. Users benefit from better mobile broadband coverage, higher data speeds and lower mobile data prices than they would otherwise.

Service neutrality is also important to unlock the potential of technology-neutral licensing. Where the latter exists but not the former, operators have limited ability to refarm their spectrum holdings for newer technologies and other types of service to maximise spectrum and meet market demand for new mobile-enabled solutions, such as FWA.

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

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.

Regulators should not delay the introduction of technology neutrality until licences are up for renewal, and they should also update the terms of existing licences.

Spectrum assignment decisions should be guided by the desire to enable new mobile technology, not to extract additional revenue, which could hinder innovation.

Service neutrality is necessary to unlock the potential of technology-neutral licensing.

The decision to allow, and actively support, technology neutrality is being made easier by technological advancements. 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 demand for mobile broadband, while also supporting legacy users by limiting the band in use or the geographies it serves. For regulators, this means they no longer need to worry that refarming would leave legacy users unserved.

Resources

Technology-Neutral Spectrum and Legacy Network Sunsets, GSMA, 2023
The digital age depends on technology-neutral spectrum licensing, GSMA, 2025

Spectrum pricing

Background

The primary goal of charging a fee for spectrum is to award it to those who will use it most efficiently to deliver maximum benefits for society. 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, since charging for spectrum also provides state revenues, governments sometimes 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, a lack of clarity on future releases or unknown renewal processes for expiring licences. Such factors can create uncertainty or artificial scarcity and encourage mobile operators to bid above their true valuation of the spectrum licences on offer.

On average, global cumulative spectrum costs now account for 7% of mobile operator revenues – a 63% increase over the past 10 years. In the worst-case scenario, spectrum prices can account for 25% of operator revenues.

Increased spectrum cost therefore has an impact on consumers. A 10-percentage point lower spectrum cost-to-revenue ratio leads to coverage of up to six percentage points higher. This effect has been observed for both 4G and 5G coverage. There is a similar negative effect on network speeds whereby a 10-percentage point lower spectrum cost has a positive impact on download speeds of 8%.

Debate

Telecoms regulators increasingly recognise the positive impact of lower spectrum prices, but governments are not always easy to convince. How can regulators and mobile operators work together to highlight the benefits of affordable spectrum to relevant levels of government?

Industry position

Spectrum is a valuable asset, but a long-term vision is needed to maximise its value. The primary goal of 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 struck the right balance between increasing revenues and awarding efficient spectrum.

Recommendations for spectrum pricing and fees:

- Spectrum prices should promote the optimal use of spectrum for the benefit of society.
- Low spectrum fees increase the funds available for investment and have a positive impact on the quality 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 set renewal fees to recoup administrative costs and ensure licences have a presumption of renewal.
- Costs related to licence conditions or obligations should be deducted from spectrum fees.
- Regulators can consider lower spectrum prices in exchange for investment commitments to improve coverage or service quality.

Resources

Global Spectrum Pricing, GSMA, 2025

Spectrum Pricing Explained, GSMA Intelligence, 2025

Spectrum for enterprise

Background

The digitalisation of industry is a priority for every country as governments seek to deliver economic growth. Simultaneously, enterprises seek to enhance productivity and streamline their businesses through effective access to connectivity.

Approaches to providing connectivity for enterprise and local networks have varied, and the use of public spectrum resources must benefit businesses and consumers simultaneously. Interventionist approaches such as spectrum set-asides should be avoided in favour of licensing mechanisms that let public mobile flourish alongside government and enterprise digitalisation.

Enterprise and government uses of spectrum include smart utility grids, industrial automation, 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 the 5G era of digitalisation.

Policymakers play a vital role by managing the spectrum that underpins these developments, and 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. Private networks do not necessarily depend on set-aside spectrum or local licences. Instead, these networks are widely provided through mobile operator licences using network slices or through bespoke infrastructure on nationally licenced spectrum. Set-asides that favour a particular category of licensee are an aggressive regulatory tool that has an economic cost and can be avoided with best-practice licensing.

Debate

Spectrum access is critical as governments focus on policies that encourage both enterprise (e.g. smart factories) and government (e.g. smart cities) digitalisation. How can governments and regulators develop spectrum policies that support private and local mobile networks without negatively affecting commercial 5G services?

Resources

Best Practice in Mobile Spectrum Licensing, GSMA, 2022
Spectrum Policy Trends 2023, GSMA, 2023
Spectrum for Digitalisation, GSMA, 2025

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. Mobile bands should be assigned fairly and efficiently.

Spectrum set-asides for government or enterprise use 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 lower network investment, slower rollouts, limited coverage and reduced data speeds. Where industries require access to specific licensed bands, they can do so, for example, via sharing and leasing agreements with mobile operators.

The following considerations should inform spectrum policy decisions about private networks:

- Well-designed licence conditions are the least intrusive mechanism for providing spectrum for enterprise or government users.
- Spectrum set-asides do not incentivise digitalisation, but can harm public mobile.
- Spectrum sharing has limitations but may be used if necessary.
- Above all, regulators need to ensure that enough spectrum is available in harmonised bands via a balanced and transparent process.
- 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.

Satellite direct-to-device (D2D)

Background

Direct-to-device (D2D) describes connectivity between satellites and mobile handsets. The use of satellite connectivity as part of a mobile network can supplement a terrestrial operator's network coverage. Providing this broader coverage layer can help mobile reach farther into sparsely populated or inaccessible locations. D2D infrastructure can also provide an added layer of network resilience: signals from satellites can still be received in the event of a terrestrial network outage, including support for emergency services where terrestrial networks fail. D2D can provide connectivity after natural disasters and digitally empower crisis-affected communities during humanitarian interventions.

Today, 58% of the world's population is connected to mobile broadband. D2D can improve resilience and supplement services when users travel to areas with no connectivity, such as deserts, oceans, mountains or national parks. It can also help connect those who live outside a mobile broadband network – approximately 4% of the global population (the coverage gap).

However, policies on supplemental satellite services should go hand in hand with other policy reforms to connect the 38% of the global population that live in an area covered by a mobile network but who are still not connected (the usage gap). The usage gap is the result of a lack of affordability and digital literacy, among other factors. Regulation that addresses both issues can deliver the mobile industry's vision of connecting everyone.

D2D can provide a valuable supplemental technology for the mobile industry, new business for the satellite and mobile sectors and improve resilience and extend access to services for end users. Governments should allow mobile operators to deploy D2D services in partnership with satellite operators.

D2D operations can use two spectrum categories: in frequency bands used by mobile services and in bands already allocated for mobile satellite service. Both types of D2D operations are available today. They both provide SOS and SMS capabilities, while D2D using mobile spectrum also offers data. Satellite's strength lies in its ability to reach remote areas. It cannot provide the capacity that terrestrial mobile networks can deliver, but with the correct regulation, D2D can supplement terrestrial mobile coverage.

Regardless of the spectrum used, D2D's largest obstacle is its technical limitations. The larger footprint of satellite beams compared to terrestrial cells limits the amount of data that can be delivered in any area. Free space pass loss is also significantly higher and these two factors impact network quality. Therefore, D2D use will be limited in densely populated areas and indoors.

Debate

D2D-capable satellite capacity is already online, and more bandwidth is expected soon. Governments see an immediate need for D2D but have no international guidelines until WRC-27. How can D2D be safely implemented in the short term?

Resources

Spectrum for D2D Policy Position Paper, GSMA, 2025

Industry position

D2D must protect mobile networks, which are used by 5.8 billion unique mobile subscribers. Any approach to introducing D2D should be based on regulatory and technical conditions that ensure coexistence with mobile terrestrial networks.

D2D operating in mobile spectrum bands provides a supplemental service to terrestrial networks and enables mobile operators to collaborate to extend coverage under commercial arrangements with satellite network operators. With the regulator's permission, this should be done through the spectrum licence of the mobile operators.

Regulator interest in D2D is growing as its use in mobile spectrum has been trialled successfully around the world, and plans have been announced to launch more satellite capacity for D2D. WRC-27 will consider creating an international framework to facilitate the development of D2D services. Where regulators plan to introduce D2D services soon, they may need to define cautious national regulatory frameworks for D2D in mobile spectrum.

Where in-country regulations allow the operation of D2D using satellite spectrum, technical and regulatory provisions to address possible interference already exist in the ITU Radio Regulations. In this case, satellite service providers must meet all eligibility and any other legal requirements of national legislation. Some regulations may need to be updated (e.g. to include low-earth orbit satellite constellations), and "same services, same rules" regulations must always apply. When using mobile satellite spectrum, the licence holder will typically be an entity separate from the mobile operator (e.g. a specialised satellite network operator). The service would then operate under the technical requirements of the satellite spectrum licence.

As a result of this separate licensing regime, it may not be necessary for the satellite operator to enter a partnership with a local mobile provider. However, services may be easier for users to adopt if satellite operators have commercial partnerships with mobile operators at the wholesale level, rather than trying to compete with them in the retail market.

3 Consumer protection

As mobile services have taken on greater economic and social importance, particularly mobile internet, it is vital that the more than 5 billion people currently using 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 the potential risks and aware of the steps they can take to reduce those risks.

The mobile industry takes consumer protection very 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. They do this by:

- Defining, sharing and promoting global best practice.
- Building and ensuring participation in multistakeholder forums.
- Educating consumers and businesses about the safe use of mobile technologies and applications.
- Commissioning research that offers real-world insights and evidence.

The following sections highlight efforts 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 people (children and teenagers) are enthusiastic users of mobile technology. Their knowledge of mobile apps and platforms often surpasses that of their parents, guardians and teachers.

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 more embedded in everyday life, mobile operators have an important role to play in protecting and promoting children's rights.

For young people, mobile devices can be key to accessing:

- Employment skills.
- Enhanced formal and informal education and learning.
- Information and services to support 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 steps to support the safe and responsible use of mobile services by young people. The GSMA plays a leading role in voluntary industry initiatives, including multistakeholder task forces.

Debate

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

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

Industry position

Mobile devices and services can 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.

Encouraging and enabling the safe, positive and responsible use of mobile by children and young people is best approached through multistakeholder efforts that include young people themselves.

Working closely with its partner UNICEF, its mobile operator members and a range of other stakeholders, including young people, the GSMA works to support children's rights to, through and in the digital environment. 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 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

Bringing Youth Perspectives into the Business of Connectivity, GSMA, 2025
Enhancing Children's Lives Through Mobile, GSMA, 2019
Internet Safety Guides, GSMA and Child Helpline International, 2017
Research Results, Global Kids Online

Cross-border flows of data

Background

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

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, the EU Binding Corporate Rules (BCRs) and the OECD Data Free Flow with Trust (DFFT), 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 the use of local technology. Such localisation requirements can be found in a variety of sector- and subject-specific rules.

These 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. 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 forums include the Global Cross-Border Privacy 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), EU BCRs, Model Contractual Clauses (MCC) and Privacy Trust Mark (PTM).

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?

How can governments collaborate to achieve evidence-based policy on data localisation?

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, EU BCR, MCC and PTM, 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. They 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

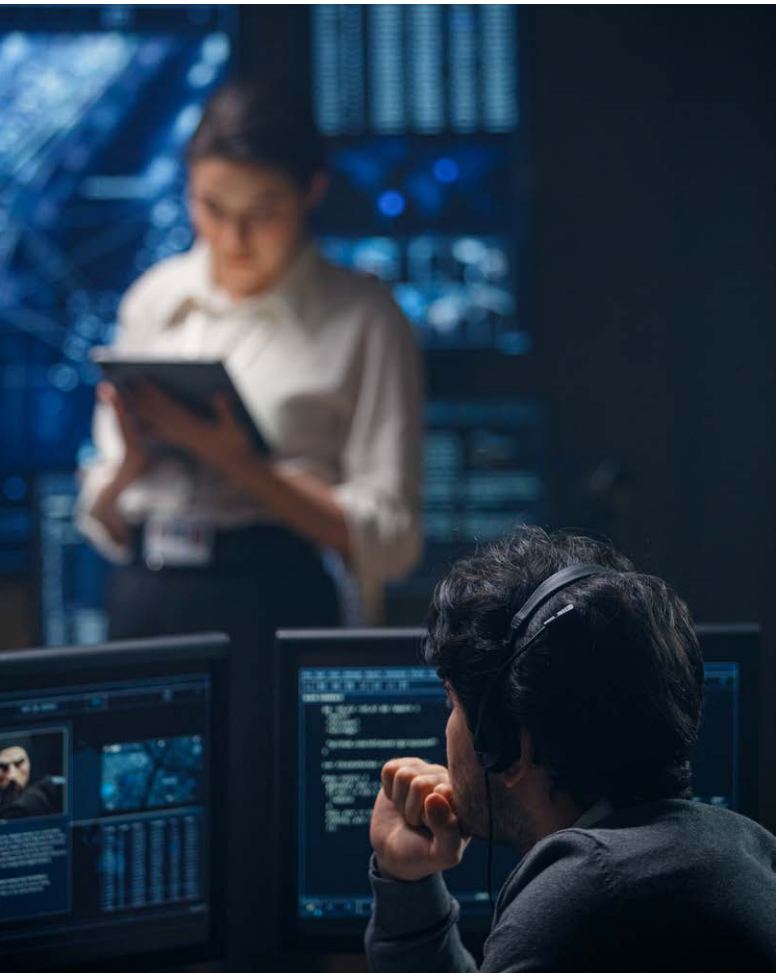
Cross Border Data Flows: The Impact of Data Localisation on IoT, GSMA, 2021
Mobile Privacy Principles, GSMA, 2016
Smart Data Privacy Laws, GSMA, 2019
Smart Implementation of Data Privacy Laws, GSMA, 2025
Data Free Flow with Trust website, OECD
Global CBPR Forum website

Cybersecurity

Background

The internet and mobile connectivity are becoming more pervasive, making it vital to ensure that individuals can use 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 their customers while also incorporating new features and enhancing existing security capabilities to minimise the potential for fraud, identity theft and other threats. This includes encryption, integrity checking and user identity validation. Governments and legislators have put requirements in place to prevent cyberattacks, and national and regional strategies have been adopted in many countries to strengthen resilience and build capacity to fight cybercrime.



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

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.

Protecting network infrastructure and devices

The mobile industry has a long history of providing secure products and services to customers. The GSMA and its members support the principles of "secure-by-design" being applied across the value chain, beginning at the very earliest stages of product development, so that security is built in as a fundamental and holistic aspect of design.

Protecting consumers from fraud

Fraudulent attacks take many forms, such as SIM swap, financial fraud, phishing, smishing or vishing, where victims are tricked into revealing sensitive personal information or making financial transactions. 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.

The mobile industry, supported by the GSMA, is extremely active in programmes to educate consumers and businesses on how to safely use mobile technologies and the applications they support to minimise illicit behaviour. The GSMA coordinates activities and leads industry-wide initiatives through the Fraud and Security Group (FASG), the Telecommunication Information Sharing and Analysis Centre (T-ISAC), 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.

Debate

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

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 that mobile infrastructure, products and services are protected appropriately.

Different types of cyberthreats have the potential to undermine the integrity of networks through unauthorised interception. This can be through hardware and software in the mobile value chain or through social engineering whereby 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 to dealing with cyberthreats 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, 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. Borders do not restrict cybersecurity, and it requires national and international cooperation, such as through the Convention on Cybercrime (the Budapest Convention) and the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention).

Resources

Mobile Telecommunications Security Landscape 2025, GSMA, 2025
Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, 2022
GSMA Mobile Cybersecurity Knowledge Base
GSMA Fraud and Security Group

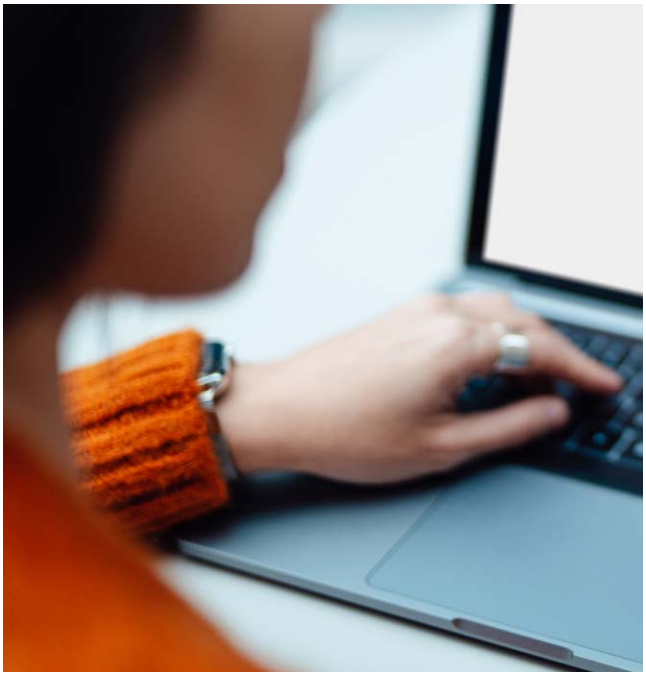
Data privacy

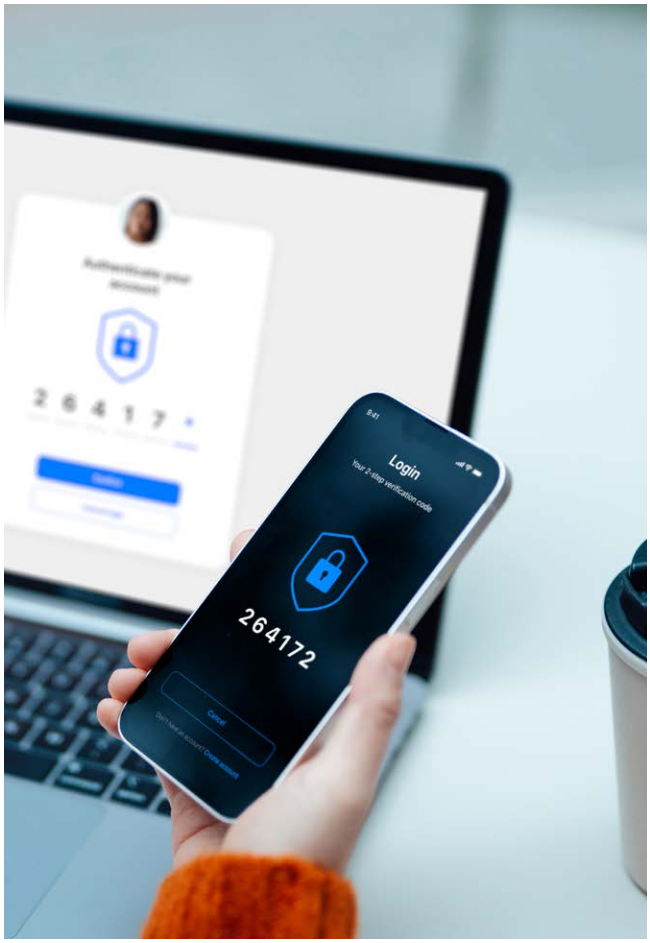
Background

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. In economies that are increasingly data-driven, lack of trust can be a barrier to growth.

One of the major challenges arising from 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 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 from 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 protection and implementation by supervisory authorities 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 ecosystem?

What role does self-regulation play in a continually changing technology environment?

What should be done to allow data to be used to support the social good and meet pressing public policy needs?

How can a risk-based approach play an important role in building trust?

Industry position

Currently, the wide range of services available through mobile devices offer varying degrees of privacy protection. For customers to be confident that their personal data is being properly protected, regardless of the 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 risk-based, 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 and the entire mobile ecosystem.

Resources

Implementation of Smart Data Privacy Laws, GSMA, 2025
Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, 2022
5G and Data Privacy, GSMA, 2020
Smart Data Privacy Laws, GSMA, 2019
Protecting Privacy and Data in the Internet of Things, GSMA, 2019
Mobile Privacy Principles, GSMA, 2016

Fraud and scams

Background

Fraud and scams are emerging as significant global threats, often by organised international criminal gangs. Despite not being responsible for perpetrating the crimes, mobile operators are usually the first point of contact for their customers when they are targeted through their mobile device and become victims.

To bypass a mobile network's technical defences, criminals use social engineering tactics to manipulate individuals who can be employees or consumers, into disclosing personal or sensitive information, or make financial transactions. The use of artificial intelligence (AI) allows criminals to deploy more sophisticated methods and widen their scope and scale to target diverse populations across different regions.

The impact of fraud and scams on victims can be significant. In addition to financial loss, the emotional distress and embarrassment leave many wary and reluctant to engage in the digital space. This erosion of trust can have a negative impact on consumers' quality of life because many services and interactions are online.

Legislators worldwide are responding to this issue through new laws and regulations. For example, the Australian Scams Prevention Framework sets out principles that regulated entities (banks, telecoms, social media companies) must comply with. Financial regulators, such as those in Africa and Singapore, are enforcing stricter authentication and know your customer (KYC) requirements for financial institutions and mobile money providers (MMPs) to reduce the likelihood of impersonation scams.

Mobile operators are investing significant resources in solutions that include firewalls, block lists and continuous system monitoring. The GSMA plays an important coordination role, providing platforms to share intelligence through the Fraud and Security Group (FASG) and Telecommunication Information Sharing and Analysis Centre (T-ISAC). The GSMA Open Gateway initiative and Scam Signal are helping to unite the mobile and financial services industries behind standardised technology solutions that can assist in combating this crime.

Debate

How should mobile operators and other organisations, such as law enforcement, financial institutions and social media/digital platforms, collaborate to effectively combat scams and fraud to reduce risk for end users and ensure criminals are prosecuted?

When legislating, how should governments address fraud and scams effectively and provide legal certainty, without discouraging industry efforts to innovate and invest in fraud prevention measures?

What measures should governments be taking to educate the public in staying safe online and reducing the risk of being targeted by scammers?

Industry position

The GSMA and its members are committed to tackling scams that exploit victims through the use of mobile technology and devices. Protecting consumers from scams requires the collective effort from everyone involved in the ecosystem, including mobile operators, digital platforms, financial institutions, law enforcement agencies, governments, regulators and individuals.

Legislation should target criminals who perpetrate illegal activity such as fraud and scams, while policies should be designed to allow investment in fraud prevention measures and not stifle innovation or the development and deployment of different technologies.

Collaborating, building partnerships and sharing actionable intelligence are all important for mobile operators to identify new threats and lead cross-sectoral initiatives to combat scams.

Multistakeholder efforts are required to encourage the safe and responsible use of mobile-based online services and devices. All participants in the mobile ecosystem – including banks, financial institutions and technology companies – have a responsibility to protect individuals, including educating them about safe behaviours and being vigilant.

Resources

Fraud and Scams: Staying Safe in the Mobile World, GSMA, 2025
Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, 2022
Mitigating Common Fraud Risks, GSMA, 2019
Mobile Money Fraud Typologies and Mitigation Strategies, GSMA, 2024
GSMA Open Gateway API Descriptions

Illegal content

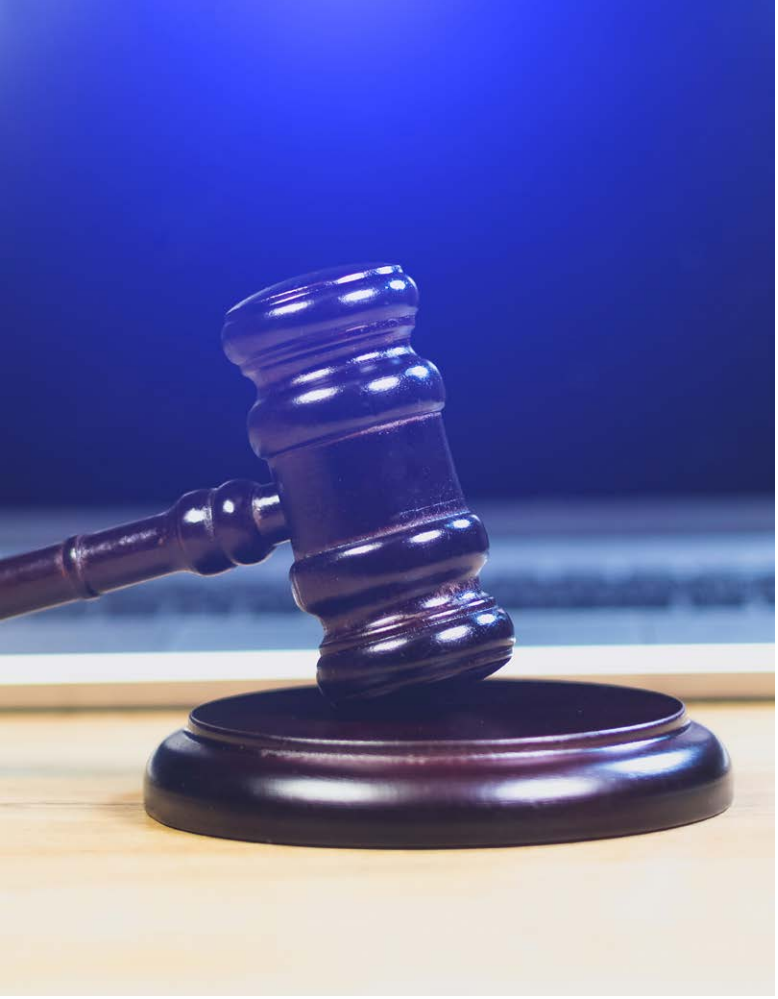
Background

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

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

Mobile operators are typically alerted to illegal content by national hotline organisations or law enforcement agencies. When content is reported, they follow procedures based on relevant data protection, privacy and disclosure legislation. In the case of child sexual abuse material, mobile operators use terms and conditions, notice and take down 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 material, 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 what 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 material. The GSMA Mobile Alliance to Combat Digital Child Sexual Exploitation provides leadership in this area and works to combat the misuse of mobile networks and services by criminals seeking to access or share child sexual abuse material.

Regarding copyright infringement and piracy, the mobile industry recognises the importance of proper compensation for rights holders and the prevention of unauthorised distribution.

Resources

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

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

Child Sexual Abuse Material: Model Legislation and Global Review, 10th Edition, International Centre for Missing and Exploited Children, 2023

INHOPE website

A Model National Response, WeProtect Global Alliance

Internet governance

Background

Internet governance involves an array of activities related to the policies and procedures for 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, other industry players and their customers.

Internet governance requires input and collaboration from diverse stakeholders with interest and expertise in technical engineering, resource management, standards and policy issues, among others. Stakeholder groups will vary depending on the internet governance issues 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 more agile and flexible ways than traditional government and intergovernmental mechanisms.

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

The decentralised development of the internet should continue outside the control of a particular business model or regulatory approach.

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

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 on their customers' mobile service use, including their personal data, and disclose it to law enforcement and national security agencies upon lawful demand. They may also require operators to intercept customer communications upon lawful demand, or to notify competent authorities before implementing features like end-to-end encryption that may prevent lawful access.

Such laws provide a framework for law enforcement and security service surveillance and guide mobile operators in their obligations. However, in some countries, there is a lack of legal and regulatory clarity on the disclosure of data or lawful interception of customer communications. This makes it challenging for the industry to protect the privacy of its customers' information and their communications.

Legislation often lags 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 Internet Protocol (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 related to government requests for disclosure of such data.

Debate

What is the correct legal framework to balance a government's obligation to ensure 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 government requests 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 using the proper processes and authorisations 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 support 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, 2015

Office of the Privacy Commissioner of Canada website

Investigatory Powers (Amendment) Act 2024: Response to Consultation

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 and 160 governments around the world had 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. In some countries, biometric data is also required for SIM registration, which can have additional privacy implications.

Some governments, including the Czech Republic, United Kingdom and United States, 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. These include 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 pragmatically and take local market conditions into account, such as the ability of mobile operators to verify customer IDs. If registration requirements are too onerous for a customer to meet, mandating a SIM registration policy may lead to implementation challenges and unforeseen consequences. For example, it could unintentionally exclude vulnerable and socially disadvantaged consumers or refugees who lack the required IDs. It might also lead to the emergence of an underground market for fraudulently registered or stolen SIM cards, driven by the desire of some mobile users, including criminals, to remain anonymous.

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 produce 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.

The GSMA urges 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 with 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

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

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

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

Access to Mobile Services and Proof of Identity, GSMA, 2020

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 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 if they are 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.

Mobile network operators 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

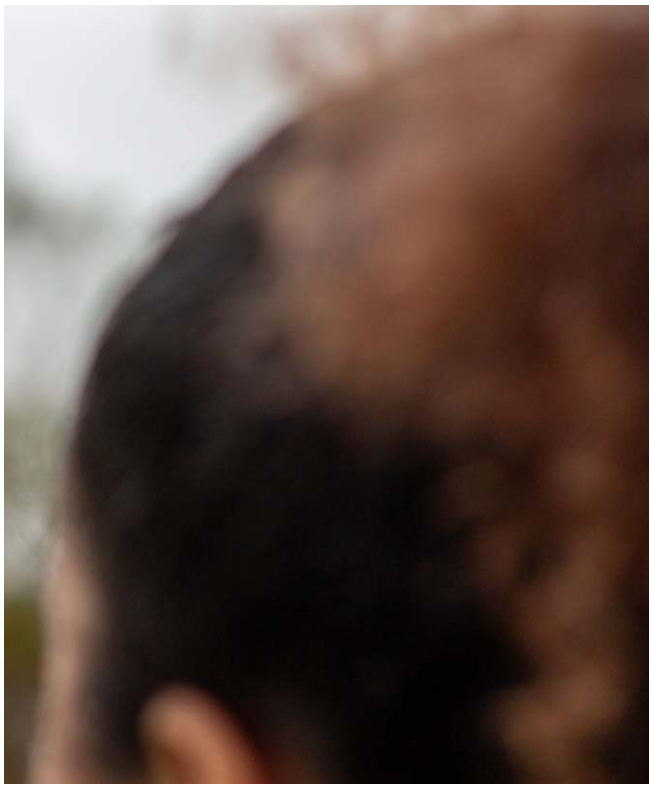
What factors and alternatives should governments consider before planning an SRO?

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 predefined circumstances, and only if absolutely necessary and proportionate to achieve a specified and legitimate aim 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, geographic scope, number of potentially affected individuals and businesses, functional scope and 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. Regardless, the SRO should always specify an end date. Independent oversight mechanisms should be established to ensure these principles are observed.

Operators can play an important role by raising awareness among government officials of the potential impact of SROs. They can also be prepared to work swiftly and efficiently to determine the legitimacy of the SRO once it has been received. This will help 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

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

GNI Submission to UN Human Rights on Internet Shutdowns, Global Network Initiative, 2022

GSMA Statement on Connectivity and Network Disruptions, 2021

Mitigating Network Shutdowns – Balancing Security and Rights, GSMA, 2025

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.

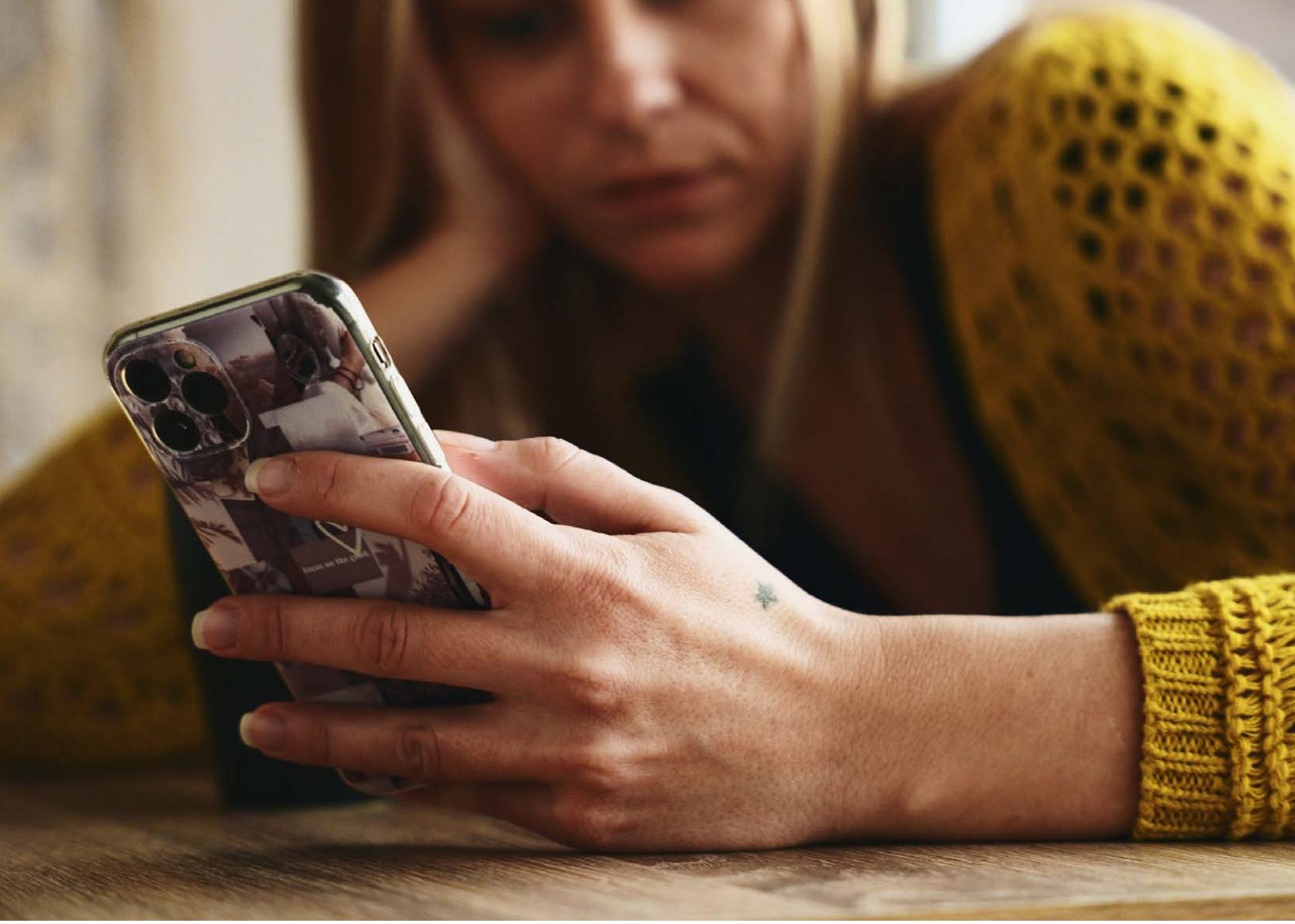
Mobile operators do not typically host content, but they can still be affected by false information. For example, misinformation linking 5G and the COVID-19 pandemic had direct consequences for the mobile industry, such as attacks on telecommunications equipment and staff. Through its work with the mobile industry, the GSMA provides access to factual information, including independent expert reports on electromagnetic fields (EMF) and health.

Legal frameworks are emerging globally to address misinformation, with a notable focus on online platforms. The EU's Digital Services Act (DSA) 2022 (which includes the Code of Practice on Disinformation) and the UK's Online Safety Act emphasise transparency, risk assessment and platform accountability regarding harmful content. Additionally, the World Economic Forum highlights the need for AI models to minimise bias and for public awareness campaigns. The European Commission has expressed concerns about 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.

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

Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, 2022
The 2022 Code of Practice on Disinformation, European Commission, 2022
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. 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 adopt systems like the Equipment Identity Register (EIR) and to connect to GSMA systems such as the GSMA Device Database.

Using the GSMA global Type Allocation Code (TAC) list of all legitimate device identity number ranges, operators can block devices with invalid IMEIs.

National authorities should study which factors, such as import duties and taxation levels, contribute to local demand for counterfeit devices. The potential to reduce tax levels on devices to narrow the price gap between counterfeit/smuggled and legitimate devices is something that should be considered carefully, 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 Registry website, GSMA
IMEI Database website, GSMA
Spot a Fake Phone website

Mobile devices: theft

Background

Policymakers in many countries are concerned about 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 responses to 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 it is 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 security solutions on mobile devices that 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 global sharing of stolen device data 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

Device Registry website, GSMA
IMEI Security Technical Design Principles, GSMA, 2016
IMEI Security Weakness Reporting and Correction Process, GSMA, 2016
Anti-Theft Device Feature Requirements, GSMA, 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 offers a host of new security capabilities that provide even more protection.

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.

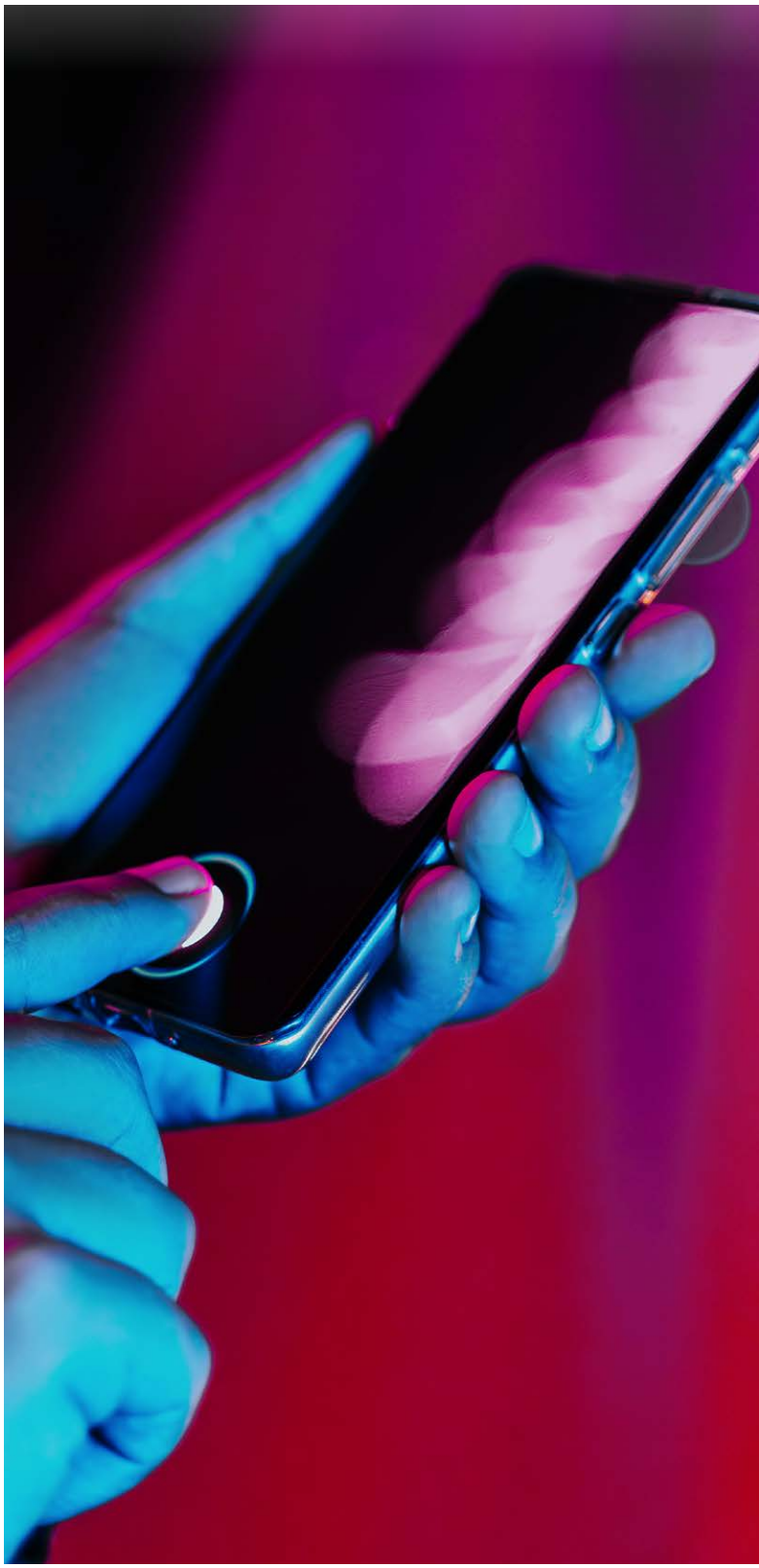
The mobile industry makes every reasonable effort to protect the privacy and integrity of customer and network communications.

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 experts to facilitate an appropriate response to threats, playing a key role in coordinating the industry response to security vulnerability research through its Coordinated Vulnerability Disclosure (CVD) programme.
- 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 conducts 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 maps these threats to appropriate and effective security controls. This analysis has been collated in a range of security guidance publications, including the GSMA Baseline Security Controls, which helps mobile operators understand and develop their security posture.
- The GSMA's Fraud and Security Group (FASG) acts as a centre of expertise for the 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

Mobile Cybersecurity Knowledge Base, GSMA
GSMA Mobile Telecommunications Security Landscape, GSMA, 2025
Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, 2022

Signal inhibitors (jammers)

Background

Signal inhibitors, also known as jammers, are devices that generate interference or 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 US.

In some regions, such as Latin America, signal inhibitors are used to prevent the illegal use of mobile phones in specific locations, such as prisons. However, blocking the signal does not address the root of the problem: wireless devices illegally ending up in the hands of inmates who then use them for illegal purposes.

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 allowing service to deteriorate.

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 in 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 impact 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, and would not affect the rights of legitimate users of mobile services.

Resources

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

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

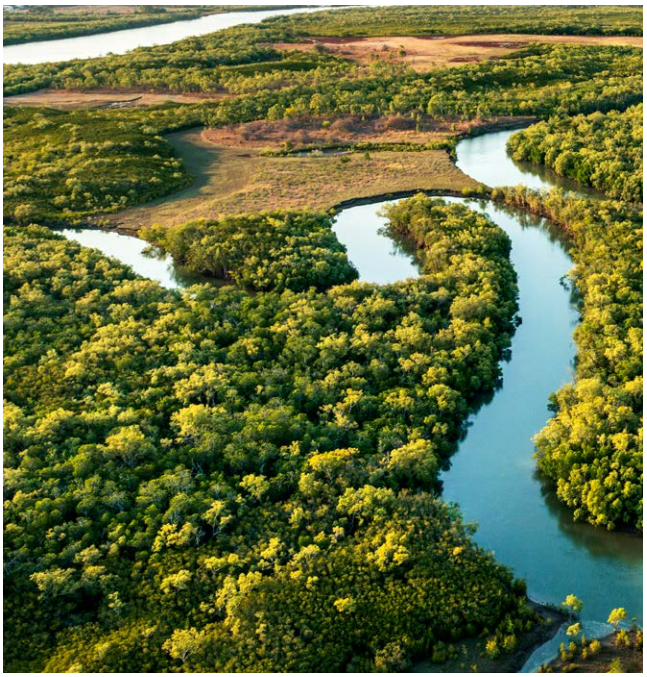
Safety, Privacy and Security Across the Mobile Ecosystem, GSMA, 2022

4 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, with a public ambition to be net zero by 2050 at the latest. 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.

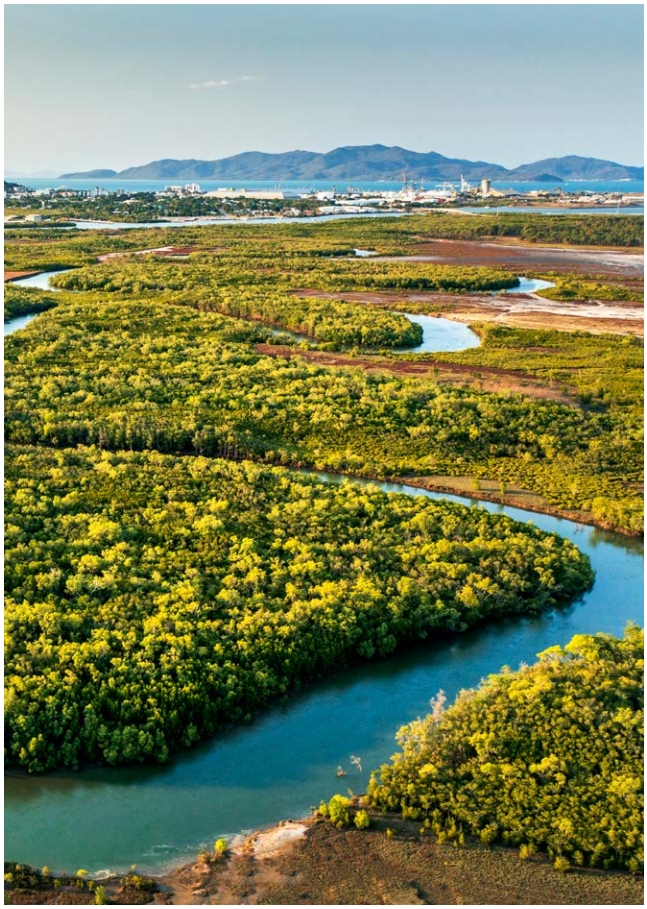
To understand how the mobile industry is progressing, mobile operators and suppliers are encouraged to disclose their climate impacts, risks and opportunities every year. Operators are setting emissions reduction targets – with best practice aligned with the ICT sector pathway to net zero GHG emissions by 2050 or earlier – and reducing their emissions by improving energy efficiency, purchasing and using renewable energy and electrifying 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.



Resources

ESG Metrics for Mobile website, GSMA

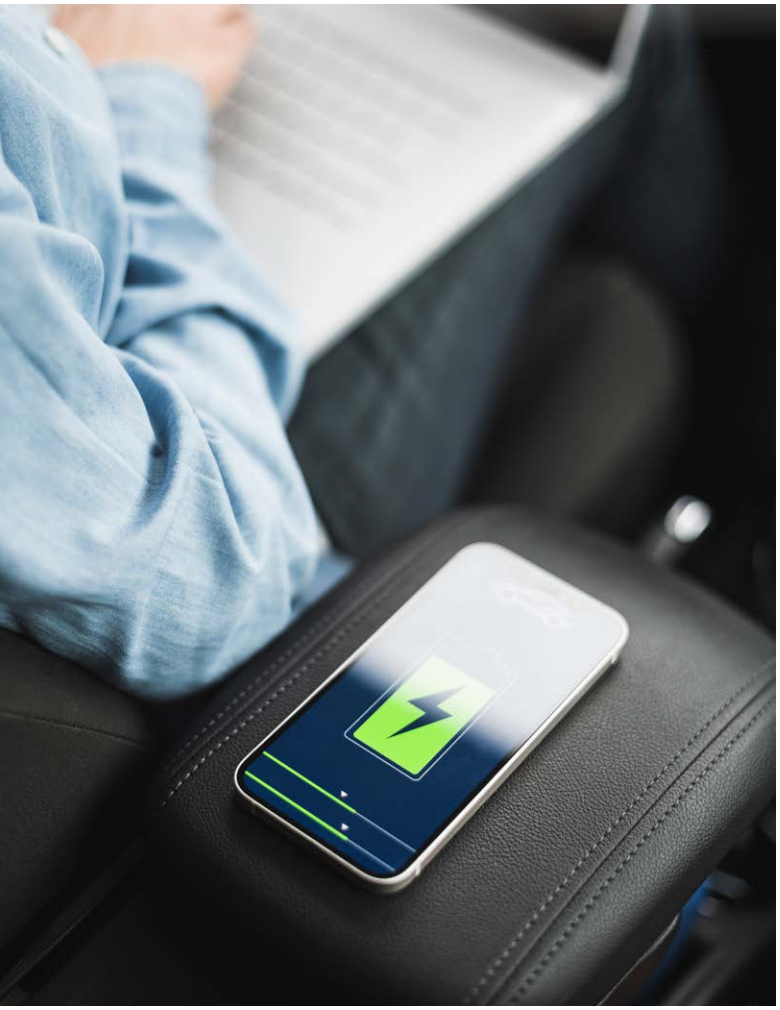
Mobile Net Zero 2025: State of the Industry on Climate Action, GSMA

Energy efficiency

Background

Energy efficiency is high on the agenda of mobile operators for both financial and environmental reasons, as network energy makes up the majority of their own emissions and a rising share of operating expenses.

As demand for widespread connectivity grows, so too does demand for mobile data. 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 GSMA Coordinated Vulnerability Disclosure (CVD) programme.
- 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 effectively 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 the aim of national energy efficiency improvements?

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

Industry position

Policies that support and incentivise the transition to more energy efficient networks and mobile industry practice 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 to do so, 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 (Second Edition), GSMA Intelligence, 2023

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.

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.

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.

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

Climate Policy, GSMA, 2023

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

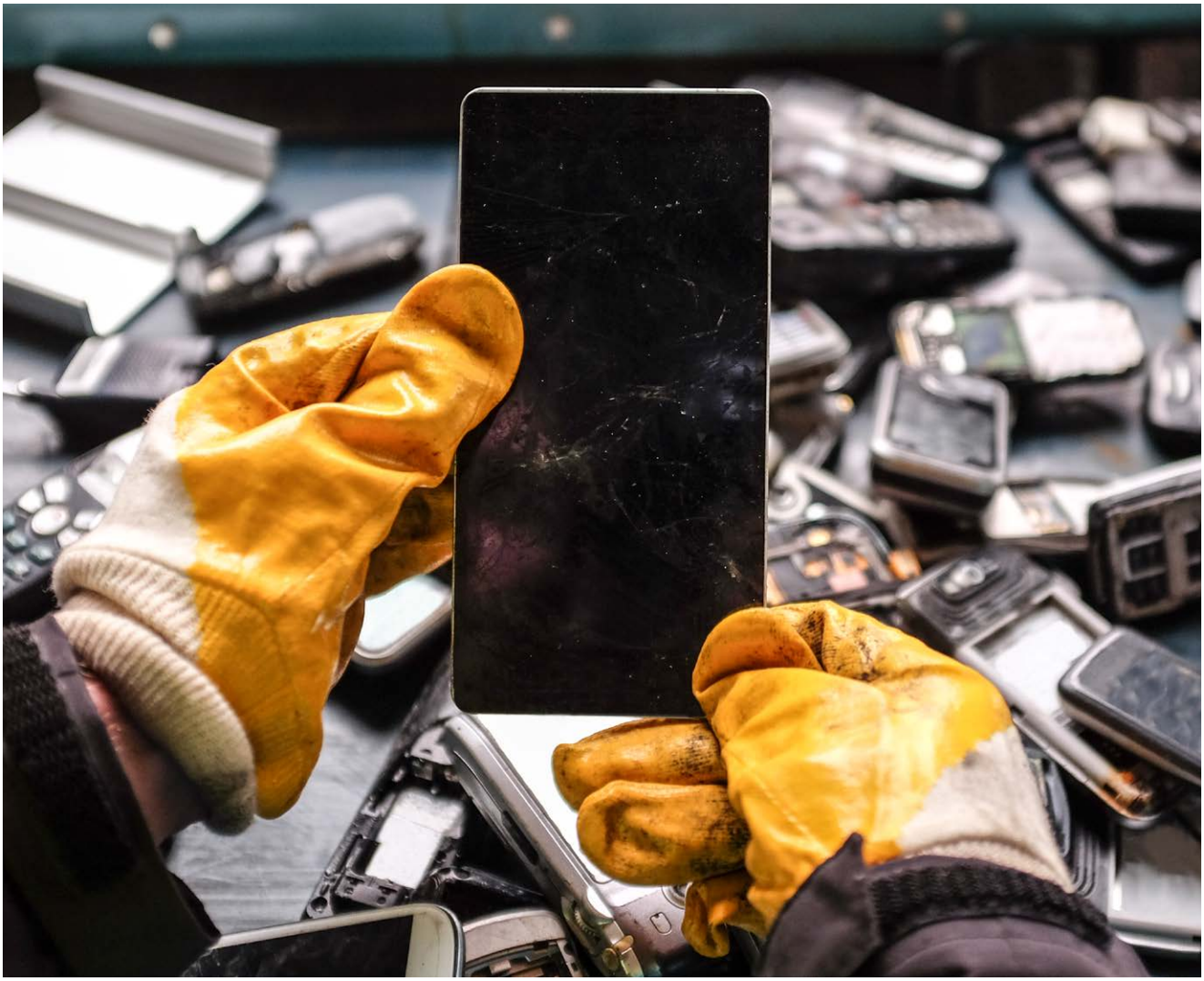
One of the biggest environmental impacts of the mobile industry is the manufacturing and use of devices and equipment. Although mobile phones and network equipment account for a small proportion of overall e-waste by weight, they can have a bigger impact than other waste streams because of the rare earth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

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.

The strategic vision is underpinned by two principles: increasing the longevity of devices and equipment and sending zero waste to landfill.

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.



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 greater 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

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 also 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, 2021

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

Appendix: Connecting the world through mobile

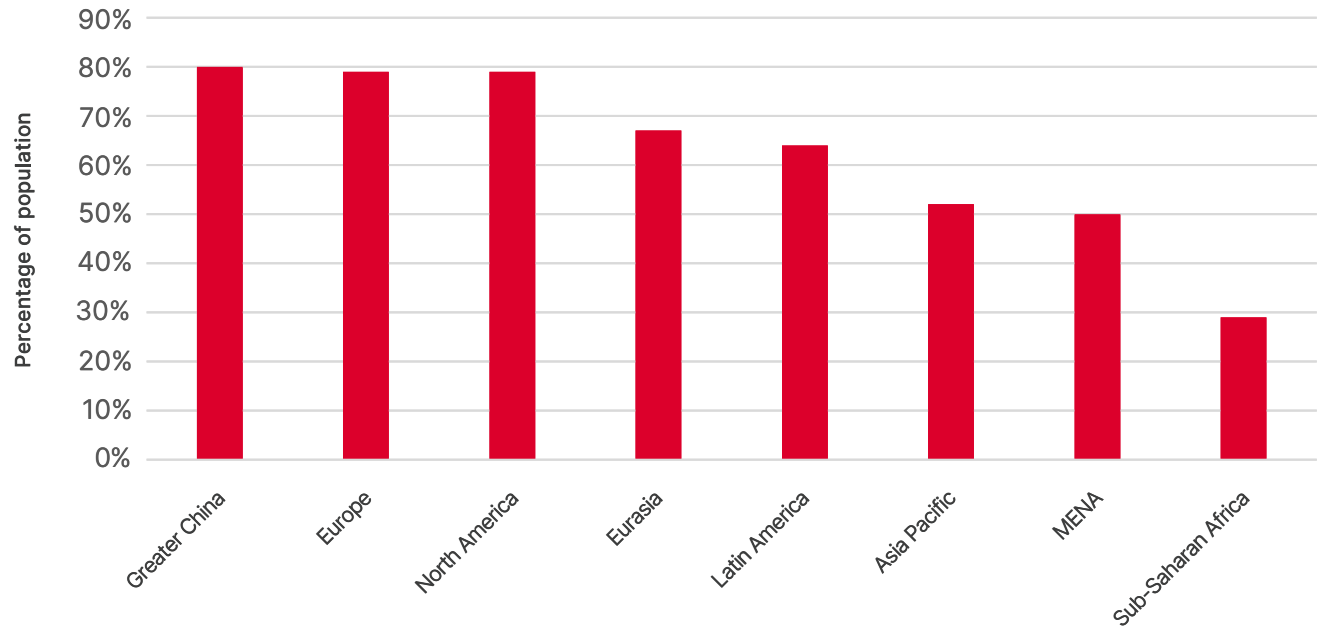
By the end of 2024, 58% of the world's population used mobile internet, equating to 4.7 billion users – an increase of 2.2 billion since 2015. More than 90% of those still not using mobile internet already live in areas with coverage but face other barriers to adoption. Looking ahead, mobile internet penetration is projected to increase to 5.5 billion by 2030, encompassing 64% of the global population.

About 40% of new mobile internet subscribers between 2025 and 2030 are expected to come from Asia Pacific, driven by growth in India, Pakistan and Indonesia. In the same period, Sub-Saharan Africa is expected to account for nearly a quarter of new mobile internet subscribers, while Latin America and the Middle East and North Africa are each anticipated to contribute just over 10%.

Over the next few years, subscribers will continue transitioning to newer network generations. By the end of 2024, 5G accounted for more than half of mobile connections in North America, Greater China and developed Asia Pacific. Growth will intensify in the second half of this decade, with 5G adoption set to exceed 80% in leading 5G markets by 2030. It is still early days for 5G adoption in most emerging 5G markets. However, 5G adoption will gather pace over the next few years with the arrival of cheaper 5G smartphones and new spectrum assignments.

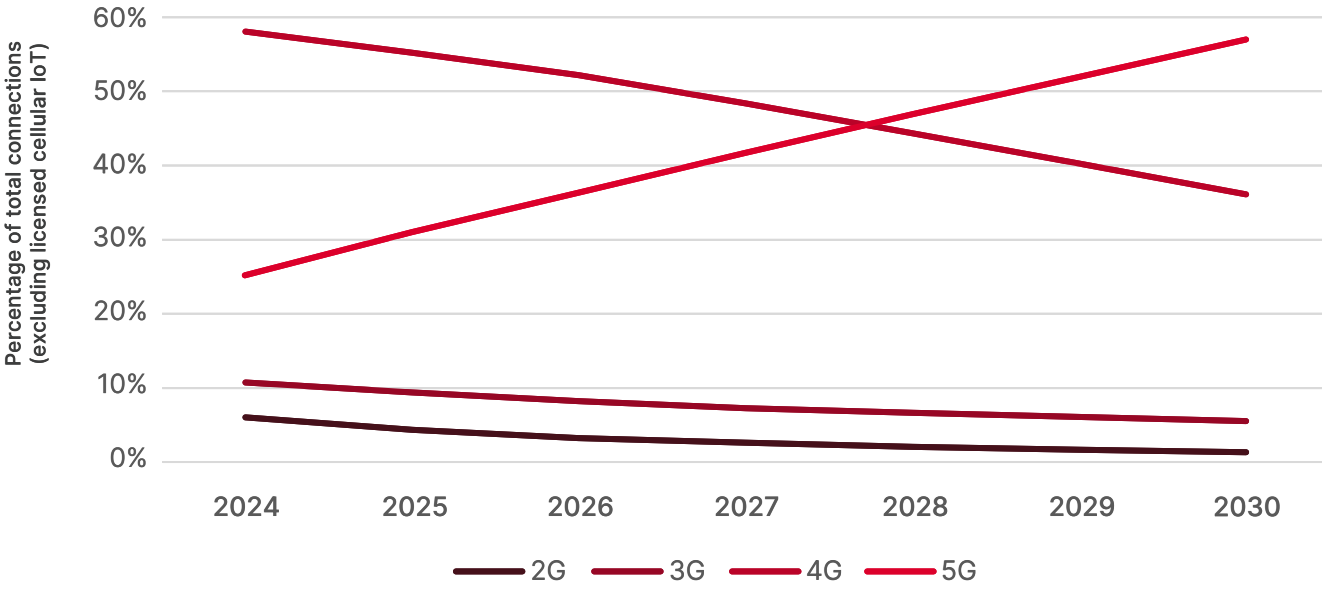
The challenge for the mobile industry will be translating 5G adoption into meaningful revenue growth. Shifting investment to more advanced forms of 5G, particularly 5G networks based on the Standalone (SA) architecture, as well as 5G-Advanced, will be important to unlock new use cases and monetisation opportunities. However, this investment will not occur automatically, and issues that limit the mobile sector's capacity to invest will need to be addressed first.

Figure 1 Mobile internet penetration by region, 2024



Source: GSMA Intelligence

Figure 2 Mobile adoption by technology



Source: GSMA Intelligence

GSMA