GSMA

Safety, privacy and security across the mobile ecosystem

Executive Summary

Executive Summary

In the last three decades, the market for mobile telecoms services has grown to represent more than 10.7 billion connections,[1] serving 5.3 billion unique mobile consumers globally.[2]

In 2021, the number of mobile internet subscribers reached 4.2 billion people globally,[3] 5G adoption also continues to grow rapidly and by March 2022 mobile 5G services were available in 73 countries and accounted for over 8% of global mobile connections.[4]

The impact of this growth can be seen in both developed and developing markets. Mobile services have allowed individuals, companies and governments to innovate in new and often unexpected ways, with consumers across the globe showing a ready appetite to adopt new technologies. The Covid-19 pandemic has exacerbated existing social and economic inequalities. When lockdown restrictions and social distancing measures were in place, people relied on mobile networks to stay connected and access life-enhancing services. The ubiquity of mobile services and smartphones in many lower- and middle-income countries (LMICs) has enabled whole new business models to emerge, supporting new forms of personal and business interaction and allowing the wider mobile ecosystem to generate a contribution of $4.5 trillion in 2021 in economic value added.[5]

The mobile industry works hard to educate consumers and has developed new features that build trust in its services. Each new iteration of technology has introduced new features, such as encryption and user identification validation, which make mobile services increasingly secure and minimise the potential for fraud, identity theft and many other possible threats. Importantly, the trust that underpins these services and allows people across the world to communicate, trade, share ideas and interact cannot be taken for granted.

[1] Mobile connections including IoT www.gsma.com
[2] https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf
[3] ibid
[4] 5G in Context, Data-driven insight into areas influential to the development of 5G (Q1 2022)
[5] https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf

Growth of potential threats

As more advanced and complex services are developed, the list of potential threats grows — and the scope for harm. Ever more sophisticated scams and attacks are developed and perpetrated, and criminals' ability to intercept communications increases frequently, from large data thefts to the hacking and disclosure of private communications during the 2016 US elections. Less high-profile, but just as damaging on an individual level, is the prevalence of phishing scams, ransomware and money fraud.[6] Of course, these target communications in general and not just communications from a mobile device, so solutions need to take a comprehensive view of the services in question.

Governments and policymakers naturally want to act to prevent such incidents and protect citizens to the greatest extent they can. However, in such a complicated environment, all interventions must be properly targeted. There is always the potential for any action, however well intentioned, to result in either a disproportionate cost or a restriction in access to the services they intended to protect.

There are also complex trade-offs between protecting the security of individual communications and law enforcement agencies needing at times to intercept certain communications to protect the public at large. The complex, multi-party nature of many of these services also needs to be kept in mind. For instance, two people communicating via a messaging chat service are actually using two different devices, possibly two different operating systems and interface applications, and multiple networks to connect via a messenger platform often hosted in a different legal jurisdiction than one or both users.

Each of these links in the chain presents its own potential weaknesses, loopholes and threats, from eavesdropping to abuse and from hacking to malware. Efforts intended to protect consumers can be misdirected by focussing on only one potential weakness and overlooking others. Actions to strengthen an already strong part of the overall service chain typically do nothing to address weaknesses in another part of the chain.

The mobile industry has made considerable investments to enable safe and secure use of its services, while also seeking to protect as far as possible the privacy of its customers. There is of course a technology dimension to its efforts: constantly improving standards, deploying better versions of technology, testing networks for weaknesses and building the capacity to detect and deter malicious attacks.

[6] See GSMA Flubot insight report: https://www.gsma.com/security/resources/t-isac-insight-report-flubot/

The GSMA plays a central role in coordinating activity and providing services such as GSMA Device Check™,[7] and security assurance schemes for SIM, eSIM and network equipment (SAS,[8] NESAS[9]). There are various other industry initiatives to make operators aware of the risks and mitigation options available to protect their networks and customers. Many mobile operators and other ecosystem players are extremely active in their markets and in international bodies to maximise the effectiveness of technology responses.

Technology alone, however, is not a sufficient response to the myriad threats and challenges. The industry, supported by the GSMA, has been highly active in programmes to educate consumers and businesses in how to safely use mobile technologies and the applications they support, in order to minimise illicit behaviour such as online abuse, fraud and breaches of privacy. In such instances, a holistic response is essential, involving governments, other agencies and non-profit support bodies, as well as the ultimate providers of services delivered online or via mobile devices, such as banking and payments.

Far more common are instances where personal data is voluntarily shared in order to access bona-fide commercial services. Here the mobile industry often faces a different challenge: with eight out of ten consumers reportedly uneasy with the degree of personal data being shared, there can be a natural tendency by consumer and politicians to expect network operators to address this. Yet technology and anti-trust considerations make it extremely difficult (at times impossible) for a mobile network operator to intervene in the exchanges between an online service provider and the end user. Furthermore, very different standards of data protection apply across jurisdictions and more importantly between the telecoms sector and online service provider sectors. Therefore, mobile network operators can only commit to protecting the user data they hold and to raise awareness that end users may be sharing far more data with organisations beyond their control. Governments and the wider ecosystem should collaborate to ensure that practical solutions enable consumers to make informed and effective choices, balancing each individual’s desire for privacy with their desire to access interesting, advertising-funded content and applications from a mobile device.

Some challenges to the provision of private and secure mobile services originate with governments and law enforcement agencies. Their legitimate and increasingly sensitive mandate to protect citizens has led them to sometimes seek wide-ranging powers to access and use personal data as well as intervene to block or restrict communication services in special circumstances.

The industry recognises its legal and moral obligation to support public safety and to respect the legitimate mandates of governments following due process, as well as its legal and moral obligation to respect human rights. With growing frequency, operators around the world have had to challenge specific interventions which they assess as disproportionate, misaligned to international human rights frameworks, or even potentially counter-productive to public safety goals.

This is a highly complex area with considerable differences between national jurisdictions, so the GSMA focuses on establishing common principles and educating all parties on best practices. Mobile network operators face two added challenges: they are in the front line when governments seek to challenge global internet companies over which they have little or no influence, and they are sometimes required to keep silent regarding such activity, despite wishing to be transparent with consumers who have placed their trust in them.

[7] https://devicecheck.gsma.com/
[8] https://www.gsma.com/sas
[9] https://www.gsma.com/nesas

Government, industry and other stakeholder action

This report takes each of the major issues of consumer protection, privacy, public safety and infrastructure security in turn. It highlights the potential issues, what is already being done to address them and what further actions may be needed. The issues are so important that the GSMA mobile operator members have concluded they must work more closely together, globally and at a national level, in order to ensure the most effective response.

None of these multifaceted issues can be 'solved' simply, or by one organisation or sector. To achieve the best outcomes for mobile users and society at large, commitment and action is needed from governments, law enforcement agencies, multilateral and non-governmental organisations. Companies across the digital ecosystem, as well as individual efforts by consumers themselves are also important. Not all issues are high priorities for all countries and thus all operators, but what is common across the issues and geographies is the need for closer cooperation between the multiple parties involved in providing end user services in order to ensure security and trust are maximised and the solutions that deliver the best overall benefit to society are developed and implemented.

The global nature of modern communication systems, from the standards, infrastructure equipment, services and operators means that one-off, unilateral actions are not as effective as a coordinated approach.

The report includes a set of principles supported by GSMA mobile operator members to guide their actions in protecting consumers and securing mobile communication networks. It also makes a call to policymakers and regulators to take a broad view of the issues at stake, in order to help develop multi-stakeholder solutions that best protect the overall interests of consumers, businesses and civil societies.

With this clear commitment to the safety, privacy and security of mobile communications services, the industry seeks to ensure that the benefits of mobile communications continue to grow for the foreseeable future, enriching lives and societies with the full potential of these exciting and dynamic technologies.

Protecting Consumers

Multi-stakeholder efforts are required to encourage the safe and responsible use of mobile-based online services and devices. In particular, governments and their law enforcement agencies should ensure appropriate legal frameworks, resources and processes exist to deter, identify and prosecute criminal behaviour. Often this will require global cooperation. Other industry ecosystem players, such as device manufacturers and mobile-based service providers, should engage in initiatives to help protect consumers when using mobile devices and services, and to educate them about safe behaviours and good practices so they can continue to benefit from these services in a safe manner. Mobile network operators can play a role in reminding consumers to be aware and vigilant and can encourage them to use the full suite of security measures available. With this in mind, the GSMA and its mobile network operator members have agreed to the following principle:

Operators will take proactive steps to address consumer protection issues related to illegal and harmful activities, linked to or enabled by mobile phone usage, by:

— Working collaboratively with other agencies to deliver appropriate multilateral solutions

— Implementing solutions that are designed to prevent use of networks to commit fraud and criminal activity, and devices being used in ways which harm the consumer

— Educating consumers on safe behaviours, in order to build confidence, when using mobile apps and services

Protecting Consumer Privacy

The key objective in protecting privacy is to build trust and confidence that private data is being adequately protected according to applicable privacy regulations and requirements. This requires all parties involved to adopt a coherent approach that is technology neutral and consistent across all services, sectors and geographies. Governments can help ensure this outcome, while allowing for the flexibility needed for innovation, by adopting risk-based frameworks to safeguard private data and encouraging responsible digital governance practices aligned to local regulation. With this in mind, the GSMA and its mobile network operator members have agreed to the following principle:

Operators will take proactive steps to protect and respect consumers' privacy interests and enable them to make informed choices about what data is collected and how their personal data is used, by implementing policies that promote:

— Storing and processing personal and private details securely, in accordance with legal requirements where applicable

— Being transparent with consumers about data that we do share in an anonymised form, and in full compliance with legal requirements

— Providing the information and tools for consumers to make simple and meaningful choices about their privacy

Protecting Public Safety

As part of laws and regulation, including licence obligations, and in accordance with local legislation, mobile network operators are obliged to take on additional responsibilities to assist law enforcement agencies in line with an overall objective to protect public safety. It is important that governments ensure they have a proportionate legal framework that clearly specifies the powers available to national law enforcement agencies. The legal framework should also ensure that assistance requests are necessary and proportionate, directed to the most appropriate communication service or technology provider, and compatible with human rights principles. With this in mind, the GSMA and its mobile network operator members have agreed to the following principle:

Operators will comply with all legal and licence obligations when addressing security or public safety concerns within the countries in which we operate, while at the same time being supportive of human rights concerns. We will cooperate with the relevant security agencies to protect public safety by:

- Working with the relevant agencies when specific situations require, to develop and implement appropriate solutions to achieve the end objective with minimal disruption to consumers and critical services
- Building networks that have the functionality to address emergency and security situations, where appropriate
- Being clear about the limit of action we can take over the value chain, and highlighting where others' actions should be undertaken

Protecting Network Security and Device Integrity

Industry players need to work together and coordinate with international law enforcement agencies to share threat intelligence to respond to malicious attacks on mobile networks and devices, as well as to identify perpetrators. This can be achieved through the engagement of existing security incident response teams and the establishment of new ones, if required, to cover any gaps. Regulations, where necessary, should be applied consistently across all providers within the value chain in a service- and technology-neutral manner, while preserving the multi-stakeholder model for internet governance and allowing it to evolve. With this in mind, the GSMA and its mobile operator members have agreed to the following principle:

Operators will take steps to protect the underlying infrastructure to ensure that we provide consumers with the most secure and reliable communication service possible, by:

- Taking steps to secure the network infrastructure that we operate and control
- Promoting public-private partnership to minimise the risk of either hacking or use of the network for malicious means through global and coordinated approaches
- Being clear about what infrastructure operators are responsible for and where the boundaries with other infrastructure or services lie

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