GSMA

Safety, privacy and security across the mobile ecosystem

Safety, privacy and security across the mobile ecosystem

This is an updated edition of the report “Safety, privacy and security across the mobile ecosystem” originally published in 2017.

GSMA

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

We invite you to find out more at gsma.com

Follow the GSMA on Twitter: @GSMA

GSMA

Contents

Executive Summary and Mobile Industry Principles 02

01. Introduction 08

02. Protecting Consumers 12
- Children and vulnerable individuals 14
- Stolen and counterfeit devices 22
- Fraud on mobile devices 31

03. Protecting Privacy 34
- Data collection and usage 36
- Consumer choice 42
- Cross border transfer of personal data 43

04. Protecting Public Safety 50
- Law enforcement assistance requests 52
- Service restriction orders and signal inhibitors 56
- Mandatory prepaid SIM card registration 60

05. Protecting Mobile Network Security and Device Integrity 66
- Physical network infrastructure 69
- Mobile device security and integrity 72
- 5G, IoT and future network developments 74
- GSMA security initiatives 76

Annex: Mobile Industry Principles 78

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

01

Chapter 1
Introduction

In all regions of the world there is an increase in both real and perceived threats to national security, public safety and individual privacy.

Mobile networks have a role to play in protecting public safety, such as when law enforcement agencies use their mandate to conduct criminal investigations with call data and interception of communications, support major incident communications, or track the spread of threats to health such as the use of location data to monitor and prevent outbreaks and the spread of Covid-19. At the individual level there are instances of fraud, identity theft, cyberbullying and other illegal activities being perpetrated via mobile networks as well as online or digital services accessed via fixed networks. Recent events, including high profile cases of data breaches, have also generated unease among many consumers about whether their security and privacy are protected, for instance, with regard to personal details about their lives.

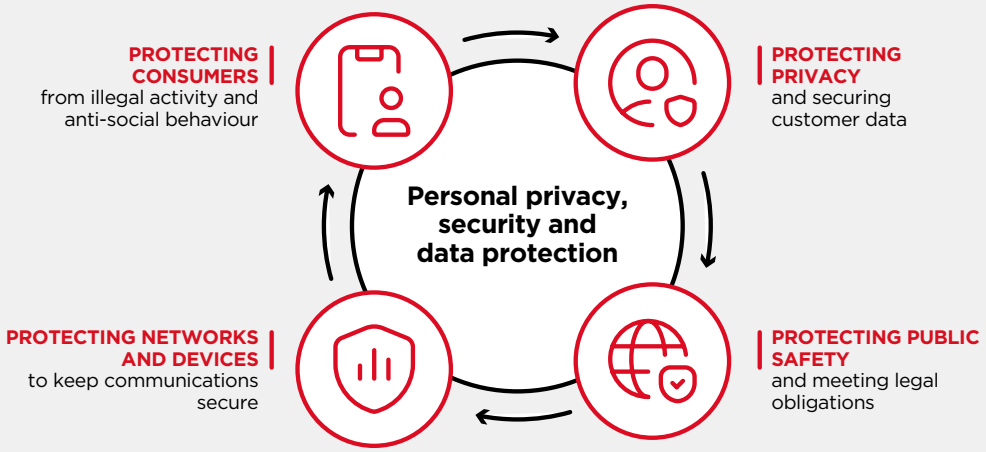
In this context, mobile network operators face an ongoing challenge to provide a safe and secure mobile experience for their consumers, while meeting their obligations to protect public safety. Much work is already underway within the GSMA and its member operators to tackle and address issues of privacy and security, and to promote the safe and beneficial use of mobile services and the vast array of applications they support.

This report seeks to explain the major issues and challenges around safety, privacy and security in the mobile world, highlighting the complexities and tradeoffs and demonstrating the industry initiatives and actions that are already taking place. Where there are opportunities to do more, the report identifies those areas and also outlines what is needed to enable such responses, whether to educate consumers, build partnerships across the ecosystem, or develop and implement multi-party technical solutions. The report addresses each issue in turn but acknowledges the many interdependencies and overlap between issues.

Structure

The overall topic of security and privacy is broad but can be considered under four main headings, shown in Figure 1.

Figure 1
Privacy and security framework



The next four sections of this report deal with each of the areas in turn, i.e.:

1. **Protecting consumers** – promoting the safe use of mobile services
2. **Privacy and data issues** – protecting consumer privacy and the safe storage and processing of individuals' personal data
3. **Protecting public safety** – defining the role and responsibilities of mobile operators in supporting government agencies to protect the public
4. **Protecting network infrastructure and devices** – ensuring the integrity and security of mobile network infrastructure and the devices used to access those mobile networks

The final section articulates the high-level principles that have been agreed to by GSMA member operators and briefly outlines plans to embed these in future GSMA activities.

As the report will make apparent, the nature of these issues requires coordinated action across geographies and also industry segments. While the mobile industry is taking a lead on addressing these issues, there are many other groups active from standards bodies such as 3GPP, ETSI, ENISA, IETF and NIST to global bodies including the ITU, the Telecommunications Industry Dialogue (ID), Global Network Initiative (GNI) and UNICEF.

All have a valuable and important role to play in shaping the discussions and developing solutions and the GSMA welcomes further collaboration and engagement from across the mobile ecosystem and the broader ICT industry on all of these topics.

02

Chapter 2

Protecting Consumers

For consumers worldwide to continue to enjoy the many benefits of mobile technology, it is important that they can use these services safely and with confidence.

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

As mobile services continue to grow rapidly in importance and scope, they are fundamentally changing the way people connect and interact with each other and with businesses. Inevitably with something so widespread, there are people who seek to use mobile technology to harm others.

This section deals with the issues that directly affect the security and well-being of consumers of mobile services and specifically those where users of mobile devices and services are exposed to threats from illegal, criminal or anti-social behaviour, including the following:

- **Safeguarding children and vulnerable individuals**
- **Theft and trade of stolen devices and the sale and use of counterfeit devices**
- **Fraud and mobile device security**

Each of these issues have a number of important implications for government, industry and other stakeholders. These are also outlined in more detail later in this chapter.

Children and Vulnerable Individuals

Mobile technology increasingly plays a role in enabling children to better access many of their fundamental rights set out in the United Nations Convention on the Rights of the Child (CRC). For example, mobile technology can facilitate children's access to quality education and appropriate information and can empower children to voice their opinions and participate in community decision-making. However, there are risks associated with connectivity, and for potentially vulnerable user groups including but not limited to children and some women, it is important to both enable the opportunities and benefits whilst combatting potential risks.

For example, a GSMA study examining the gender gap in terms of mobile device ownership and usage found that safety and security remains one of the top three barriers to mobile phone ownership and usage by women in low and middle income countries. This barrier covers information security concerns, concerns around receiving unwanted contact from strangers and being exposed to harmful content.[10] While it is important to note that only a subsection of women, as with men, may be considered vulnerable, these concerns must be acknowledged and addressed to ensure that the many benefits of connectivity can be accessed by all, especially those groups which potentially stand to gain most from using mobile services.

Consumers need to familiarise themselves with how to use mobile device features (e.g., cameras) and mobile-based services safely. The fact that mobile devices are becoming more powerful and can be used to carry out an ever-increasing set of common tasks, including accessing formal education and informal learning, banking and e-Health applications, only increases this need. As consumers learn to embrace these many benefits, there is an opportunity to actively broaden their evolving digital skills to include internet safety considerations through education and awareness programmes. Programmes designed to help build this "digital resilience" will require input from a range of stakeholders. It is important that mobile network operators participate in designing these programmes to ensure they address the needs of a rapidly evolving industry and clarify the roles of different players in the information and communication technology (ICT) ecosystem. Mobile network operators are already playing a role in promoting the benefits of mobile technology while educating potentially vulnerable groups on how to build digital resilience, how to use the services safely, and how to respond to and report abuse when it occurs.

10 The Mobile Gender Gap Report 2022 https://www.gsma.com/r/gender-gap/

Supporting the inclusion and safety of women

On average, women are 7% less likely than men to own a mobile phone across low- and middle-income countries, and are 16% less likely to use mobile internet. This translates to 264 million fewer women than men accessing mobile internet. The reasons for this are varied and the GSMA Connected Women programme has been working to identify and address these. Security and harassment concerns have emerged as important barriers to the uptake of mobile devices and services by some women.[11]

Mobile network operators recognise that by using mobile safety services, women can continue to benefit from the security afforded by connectivity while minimising the potential for harassment. For example, services that automatically block unwanted callers have been launched by mobile network operators in multiple markets and can be particularly appealing to female users. Also, services for feature phone or basic phone owners exist, such as 'Banglalink Emergency,' which automatically sends an SMS alert to three pre-registered contacts when the user dials a short code. The user's location is also sent to those contacts, thus improving their level of safety.

Safeguarding young users and child online protection

A second group of potentially vulnerable users of mobile services is children. In understanding the topic of child online protection, it is important to distinguish between two distinct issues:

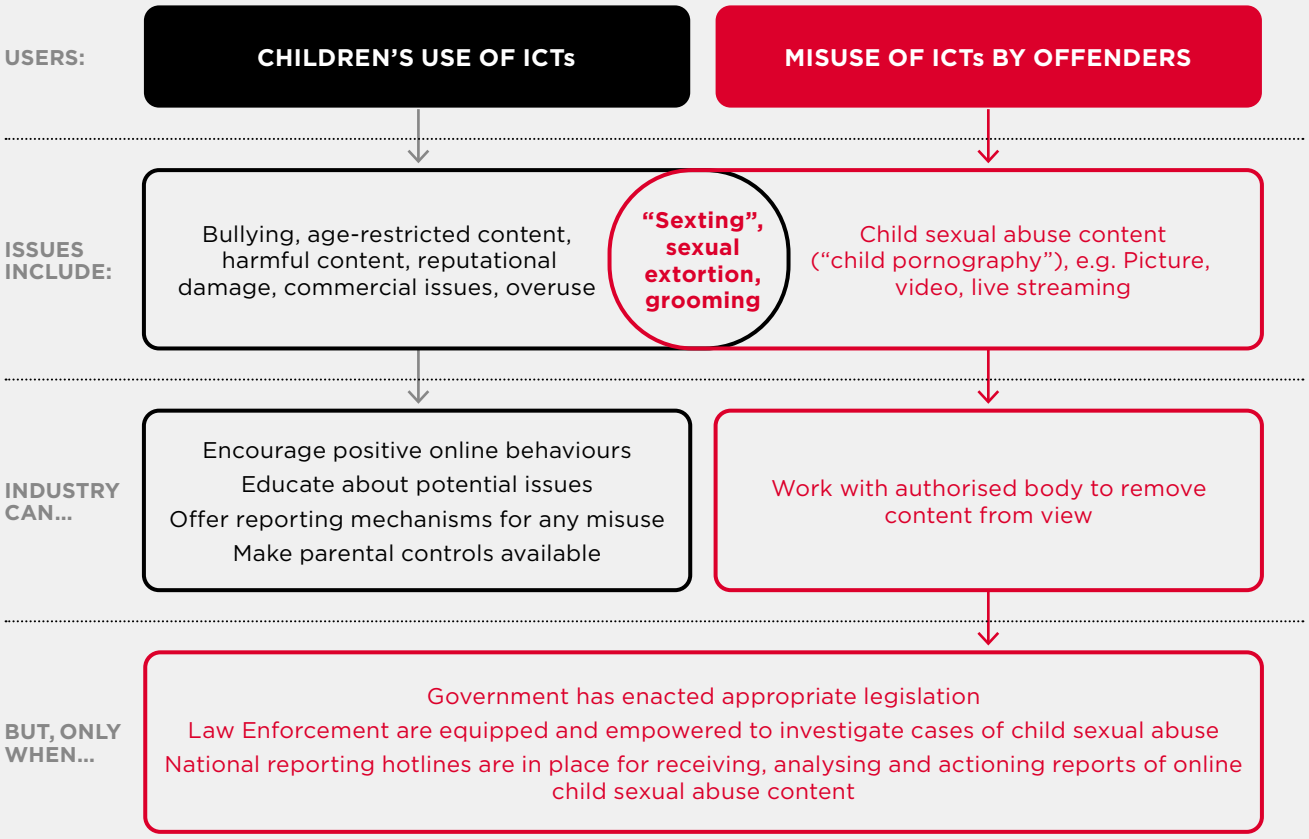
1. Encouraging the safe and responsible use of mobile services by children.
2. Combatting the misuse of mobile services by adults/offenders, e.g., to make, distribute or access illegal child sexual abuse content.

As shown in Figure 2, it is helpful to separate these out because the groups affected, and the response mechanisms required are very different.

11 ibid

Figure 2

Child online protection – issues and users



A key element in enabling children and young people to lead safer digital lives is encouraging positive online behaviours, as well as educating them about potential risks and thus empowering them to navigate the internet more safely and confidently. This is something that the mobile industry is contributing to, alongside other stakeholders including educators, parents and children's groups, by implementing and enforcing acceptable use policies, offering reporting mechanisms for any misuse, and making parental controls available.

Addressing the second issue and robustly combatting the misuse of technology to access, share or profit from child sexual abuse content requires a number of actions from a range of stakeholders. Governments need to have appropriate legislation in place, law enforcement must be equipped and empowered to investigate all aspects of online child sexual abuse (from grooming to the sharing of child sexual abuse content), and national hotlines for reporting child sexual abuse discovered online must be in place.

Industry can then contribute to this shared response, for example, by working closely with the national hotline to remove child sexual abuse content from their services as soon as they become aware of it, and by working with government in appropriate circumstances where lawful process exists.

In the areas of overlap, shown in Figure 2, both responses are required. For example, to mitigate risks of young people sharing self-generated sexual images of themselves ("sexting"), those children must understand the potential consequences of sharing and losing control of images. When self-generated sexual content is obtained and shared by an offender, processes for removing the content from view (as discussed in further detail in the sub-section relating to child sexual abuse content), as well as investigating and prosecuting the offender, need to be instigated.

The mobile industry has taken active steps, together with other stakeholders, to encourage the safer use of mobile services by children and young people.

The GSMA and its mPower Youth[12] initiative is dedicated to helping young people make the most of their mobile experience as well as collaborating with stakeholders across the mobile ecosystem as well as NGOs and government organisations. Along with other activities, the mPower Youth program informs approaches to promoting safe and responsible usage of mobile devices. Mobile network operators' approaches include wide-ranging education and awareness raising programmes, as well as offering technical solutions such as the provision of parental control services. Through its partnership with Child Helpline International (CHI), the GSMA has developed guidelines on safer internet issues as support for the child helpline community so that when children do encounter problems online, they can be signposted to a child helpline where a trained counsellor will be able to support them.[13]

When it comes to protecting children's rights online, companies and other stakeholders have to strike a careful balance between children's right to protection and their right of access to information and freedom of expression. Therefore, companies must ensure that measures to protect children online are targeted and are not unduly restrictive, either for the child or other users. The ITU and UNICEF Guidelines for Industry on Child Online Protection 2020 outline steps which can be taken to help protect and promote children's rights in a digital world.[14]

The rapid evolution of the mobile ecosystem adds complexity to this field. The model of operator-curated content services has evolved; in the current landscape, users have many means to access all varieties of digital content via their mobile devices. Many players have a role in the delivery of this capability, including mobile network operators, as illustrated by Figure 3.

Figure 3
The mobile ecosystem

12 http://www.gsma.com/mpoweryouth
13 https://www.gsma.com/mpoweryouth/resources/internet-safety-guides/
14 https://www.unicef.org/documents/guidelines-industry-online-child-protection

Traditional distinctions between different parts of the telecommunications sector and between internet companies and broadcasters are fast breaking down or becoming irrelevant. Government, the private sector, policymakers, educators, civil society and parents each have a vital role in encouraging the safer use of mobile services by children and young people. Cooperation and partnership between these parties are the keys to establishing the foundations for safer and more secure use of the internet and associated technologies.

The GSMA plays a leading role in self-regulatory initiatives for the mobile industry and was a key contributor to the ITU 2020 Guidelines for Industry on Child Online Protection.[15] The GSMA actively engages with governments and regulators, policymakers, law enforcement and industry to facilitate the development of collaborative approaches to encouraging safe and responsible use of the internet.

Deeper Dive

ITU guidelines for industry on child online protection

The Guidelines for Industry on Child Online Protection are aimed at establishing the foundation for safer and more secure use of internet-based services and associated technologies for today's children and future generations.

The Guidelines for Industry on Child Online Protection are the result of consultations with members of the Child Online Protection Initiative, as well as a wider open consultation that invited members of civil society, business, academia, governments, media, international organizations and young people to provide feedback on the guidelines.

Cooperation and partnership are the keys to establishing the foundations for safer and more secure use of the internet and associated technologies. Government, the private sector, policymakers, educators, civil society, parents and caregivers each have a vital role in achieving this goal. Industry self-regulatory initiatives can act in five key areas:

1. **Integrating child rights considerations into all appropriate corporate policies and management processes**
2. **Developing standard processes to handle child sexual abuse material (CSAM)**
3. **Creating a safer and age-appropriate online environment**
4. **Educating children, parents and teachers about children's safety and their responsible use of ICT**
5. **Promoting digital technology as a mode for increasing civic engagement**

15 https://www.itu-cop-guidelines.com/

Combatting online child sexual abuse content

Laws regarding illegal content vary significantly from country to country; however, CSAM is almost universally considered to be illegal. Certainly, the sexual exploitation of children by individuals or organisations seeking to consume, share or profit from CSAM is one that is universally agreed to be unacceptable.

As discussed above, tackling the misuse of technology with respect to CSAM requires governments to have appropriate legislation in place, law enforcement to be equipped and empowered to investigate, and operational national hotlines to be in place for reporting online child sexual abuse.

Internet service providers and mobile network operators are able to play a key role in preventing the re-victimisation of children who have experienced child sexual abuse by taking steps to restrict access to CSAM. For example, members of the GSMA Mobile Alliance Against Child Sexual Abuse Content (Mobile Alliance),[16] work to obstruct the use of mobile services by individuals or organisations wishing to consume or profit from CSAM. They achieve this through collaboration and information sharing, working with national internet reporting hotlines, having 'notice and take down' processes in place and restricting access to URLs or websites deemed by an appropriate authority to contain CSAM. It is an important point that an appropriate authority (such as INTERPOL, a national hotline or a law enforcement agency) determines which URLs or domains need to be blocked. Mobile network operators can then refer to this list and ensure it is implemented without being put in a position where they are required to judge the legality of specific content.

The members of the GSMA Mobile Alliance are committed to monitoring emerging trends impacting this area and to implement appropriate responses.

16 https://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance

Deeper dive

GSMA Mobile Alliance Against Child Sexual Abuse Content

The Mobile Alliance was founded by an international group of mobile network operators within the GSMA to work collectively on obstructing the use of the mobile environment by individuals or organisations wishing to consume or profit from CSAM.

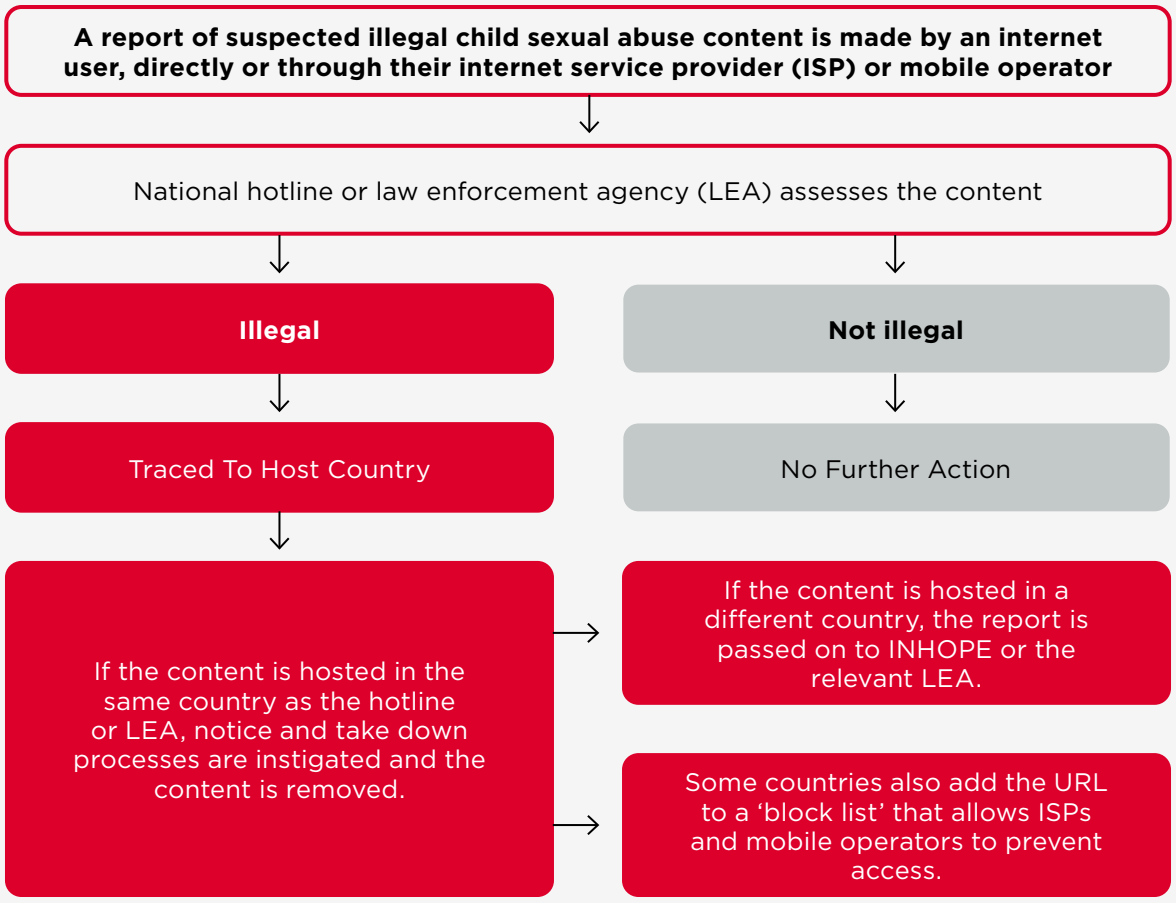
Mobile Alliance members have made the commitment to combating CSAM through a series of activities such as implementing 'notice and takedown' processes to enable the removal of any CSAM posted on their own services. Other activities include supporting or promoting hotlines or other mechanisms for consumers to report CSAM and technical measures to restrict access to URLs or websites identified by an appropriate, internationally recognised agency as hosting CSAM.

Through a combination of technical measures, cooperation and information sharing, the Mobile Alliance is working to combat online child sexual abuse and exploitation around the world.

The Mobile Alliance also contributes to wider efforts to eradicate online CSAM by publishing guidance and toolkits for the benefit of the whole mobile industry. For example, it has produced a guide to establishing and managing a hotline in collaboration with INHOPE, the umbrella organisation for hotlines, and a guide to Notice and Take Down processes in collaboration with UNICEF.

Deeper dive

Example of how a report of child sexual abuse content is handled by hotlines and their partners



Key implications for government, industry and other relevant stakeholders

Mobile devices and services enhance the lives and rights of young people. This perspective needs to be embraced, encouraged and better understood by all stakeholders to ensure young people get the maximum benefits from mobile technology. In March 2021 General Comment 25 on children's rights in relation to the digital environment was adopted by the UN Committee on the Rights of the Child (UNCRC).[17] This marks an important milestone in child rights by confirming, for the first time, that children's rights apply equally online as they do offline and that governments must support both opportunities and take steps to combat risks.

Addressing child online protection is best approached through multi-stakeholder efforts to encourage the safe and responsible use of online services and internet devices among children and young people and to empower parents and carers to engage with and help protect their children in the digital world.[18]

Furthermore, the full suite of responses to addressing and combating CSAM include legislation, reporting hotlines, law enforcement commitment, victim support, and the technical measures and processes to support these. While mobile network operators seek to play a role in helping to tackle this issue, for example, through the Mobile Alliance, they need support, leadership and accountability from the other relevant agencies and organisations to make a real impact.

The mobile industry condemns the misuse of its service for sharing CSAM.

- The GSMA's Mobile Alliance Against Child Sexual Abuse Content provides leadership in this area and works proactively to combat the misuse of mobile networks and services by criminals seeking to access or share CSAM[19]
- Mobile network operators use terms and conditions, notice and take down processes and reporting mechanisms to keep their services free of this content[20]
- The mobile industry is committed to working with law enforcement agencies and appropriate authorities to enable swift removal or disabling of confirmed instances of illegal content hosted on their services,[21] including CSAM

National governments should be open and transparent about which content is illegal in their country before handing enforcement responsibility to hotlines, law enforcement agencies and industry, subject to legal process.[22] However, these proactive initiatives should not be extended to actions that would breach international human rights conventions or private sector responsibility as defined by the United Nations' Guiding Principles on Business and Human Rights. Governments can engage with initiative such as the WePROTECT Global Alliance and refer to their Model National Response Framework or the Child Online Safety Toolkit which brings together international guidance into one useful guide to support the development of government strategies and responses to online safety.[23]

17 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
18 GSMA Mobile Policy Handbook: Children and Mobile Technology
19 GSMA Mobile Policy Handbook: Illegal Content
20 ibid
21 ibid
22 ibid
23 http://www.weprotect.org/the-model-national-response/ and https://childonlinesafetytoolkit.org/

Stolen and Counterfeit Devices

Mobile device theft and trade

The nature of mobile devices — small, portable and valuable — and the information stored on them make them attractive to criminals. This has created an international underground market for stolen smartphones and other mobile devices. Policymakers in many countries are concerned about the incidence of mobile device theft and involvement of organised crime in the bulk export of stolen and counterfeit devices, which are often transported across borders to exploit price arbitrage opportunities and to work around domestic blocking initiatives. To combat this activity and remove the value from this illicit trade, information must be shared among mobile operators in country and internationally.

Creating barriers to mobile device theft and trade

The GSMA coordinates a system of information sharing among mobile operators through its Device Registry service[24] to prevent reported stolen mobile devices from connecting to mobile networks worldwide. It also offers law enforcement and others the ability to identify whether a device has been reported lost, stolen or identified as counterfeit.

The GSMA recommends that mobile operators deploy the capability to block the connection of devices flagged as lost or stolen, or for other approved circumstances.[25] When victims inform their mobile service provider that the device is no longer in their possession, the operator can quickly prevent that device from accessing the network. To meaningfully combat trade in stolen phones, the device would ideally be blocked from connecting to any network. If a stolen device loses its ability to connect, then it has little value on the shadow or underground market. Device blocking can also limit non-network services such as insurance and repair.

Industry efforts to block the use of stolen devices start with the unique International Mobile Equipment Identifier (IMEI) assigned to every mobile-enabled device. The GSMA Device Registry maintains a central list of devices reported lost or stolen, known as the GSMA Block List. Mobile operators connected to the Block List maintain a continually updated list of device identifiers and are encouraged to deny these devices access to their network.[26] In this way, the GSMA Device Registry enables mobile operators around the world to prevent stolen devices transported to other countries from being granted network access.

Information gathered from mobile operators, device manufacturers and other GSMA-approved organisations that manufacture, insure or trade mobile devices is the basis of the Block List. The GSMA's Device Blocking and Data Sharing Recommended Practice[27] sets out best practice for mobile operators to block devices on their networks.

Although the GSMA does not handle personal data associated with mobile devices, in the context of increasingly broad data privacy regulation, it is recommended that mobile operators treat device identity data such as IMEI and GSMA Block List information as if it were personal data. Operators alone can link IMEIs of mobile devices to their own customers, and it is the responsibility of each participating mobile operator to observe the laws and industry principles governing privacy and data protection.

The GSMA Device Registry is currently used by over 125 mobile operators, collectively helping to protect more than 1 billion mobile customers. In Latin America, where handset theft is prevalent, most of the mobile operators spanning 18 countries share device data through the GSMA for this purpose. Of course, a device blocked by all mobile operators in one region could still be used in another location if an operator there was not using the global Block

24 https://www.gsma.com/services/deviceregistry/
25 Other cases approved for device blocking include broken, faulty or fraudulently obtained devices, indications of a duplicate IMEI, or court-ordered blocking.
26 This is typically done by implementing a standards-based Equipment Identity Register (EIR).
27 https://devicecheck.gsma.com/fs45/FS.45_v2.0

List. The theft and sale of devices is an international problem, and only when the majority of operators adopt this practice will mobile device theft be deflated.

IMEI blocking depends on the secure implementation of IMEIs by manufacturers to prevent tampering or counterfeiting. The GSMA's Device Registry also records cases of duplicate IMEIs and alerts operators of counterfeit devices. The world's leading device manufacturers support two key GSMA initiatives to strengthen IMEI security: definition of technical design principles for IMEI security implementation, and participation in the GSMA's IMEI Security Weakness Reporting and Correction Process.

More could be done by some device manufacturers to enhance IMEI integrity, which is essential to effective device blocking. Mobile operators and other large suppliers and retailers of mobile devices can make informed purchasing decisions when choosing which devices to sell to their consumers, with the security of IMEI implementation a key consideration. It is important that all stakeholders — manufacturers, mobile operators, governments and consumers — work together to ensure full IMEI integrity and the prompt remediation of problems that may arise.

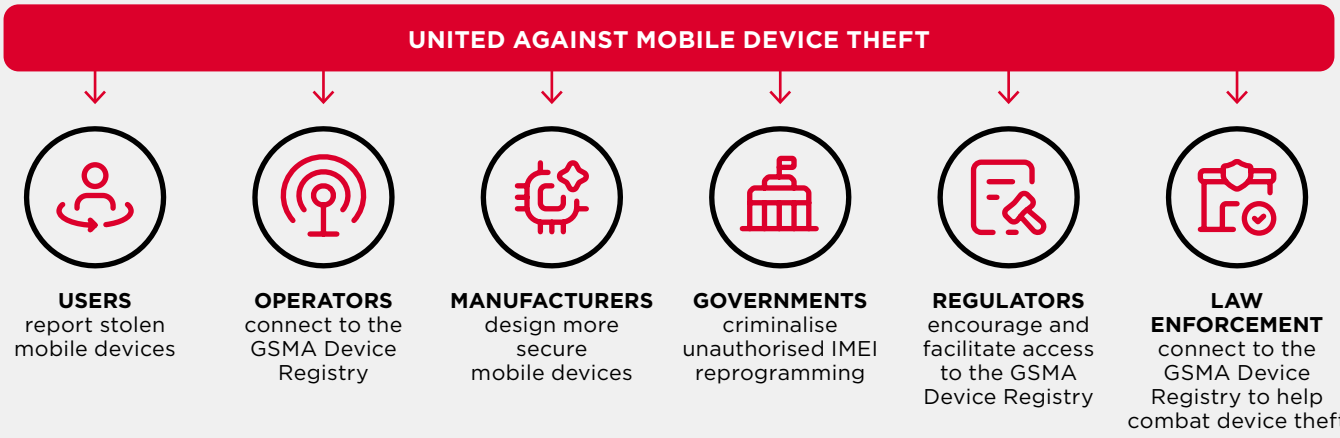
Governments are encouraged to criminalise unauthorised alteration of IMEIs in mobile devices (also referred to as IMEI reprogramming or adulteration). A number of countries such as India, Canada and the UK have made it a criminal offence to change the IMEI of a mobile device following its manufacture. Others are encouraged to follow suit and to actively prosecute offenders that bypass security controls.

To enable a wider range of stakeholders to combat device crime, the GSMA provides services, including GSMA Device Check,[28] 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 flag stolen devices.

GSMA Device Check also offers device recyclers the opportunity to identify and eliminate devices reported by participating operators as lost or stolen before they enter the recycling stream. The recycling of mobile phones, tablets and other mobile devices has become a huge business with millions of units being repurposed each year. However, with this growth, there has been an increased risk of stolen or lost devices. If device recyclers accept stolen or lost devices, it hurts their reputation and increases costs and losses.

Another form of deterrence for mobile device theft is a 'kill switch', which provides a way to disable crucial functions of a mobile device. For example, handset manufacturers can include security software in a smartphone's operating system that allows owners to remotely disable a stolen phone and render its software inoperable. The device can only be reactivated if the legitimate device owner authorises it. The GSMA Anti-Theft Device Feature Requirements defines a set of features that can be invoked by device owners to locate, disable and re-enable their device if it is misplaced, lost or stolen.[29]

Figure 4
United Against Mobile Device Theft



28 https://www.gsma.com/services/tac/about-device-check/
29 GSMA, 2016. Anti-Theft Device Feature Requirements, Version 3.0

Key implications for government, industry and other relevant stakeholders

The GSMA aims to restrict the sale and use of stolen or lost devices by offering expertise and resources to government, industry and other stakeholders looking to develop local solutions in a collaborative way.

A collaborative approach among the main stakeholders is essential:

- Users can report stolen devices to their service provider, enable anti-theft features on their devices and, in countries where operators are connected to the GSMA Device Registry, use the IMEI to check the status of a device they plan to buy.
- Mobile operators can block stolen devices from their networks, connect to the Device Registry to share Block List data and encourage their device suppliers to adequately protect the integrity of the IMEI implementations in their products.
- Device manufacturers can design more secure devices (i.e., make it impossible to reprogramme IMEIs) and implement kill-switch functionality to allow users to remotely disable lost and stolen devices.
- App store owners and operators can obtain the IMEIs of stolen devices from the GSMA and use those to deny app store access to devices that have been reported stolen.
- Governments can introduce legislation to criminalise unauthorised IMEI reprogramming and otherwise support industry and law enforcement efforts to combat device theft.
- Regulators can encourage local networks to connect to the GSMA Device Registry to share stolen device data, provide IMEI-checking services to allow users to check the status of devices before they buy, and provide a regulatory environment that supports effective, consumer-friendly solutions to combat device theft.
- Law enforcement agencies can take advantage of free access to the GSMA's stolen device data and focus sufficient resources on device theft to ensure offenders are identified and prosecuted.

It is important to avoid solutions that may be less effective or have negative consequences:

- The optimal solution to prevent the use of lost or stolen devices at a network level is the use of block lists.
- Non-standards-based solutions to combat mobile device theft should be avoided, as these are proprietary and tend to be technically difficult and expensive to implement. Approaches that are contrary to global mobile standards, such as tying specific devices to individual mobile users, tend to be difficult for users and their service providers to comply with and could raise a number of complex legal and competition-limiting issues.
- Building a national device identifier database is costly and unnecessary. The GSMA Device Check and Device Registry services are capable of meeting device blocking and data sharing needs. Additionally, maintaining one single global repository of device data is preferable as it ensures consistency, wider data sharing and avoids fragmentation, which would ultimately undermine the effectiveness of all approaches.

Case Study

Colombia and Ecuador Press Reset on Device-Theft Initiatives

Mobile operators in Latin America were early adopters of policies to identify and block network access to stolen and unauthorised devices, and they have been contributing to the GSMA's Device Registry and blocking reported handsets for almost a decade. During 2021 alone, nearly 5 million devices were blocked in Latin America using the GSMA Device Registry, representing around 40% of Block List activity worldwide.

Reacting to the scale of the problem, some governments in the region have chosen to go further, setting up national systems and processes to control mobile handset imports and use of stolen devices. There is, however, a risk that the additional complexity created by such public initiatives could prove to be a burden for operators and a barrier to consumer adoption, while delivering marginal results at best. Colombia and Ecuador offer two examples of countries that have scaled back their original vision.

Colombia

In Colombia, the telecommunications authority Communications Regulation Commission (CRC), in collaboration with the ICT Ministry and mobile operators, implemented a system to identify, register and manage access of devices to the country's mobile networks, and to establish a process for blocking those identified as stolen. This IMEI-based approach, first implemented in 2011, was a regional forerunner that aimed to ensure only legal and legitimate mobile devices could be used.

To lay the regulatory groundwork, the CRC passed a series of resolutions addressing issues such as the sharing of data between the mobile operators and assigning the legal and financial responsibility for a centralised database to the operators. This database consisted of a 'positive list' of all legally imported and acquired mobile devices approved for use in the country, together with the names of the registered owners of each device, and a negative list of devices that should be denied network access. Unfortunately, in addition to the data protection risk this approach introduced, collection and reporting of such information imposed a significant compliance burden and created a barrier to selling or transferring handsets. Consequently, the government's admirable goal of addressing a serious societal problem failed to make a meaningful difference, while imposing costly obligations on the mobile ecosystem. Over a decade later, with the results failing to justify the costs, Colombia is re-evaluating and may eliminate handset registration requirements altogether, as part of a wider regulatory simplification scheme.

Case Study

Ecuador

In Ecuador, the regulator chose to implement a positive list including the type allocation codes (TACs) of legitimate, approved mobile devices, hence blocking invalid IMEIs. However, during the COVID-19 quarantine in 2019-20, the government decided to ease the restriction, acknowledging that the restriction was a potential barrier to citizens' adoption of mobile communication services. Now it is resuming the blocking policy, but providing a 30-day period for users to acquire a new handset.

Both of these 'cautionary tales' underscore the importance of rigorous impact analysis that helps regulators to strike the right balance between, in this case, consumer safety and mobile service accessibility.

Preventing the sale and use of counterfeit devices

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 via underground markets by organised criminal networks. As a result, there is limited awareness among consumers and governments about the true scale and impact of trade in counterfeit mobile devices. According to a report published in 2017 by EUIPO and ITU on the economic cost of IPR infringement in the smartphone sector, worldwide the effect of counterfeiting on smartphone sales in 2015 was estimated to be 184 million units, valued at 45.3 billion euros (12.9% of total sales).[30]

30 https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study11/smartphone_sector_en.pdf

Counterfeiting mobile devices is a crime that breaches intellectual property and legitimate trading rules and results in the loss of revenue for manufacturers and tax income for governments.

Trade in counterfeit devices also has an impact on consumers. In many markets, the prevalence of counterfeit devices may be so high that consumers are buying them unwittingly. Aside from the poor performance often associated with counterfeit devices, many have been reported to contain hazardous materials that pose a threat to the environment. For example, a number of studies have measured levels of lead in solder joints that exceed globally acceptable limits. Such devices pose a threat to the environment if not disposed of using environmentally sound procedures.

Counterfeit mobile devices are not easy to identify and block, given that many have IMEIs that appear to be legitimate. To help address this issue, the GSMA Device Database can help reveal discrepancies between a device's IMEI and the registered characteristics that the device should have, if legitimate. Devices with invalid or non-existent IMEIs are added to the Block List. However, in the case of IMEIs that belong to legitimate devices but have been used by counterfeiters in their products, it is difficult to differentiate and isolate the legitimate device from the counterfeits.

Furthermore, counterfeit devices can only be blocked after consumers have, often unknowingly, purchased one and attempted to connect it to a mobile network.

Disruptive action such as blocking devices that have already been traded often punishes innocent parties and not those who trade counterfeit goods. Measures should not inconvenience innocent users and disrupt the legitimate market while those engaged in counterfeiting and illegal trading continue to benefit. Specifically, the manufacture and distribution of counterfeit devices should be targeted by the appropriate authorities to take them out of circulation before they reach unsuspecting consumers.

The GSMA partnered with the World Customs Organisation (WCO) in 2016 to collaborate in the fight against counterfeiting and fraudulent trading of mobile devices. Under the agreement, WCO customs officials are able to access the GSMA's database to cross-check and filter out counterfeit devices at the point of import. However, this solution cannot be applied to mobile devices that circumvent the customs process, in which case customs and law enforcement agencies need to increase their focus on illegal trafficking. Due to the complexity of this issue, law enforcement efforts to combat the distribution and sale of counterfeit devices have not been sufficient to contain the problem. Current national legislation and regulations have had limited effect, as counterfeit device distribution is typically international, and clampdown efforts in individual countries are easily avoided.

Furthermore, there is no evidence that establishing national registries of authorised devices is effective in combating the sale and use of counterfeit devices. Such an approach can impede the free movement of mobile devices around the world and would be considered illegal in some countries. Rather, the development of global, multi-stakeholder solutions is needed, as described in the next section.

Key implications for government, industry and other relevant stakeholders

The GSMA recognises the problems that counterfeit devices pose to users, operators, legitimate manufacturers and governments, and supports the need to maintain integrity in the mobile device market. The GSMA is willing to work with its members, governments and other stakeholders to develop solutions that can be effective in combatting the production and supply of counterfeit devices.

Collaboration among a range of stakeholders is essential:

- Regulators can work with device manufacturers and mobile operators to understand the extent of counterfeit device penetration and to agree measures that do not penalise legitimate device manufacturers or innocent users exploited by counterfeiters.
- Governments can disrupt the counterfeit device market by reducing tariffs and duties on legitimate imported devices, which will reduce the cost of ownership of legitimate devices and can also support consumer awareness and education programmes to highlight the risks of buying counterfeit devices.
- Customs agencies can ensure they have the ability to verify whether devices contain legitimate identifiers at the point of import by obtaining cost-free access to IMEI data through the GSMA Device Registry and by increasing their focus and resources to identify and prosecute offenders.
- Device manufacturers can work with government, regulators and customs agencies to help educate stakeholders on counterfeit devices and provide intelligence to the appropriate authorities on activities related to the production, distribution and sale of counterfeit devices.
- Mobile operators can work with the GSMA Device Database to obtain the definitive list of legitimate device identifiers, and then if required can deny access to devices identified as counterfeit.
- Users can check the legitimacy of devices they plan to buy against verification services provided by other stakeholders where available.

It is important to avoid solutions that may be less effective and/or have unintended negative consequences:

- Non-standards-based solutions to combat counterfeit mobile devices should be avoided, as these are proprietary and tend to be technically difficult and expensive to implement. Approaches that are contrary to global mobile standards, such as tying specific devices to individual mobile users, tend to be difficult for users and their service providers to comply with and could raise a number of complex legal and competition-limiting issues.

Fraud on Mobile Devices

Fraud can take many forms, and some of these exploit mobile devices as a channel. These include attacks such as service fraud (e.g., identity fraud or mobile money fraud), mobile spam[31] and, increasingly scams or "social engineering" fraud (e.g., phishing, SMiShing or vishing), which tricks victims into revealing sensitive information about themselves and the services they consume, without realising they have compromised their own security.

2020 was a year of unprecedented challenges, as the Covid-19 pandemic environment provided opportunities for fraudsters, in the form of new-to-digital consumers, heightened vulnerabilities and anxieties, as well as new channels to exploit.

Social engineering fraud uses manipulation to influence a person to take harmful actions such as divulging personal details or passwords. Once personal details have been accessed, criminals can then record this information and use it to commit other fraud related crimes such as identity theft and bank fraud. Scammers that engage with their intended victims typically build rapport and confidence, at times by leveraging publicly available information. In the United Kingdom during the pandemic, criminals sent scam texts, phone calls and emails impersonating trusted organisations such as the National Health Service (NHS), the police and the government to trick people into giving away their personal and financial details.

This type of fraud is on the rise and has been identified by the international police agency INTERPOL as one of the world's emerging fraud trends For example, in the UK fraud and cyber-related offences made up over 50% of all crime and the total financial fraud loss in 2020 was £1.26bn.[32] Fraudsters succeed when they are able to convince their victim that they are legitimate, either in person or via a service or website. Technology solutions offer some defence: for example, mobile operators have adopted GSMA recommended techniques for detecting and dealing with the international transmission of fraudulent mobile spam.

Although less common now, voicemail systems have been targeted as a means to compromise the security of mobile users by allowing unauthorised parties to listen to voicemail messages or to make fraudulent calls. Voicemail systems can be used as a fraud enabler and the GSMA has provided guidance for operators and consumers on how to ensure robust consumer authentication is deployed to protect users' voicemail accounts by ensuring that only legitimate consumers access voicemail services in a way that provides a balance between usability and security.

The GSMA offers its members considerable security expertise and services through a range of activity areas that collectively build a knowledge base, guidelines and services that build stronger mobile network security resilience. The GSMA's Fraud and Security Group (FASG)[33] aims to maintain or increase the protection of mobile operator technology and infrastructure as well as customer identity, security and privacy such that the mobile industry's reputation stays strong and mobile operators remain trusted partners in the ecosystem. The GSMA T-ISAC[34] is the central hub of security information sharing for the telecommunication industry. Drawing on the collective knowledge of mobile operators, vendors and security professionals, the T-ISAC collects and disseminates information and advice on security incidents within the mobile community – in a trusted and anonymised way. The GSMA encourages information sharing to combat all types of fraud, including network fraud. Mobile operators can reduce the adverse effects by sharing their high-risk number data as fast and as wide as possible. This enables operators to build up and maintain an accurate, global resource of high-risk numbers.[35] The GSMA works with organisations such as the Communications Fraud Control Association (CFCA)[36] and the Telecommunications UK Fraud Forum (TUFF)[37] in this regard.

However, human behaviour is also at the core of the issue of mobile fraud, so education on how to protect personal details and raising awareness of

31 'Mobile Spam' refers to bulk unsolicited mobile messages. Most spam is intended to defraud or scam the recipient, and is dependent on the charging model in place (i.e., low barrier to sender if the recipient is the party charged)
32 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1015382/Crime-plan-v10.pdf and https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf
33 https://www.gsma.com/aboutus/workinggroups/fraud-security-group
34 Please add footnote: https://www.gsma.com/security/t-isac/
35 https://www.gsma.com/services/fis-hrn/
36 https://cfca.org/
37 https://www.tuff.co.uk/

potential threats are key levers to minimise risk. Mobile network operators are well positioned to help educate consumers about the need to be aware and vigilant. However, more specific messages should be reinforced by the ultimate service providers for example, banks and retailers who are best placed to provide and enforce the particular technical security measures related to their service.

To support mobile operators in this, GSMA recommends three guiding principles[38] when developing messages for consumers on this issue:

1. **The message should be relevant and specific**
2. **The message should be simple and easy to understand**
3. **The message should be reinforced during customer interactions**

Terminology

Social engineering fraud examples:

Phishing – method used to infect computers or mobile devices to access valuable personal details. Phishing fraudsters generally use communications such as email to tempt people to access what appear to be authentic websites or services in order to extract personal details.

SMiShing – or 'SMS phishing' uses phone text messages to deliver the "bait" which then induces people to divulge their personal information.

Vishing – is when fraudsters persuade victims to hand over personal details or transfer money, over the phone by impersonating a genuine service, e.g., a bank

Fraudulent SIM swap and social engineering of call centre staff – is when fraudsters get someone's SIM reassigned to them in order to gain access to their mobile phone account and subsequently a series of accounts which they interact with such as banks, shops, travel companies etc.

Key implications for government, industry and other relevant stakeholders

Fraud in all its forms is a complex issue and almost always already illegal in most countries. Mobile network operator actions can only influence consumers' behaviour with the objective of mitigating the risk of fraud through prevention. Legislation and regulation should focus on perpetrators; education and awareness have to be the primary ways to foster consumers' ability to protect themselves. In particular, in markets where there is a low level of technological understanding, consumers today are often not using available protective technology features to their full potential.

- It is important that the ultimate service providers, (e.g., banks in the case of money services), implement the highest possible levels of security, appropriate to their market
- Preventative controls, such as consumer awareness campaigns to increase consumer education and protection, should be used and promoted to help consumers minimise their exposure to fraud
- Mobile network operators need to develop robust risk management strategies to mitigate the risk of fraud. The types of actions taken and the level of implementation will be determined by individual operator threat assessments and be specific to the services they offer and the consumers in their markets

38 L. Gilman, 2012. "Mitigating the risk of fraud through consumer communication", GSMA

Case Study

Mobile money risk management: consumer communication

Safaricom M-PESA is an example of how communication has been used as a tool to help prevent mobile money related fraud. One of the top priorities for Safaricom's M-PESA is mitigating the risk of scams against consumers. In addition to reactive measures, and rather than attempting to only use detective controls (i.e., monitor and report trends ex-post), Safaricom relies heavily on a preventive control to reduce risks of scams against consumers. Safaricom has found the most effective preventive control is raising consumer awareness through clear communication. In 2021 Safaricom launched a customer awareness drive to protect stakeholders from identity theft and social engineering fraud. It highlighted the issues through an above-the-line campaign under the tag Jichanue and Take Control, using radio, TV and digital channels. It established Fraud Management Squads specialising in analytics, customer awareness and process review to drive customer safety through accelerated use of machine learning and automations, continuous customer fraud awareness and process reviews. Increasing consumer awareness through clear communication has been vital to Safaricom's success in managing fraud against M-PESA consumers.[39]

Consumer communication is a tool that should be used as part of a broader risk-management strategy and should be complemented by relevant data and dashboards and defined internal procedures. For example, the GSMA has developed a comprehensive mobile money risk-management framework and toolkit for operators to use.

The GSMA's report "Cybersecurity: A governance framework for mobile money providers" presents a holistic framework that mobile money providers can use to improve security and provide safeguards against cybercrime. The framework has three dimensions — people, process and technology — and provides guidance for mobile money providers to ensure the security of their operations and their customers.[40]

39 See Safaricom's 2021 Annual Report and Financial Statements

40 https://www.gsma.com/mobilefordevelopment/resources/cybersecurity-a-governance-framework-for-mobile-money-providers/

03

Chapter 3

Protecting Consumer Privacy

To realise the benefits of data-driven innovation for society and the economy, individuals need to be empowered and trust that their personal data is being properly protected.

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 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

The last decade has witnessed a huge increase in the richness of communication services. The very nature of these services means that the organisations providing them gain access to considerable information about users — their identity, who they communicate with, their location and their personal interests reflected in the sites and services they access.

Online service providers can analyse communications such as words typed into search engines or locations typed into map applications and combine these datasets to derive users' interests and intent.

Consumer privacy continues to come under the spotlight as the technology used becomes increasingly pervasive. Mobile operators use only a limited set of personal data to enable the provision of communications services; personal information is more intensely used by other companies in the internet ecosystem.[41] Although users may not always realise it, many of those online services are offered for free on the basis that the provider can use that personal data to sell advertising or market paid services to the user. This section addresses what data is collected from users across the internet ecosystem and how it is stored, used and accessed, as well as the related privacy implications.

The specific issue areas covered are:

- **Data collection and usage, with a focus on supporting innovation**
- **Consumer choice, with a focus on embedding choice in online services and applications**
- **Cross-border flow of data, acknowledging national security concerns**

Each of these issues has a number of important implications for government, industry and other stakeholders. These are also outlined in more detail later in this chapter.

Data Collection and Usage

The GSMA forecasts that there will be an additional 1.6 billion smartphone connections by 2025, bringing the overall smartphone adoption level to over 80% of total mobile connections.[42] As connectivity becomes increasingly fluid and flexible, 5G will change the types of service and business models that are possible in unpredictable ways; much in the same way as the sharing economy and apps have changed the way we interact with organisations, government and each other. The volume and granularity of traffic and location data generated during 5G communications will increase, and new data-driven applications that leverage 5G could lead to a greater volume and variety of personal data use.

While 5G represents a significant shift in the use of mobile networks, existing data privacy regimes that are technology neutral already address a wide range of uses of data collected through apps, mobile device operating systems, social media, websites and network operators and are likely to be sufficient to address the use of new 5G capabilities within the online ecosystem.[43]

However, research shows that consumers are concerned about their privacy and seek reassurance that they can trust companies with their data. A GSMA study conducted in 2019 found that those in Europe and the US in particular remain averse to sharing personal data, regardless of purpose:

- More than two thirds of respondents were very or somewhat concerned about data privacy; half of them were more concerned than they were in 2018.
- The majority were uncomfortable with their personal data being used for targeted advertising or personalised services (90% and 84% of European and US respondents respectively, on average).
- The same goes for other purposes, including helping companies with product innovation, gaining some form of financial benefit or helping innovation for the public good. At least 75% of respondents rejected sharing data for these purposes.[44]

41 GSMA report: The Internet Value Chain 2022 https://www.gsma.com/publicpolicy/wp-content/uploads/2022/05/Internet-Value-Chain-2022.pdf
42 GSMA report: 5G in Context, Q1 2022 Data-driven insight into areas influential to the development of 5G May 2022
43 5G and data privacy https://www.gsma.com/publicpolicy/resources/5g-and-data-privacy
44 GSMA Intelligence: Consumer Insights Survey 2019

When considering the issues around collection and use of personal data, it is important to note two key distinctions:

- Privacy laws, where they exist, vary by jurisdiction; although the European Union's General Data Protection Regulation has set a benchmark for many countries, there is no globally interoperable framework. Often, the organisations governed by these laws have an international footprint. This can create uncertainty around the appropriate legal baseline and can be further complicated if the service provider stores and processes data in a third country.
- A second distinction is between the mobile operator and the third-party online services and apps that users can access over the network. These organisations are not subject to the laws and licence obligations relating to the protection of privacy that apply to mobile operators.

Terminology

Personal data – this can mean many things to many people in the online world, and has various meanings defined in law. This document does not seek to reinterpret the law. But when we use the term 'personal data,' we intend it to include (but not be limited to) information that relates to a living individual and:

- is collected directly from a user (e.g., entered by the user via an application's user interface and which may include name, address and credit card details)
- is gathered indirectly (e.g., mobile phone number, email address, name, gender, birth data, location data, IP address, IMEI, unique phone ID)
- concerns a user's behaviour (e.g., location data, service and product use data, website visits)
- is generated by a user and is held on a user's device (e.g., call logs, messages, user-generated images, contact lists or address books, notes, and security credentials)

User – when we refer to user we generally mean the end user of the mobile device who initiates the use of an application or service, and who may or may not be the 'customer' of an application or service provider.

The rules that govern the use of personal data vary significantly, from sector to sector, from technology to technology and from country to country. This can be confusing for people who rightly expect the same protection regardless of who is using their data and how it is processed. In addition, laws can quickly become outdated in the dynamic, rapidly changing digital ecosystem, and the traditional sectoral approach is becoming less relevant.

These inconsistencies in privacy requirements across different services and applications can lead to an experience where users might unwittingly provide easy access to their personal data, leaving them exposed to unwanted or undesirable outcomes.

Furthermore, some online services and application practices will result in consumers 'consenting' to privacy related terms and conditions without reading the notice or understanding the implications of their decisions. According to New Scientist, privacy policies are four times as long as they were 25 years ago.[45] Because of the often-misunderstood distinction between the mobile operators and the other services which users access via their mobile devices, there is also the risk of consumers being unaware of who is handling their data, and in some cases believing their privacy to be better protected than it is in reality.

Deeper dive

Big Data and AI

Increases in computing power, falling costs, and advances in analytics, AI machine learning and related disciplines make it possible to process and analyse huge volumes of data. This allows meaningful insights to be drawn, where appropriate, from mere correlations in the data rather than having to identify causal connections. These capabilities, referred to as big data analytics techniques, represent a sea-change in society's ability to not only create new products and services, but also solve some of the most pressing public policy needs of our time – from road management in congested and polluted urban areas to understanding and preventing the spread of diseases.

Mobile operators are increasingly using data they collect and accessing context data from additional sources for big data services. Therefore, they have an important role to play as responsible stewards of that data and potentially as facilitators in a future marketplace for access to this type of data.

In practice, big data analytics and AI can be used to find common patterns across large data sets through statistical techniques which aggregate across large numbers of users, devices and data. Therefore, to a great extent, these statistical techniques can be considered to be privacy enhancing techniques when applied correctly.

In collaboration with representatives from the mobile ecosystem, the GSMA has identified safeguards that organisations can adopt to identify and reduce privacy risks when engaging in services or projects that involve big data analytics.[46] Additionally, the GSMA has developed a digital toolkit outlining the components required to implement mobile data-driven solutions.[47]

As the adoption of Artificial Intelligence (AI) accelerates, it is vital that AI systems are designed, developed and deployed ethically. The GSMA provides principles that, when applied alongside existing laws, regulations, and privacy principles such as the GSMA Mobile Privacy Principles, can help mitigate ethics and privacy risks associated with AI. Additionally as AI is at the core of operational and business models for an increasing number of mobile network operators. The GSMA AI Ethics Playbook is a practical tool to help organisations consider how to ethically design, develop and deploy AI.

45 https://www.newscientist.com/article/2307117-privacy-policies-are-four-times-as-long-as-they-were-25-years-ago/
46 https://www.gsma.com/publicpolicy/resources/mobile-privacy-big-data-analytics
47 https://aiforimpacttoolkit.gsma.com/

Case Study

In response to the Covid-19 outbreak, strict measures to contain the spread of the virus were implemented in Nigeria. Before Covid-19, approximately four in 10 Nigerians were living below the national poverty line, with millions more living just above, making them vulnerable to falling back. MTN collaborated with the Nigeria Governors Forum to enable data-driven insights to shape resource planning and response measures. Very limited but indicative data was provided to ensure privacy of the customers, which was sufficient to produce the required insights. The datasets were used to predict the worst-case scenario for infections in each state and to support the health committees with local resource planning decisions. The predictive analysis utilised anonymised and aggregated mobile network data, combined with geospatial reference datasets from open-source public data repositories and applied to an epidemiological model. From this, the geographies with the most vulnerable population were identified through the application of anonymised and aggregated mobile money transactions.[48]

Addressing consumer privacy when collecting and using data

The GSMA developed a set of Mobile Privacy Principles, which describe the way mobile consumers' privacy should be respected and protected when they use mobile applications and services that access, use or collect their personal data. The principles do not replace or supersede applicable law but are based on recognised and internationally accepted principles on privacy and data protection.[49] These principles seek to strike a balance between protecting an individual's privacy and ensuring they are treated fairly, while enabling organisations to achieve commercial, public policy and societal goals. Generally speaking, they are flexible enough to accommodate new technologies and business methods as they arise. Of the nine principles, six are particularly relevant to the collection and use of personal data:

- **Openness, transparency and notice**
- **Security**
- **Purpose and use**
- **Children and adolescents**
- **Data minimisation and retention**
- **Accountability and enforcement**

48 https://www.gsma.com/betterfuture/wp-content/uploads/2021/03/GSMA-AI4I-Covid-Response-Report_March2021.pdf
49 GSMA Mobile Privacy Principles (2016) http://www.gsma.com/publicpolicy/mobile-privacy-principles

GSMA Mobile Privacy Principles

Openness, Transparency and Notice

Responsible persons shall be open and honest with users and will ensure users are provided with clear, prominent and timely information regarding their identity and data privacy practices. Users shall be provided with information about persons collecting personal information about them, the purposes of an application or service, and about the access, collection, sharing and further use of a users' personal information, including to whom their personal information may be disclosed, enabling users to make informed decisions about whether to use a mobile application or service.

Purpose and Use

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

User Choice and Control

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

Respect User Rights

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

Data Minimisation And Retention

Only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop applications and services should be collected and otherwise accessed and used. Personal information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous.

Security

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

Education

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

Children and Adolescents

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

Accountability and Enforcement

All responsible persons are accountable for ensuring these principles are met.

Key implications for government, industry and other relevant stakeholders

The GSMA and its members believe that privacy and security are fundamental to building consumer trust in mobile services and are committed to working with stakeholders from across the mobile industry to develop a consistent approach to privacy protection. For services that they provide themselves to their consumers, mobile operators will endeavour to protect digital identities, secure communications and personal data. The wide range of third-party services available through mobile devices offers varying degrees of privacy protection. Therefore:

— To give customers confidence that their personal data is being properly protected, irrespective of service or device, a consistent level of protection must be provided.

— The necessary safeguards should be derived from a combination of internationally agreed approaches, national legislation and industry action.

From the perspective of being transparent and informing consumers industry, data protection authorities and other regulators should:

— Be clear with consumers about what they do protect, and what consumers should expect in terms of privacy.

— Make clear what they have no control over, such as third-party applications and services. For sophisticated consumers, this may be known, but for many segments of consumers it is not.

When legislation and regulations are being formulated or revised:

— Governments should ensure legislation is service and technology-neutral, so that its rules are applied consistently to all entities that collect, process and store personal data.

— Because of the high level of innovation in mobile services, legislation should focus on the overall risk to an individual's privacy, rather than attempting to legislate for specific types of data. For example, the same data element can be used to derive value that can be commercial (e.g., sold to third-party organisations), operational (e.g., inform internal decision-making and resource allocation) or public (e.g., inform disaster recovery efforts).

Consumer choice

Empowering consumers to choose

Many online services are offered to consumers free, whereby the provider earns income from advertising related income streams. To maximise these streams, most online services, from websites to bespoke apps, will use information about the user so that advertisers who want to reach such a profile will bid to place an advertisement (in various formats) in front of that user.

These sort of micro segments and millisecond auctions are increasingly common and rely on the service provider making use of the user-specific information they may have obtained directly or have purchased. While there is clearly a balance to be struck between users sharing some information in return for the use of free services, it is important that users are able to make clear and informed choices about this sharing. Research conducted on behalf of the GSMA shows that mobile users want simple and clear choices to control the use of their information. The GSMA has worked closely with its members to proactively address key mobile privacy challenges and, as part of this, commissioned global research on more than 11,500 mobile users (Brazil, Colombia, Indonesia, Malaysia, Singapore, Spain and the UK). The findings show that mobile users from these countries share similar attitudes and concerns about their privacy.[50] The study found that over 80% of mobile internet users were concerned about sharing their personal data when accessing apps and services. Furthermore, before installing an app, the majority (65%) of app users seek to find out what information the app wants to access on their device, demonstrating a desire to understand how their privacy might be affected. Most mobile users (81%) also want to be asked for permission before third parties access their personal data on their mobile devices, and to have more control over the types of data different companies might access.

50 The "Mobile Privacy: Consumer research insights and considerations for policymakers" paper presents the key research findings and discusses the implications for policymakers. For the detailed report http://www.gsma.com/publicpolicy/mobile-privacy-consumer-research-insights-and-considerations-for-policymakers

Key implications for government, industry and other relevant stakeholders

Three of the nine Mobile Privacy Principles developed by GSMA are particularly relevant to customer choice with respect to their personal information:

- User Choice and Control: users shall be given opportunities to exercise meaningful choice and control over their personal information.
- Respect User Rights: users should be provided with information about, and an easy means to exercise their rights over the use of their personal information.
- Education: users should be provided with information about privacy and security issues and ways to manage and protect their privacy.

However, these principles, even where fully enacted, can only go so far in providing consumers with the required level of choice. Mobile operators have no influence over the privacy terms and conditions that online service providers use. There is a risk that new laws and regulations could have the unintended effect of over-burdening mobile user and exacerbating the 'privacy fatigue' that can result from being asked to consent to conditions that users have not actually read or understood.

For services that they provide, mobile operators will strive to have clear privacy policies and to make it easy to understand and control how personal data is used.

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.

Cross-border transfer of personal data

The third aspect of consumer privacy relates to the jurisdiction(s) where personal data is stored and/or accessed, and the implications of cross-border data flows. Storing and processing data in centralised locations will often enable mobile operators to improve the performance and economics of providing services that may not be viable in a single country operation. Consumers benefit from the many services, innovations and support this enables. When data is moved from one territory to another, this may lead to questions regarding the appropriate legal jurisdiction. Interoperable frameworks and accountability mechanisms can help governments address jurisdictional challenges and facilitate cross-border data flows.

Frameworks such as APEC Cross Border Privacy Rules (CBPR) and the EU's Binding Corporate Rules are setting common, international principles including accountability mechanisms that govern how data should be handled when being transferred between countries. However, their successful adoption is undermined by the implementation by governments of 'data localisation' (also known as 'data sovereignty') rules that impose local storage requirements or use of local technology.[51] Such localisation requirements are sometimes imposed by countries in the belief that supervisory authorities can more easily scrutinise data that is stored locally.

51 Svantesson, D. (2020-12-22), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301, OECD Publishing, Paris. http://dx.doi.org/10.1787/7fbaed62-en

Although some of these rules may seek to protect individual privacy, they are creating a fragmented patchwork of laws and regulations which are both confusing and risk constraining the benefits of an open network infrastructure. These data localisation rules may also have a negative impact on digital trade and global economic growth, for example, data localisation has had a considerable negative impact on employment causing job losses of around 205,000 in Brazil; 372,000 in Indonesia; and 182,000 in South Africa. The negative impact on investment caused by the economic cost of data localisation rules is even more pronounced — with $5 billion lost in Brazil and Indonesia and $4 billion in South Africa.[52]

Addressing the privacy and security of cross-border data flows

Mobile networks generate large amounts of data. Every call and data transfer is logged and processed in order to bill individual users for the services they use. Operational data related to traffic loads, fault logs or customer enquiries (e.g., change of tariff, change of address) is continually generated and stored. As a result, mobile operators rely heavily on data centre storage and processing services.

Ensuring the integrity and security of such data is a major undertaking and requires complex solutions. Many mobile operators, particularly those that are subsidiaries of international groups or that choose to use third-party providers, may find that the best solution is to host and process data for multiple countries in one central location. Doing so allows them to achieve economies of scale and build a more robust solution with greater functionality, security and increased redundancy than would be possible in a fragmented, single-country approach. A centralised approach allows operators to build deeper expertise and implement back-up and redundancy solutions that may not be economically feasible or even possible for a single operation in a single country. Delivering such solutions does of course involve the transfer of consumer data to those multinational data centres which in many cases are located in countries other than that of the original network operator.

While the technical benefits are clear, the legal implications are complex: which countries' data protection rules should apply – the country where the data is processed, the country of the end user, or the country in which the data controller (e.g., the mobile operator) is located?

There are several reasons countries seek to impose data localisation rules, including the belief that supervisory authorities can more easily scrutinise data that is stored locally. An additional common reason is the desire to protect individual privacy and ensure it meets the expectations and standards of that country: an obvious way to enforce this is to require that the data stays in the country. However, there are solutions and principles that can mitigate these risks without restricting data flows and the benefits that ensue.

Restrictions do not necessarily lead to better protection for personal data. A fragmented approach results in inconsistent protection (e.g., differences across jurisdictions and sectors in what can be stored and for how long) and causes confusion impacting the secure management of personal data. Fragmentation through localisation may also create barriers that make investments in security protection prohibitively expensive. Collectively, this may undermine efforts by mobile operators to develop privacy-enhancing technologies and services to protect consumers.

52 GSMA report: Cross-Border Data Flows The impact of data localisation on IoT January 2021 https://www.gsma.com/publicpolicy/resources/cross-border-data-flows-the-impact-of-data-localisation-on-IoT

It is important to restate the distinction here between the personal data that mobile operators have access to and process, versus personal data collected and stored by online service providers and internet intermediaries. As discussed in the section on consumer choice, these services are very different, and the fact that they are operated from outside the country of use in many cases further multiplies the legal complexities. The privacy concerns and issues are just as relevant here, but this is outside the control of mobile operators, both in terms of what data has been transferred by users and how it can be accessed.

A key concern is that cross-border data transfers are currently regulated by a patchwork of international, regional and national instruments and laws. While these adopt common principles, they do not create an interoperable regulatory framework that reflects the realities, challenges and potential of a globally connected world. Data protection rules should be made interoperable across countries and regions to the greatest extent possible. Interoperability creates greater legal certainty and predictability that allows a company to build a scalable and accountable data protection and privacy framework.

Interoperable data protection frameworks would help strengthen and foster appropriate and effective mechanisms to ensure data is managed in ways that safeguard the rights and interests of consumers and citizens. Interoperable data protection frameworks incorporating effective accountability mechanisms can help strengthen and protect important rights that help individuals and economies flourish. For example, efforts to make the APEC CBPR system and EU Binding Corporate Rules interoperable have the potential to benefit industry, digital trade and consumer interests and rights.

Key implications for government, industry and other relevant stakeholders

The international flow of data plays an important role in innovation, competition and economic and social development. Therefore:

- Restrictions and conditions on international dataflows should be kept to a minimum and applied in exceptional circumstances only.
- Cross-border data transfer rules should be risk-based and support measures to ensure data is handled with appropriate and proportionate safeguards while helping realise potential social and economic benefits.
- Regional data privacy initiatives should be encouraged and implemented on the basis of common principles, should support interregional data flows, and should be interoperable with existing APEC and EU approaches and with similar national approaches.
- To the extent that governments need to scrutinise data for social purposes, they should achieve this through existing lawful means and appropriate intergovernmental mechanisms that do not restrict the flow of data.

Mobile operators recognise concerns about keeping data safe and secure and to help ensure individuals' rights are not prejudiced. They also recognise the broader challenges of national and international surveillance. However:

- Governments should only impose measures that restrict cross-border data flows if they are absolutely necessary to achieve a legitimate public policy objective.
- The application of these measures should be proportionate and not be arbitrary or discriminatory against foreign suppliers or services.

The GSMA and its members remain committed to working with stakeholders to ensure that cross-border data flows are managed in ways that safeguard the personal data and privacy of individuals. The GSMA and its members also recognise the importance of addressing challenging issues arising from cross border data flows, including jurisdictional issues.

The mobile industry believes that cross-border data flows are essential to unlock benefits for individuals, organisations, governments and the economy both nationally and internationally. To identify the benefits of free movement of data is not to suggest that there should be no regulation in this area. A shared view by many policymakers, organisations and civil society is that smart data privacy regulation can both enable data flows and protect citizens, providing consumers and policymakers with confidence in digital goods and services. In order to enable the benefits highlighted in this paper, the GSMA would encourage governments to act on the following recommendations[53]:

53 https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf

Recommendation 1: Commit to facilitating cross-border data flows and removing unnecessary localisation measures

Governments should make a firm commitment to facilitating cross-border data flows and removing unnecessary localisation measures in order to realise the benefits of the free movement of data for individuals, businesses and governments.

Public commitment, whether at a national level or within the context of a regional or multilateral body, can set a clear direction and strategic vision to stimulate the digital economy nationally and encourage alignment across the region. Where localisation measures do go ahead, governments should consult with stakeholders regarding how the measures will be interpreted and implemented.

Recommendation 2: Ensure privacy frameworks are fit for a digital age

Policymakers should ensure that legal frameworks effectively address data protection concerns in their country. Such frameworks should describe citizens' and consumers' privacy rights and the obligations on organisations when collecting, analysing, processing and storing data.

In order to be fit for a digital age, national privacy frameworks should be based on "the core set of data protection principles that are said to be at the heart of most national [privacy] laws and international regimes"[54]. Such approaches should reflect consumer concerns over data privacy and security[55] and should operate on a technology- and sector-neutral basis so customers are assured of consistent treatment of their data. They should also provide for the creation and resourcing of a national data protection authority.

Privacy regulation should focus on risks of harm to individuals and incorporate measures to ensure accountability on the part of organisations collecting data, while providing for flexible implementation to allow organisations to innovate rapidly, achieve larger scale and reduce their costs of production.

Recommendation 3: Review legacy sector-specific privacy rules

Historically, operators have often been the subject of sector-specific restrictions on international data flows. The core purpose of telecoms operators is connecting people regardless of location and distance. While telecommunications started with telegrams and progressed to voice calls, SMS and emails, it now involves the exchange of data at scale, and operators' infrastructure and services carry this data. With data being a driving force in the digital economy, it no longer makes sense to treat telecoms operator data differently from data generated by other providers of electronic communications or indeed by the wider digital economy. Enacting a national privacy framework that is fit for a digital age provides an opportunity for a review of legacy sector-specific rules on privacy to ensure they are still required.

54 UNCTAD, Data protection regulations and international data flows: Implications for trade and development, 2016. See: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

55 See research published by the GSMA: https://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf

Recommendation 4: Encourage regional data privacy initiatives

Supranational bodies including APEC and the European Union have already adopted regulatory models for data protection and privacy while ensuring that data can flow freely across the region. These models provide a proportionate and effective response for policymakers who wish to protect citizens and consumers while also supporting future international trade in physical and digital goods and services.

Regional data privacy initiatives should be encouraged and implemented on the basis of common principles, should support interregional data flows, and should be interoperable with existing APEC and EU approaches[56] and with similar national approaches. Regional initiatives build regulatory capacity in data privacy and the development of industry best practice for the treatment of data. This will build confidence between countries, facilitate sharing of best practice between policymakers and allow data privacy regulators to detect and address non-compliance more easily.

Addressing national consumer privacy and security concerns consistently by region will facilitate cross-border data flows while providing data governance mechanisms to ensure industry accountability nationally and internationally.

Recommendation 5: Avoid localisation by addressing foreign surveillance concerns pragmatically

Governments should consider the range of options available to protect data that is deemed sensitive, rather than mandating its localisation. These options include encryption, anonymisation and aggregation, and, in certain circumstances, may include the specification of particular regional hubs for specific types of data.

Recommendation 6: Avoid localisation by addressing law enforcement and national security concerns pragmatically

Governments should engage with initiatives such as the additional protocol to the Budapest Convention on Cybercrime, the US CLOUD Act and the EU eEvidence proposal to provide clear and predictable frameworks that give organisations legal certainty and give authorities more direct and timely access to the offshore data they need, thereby removing the need for localisation measures.

Adopting these recommendations will:

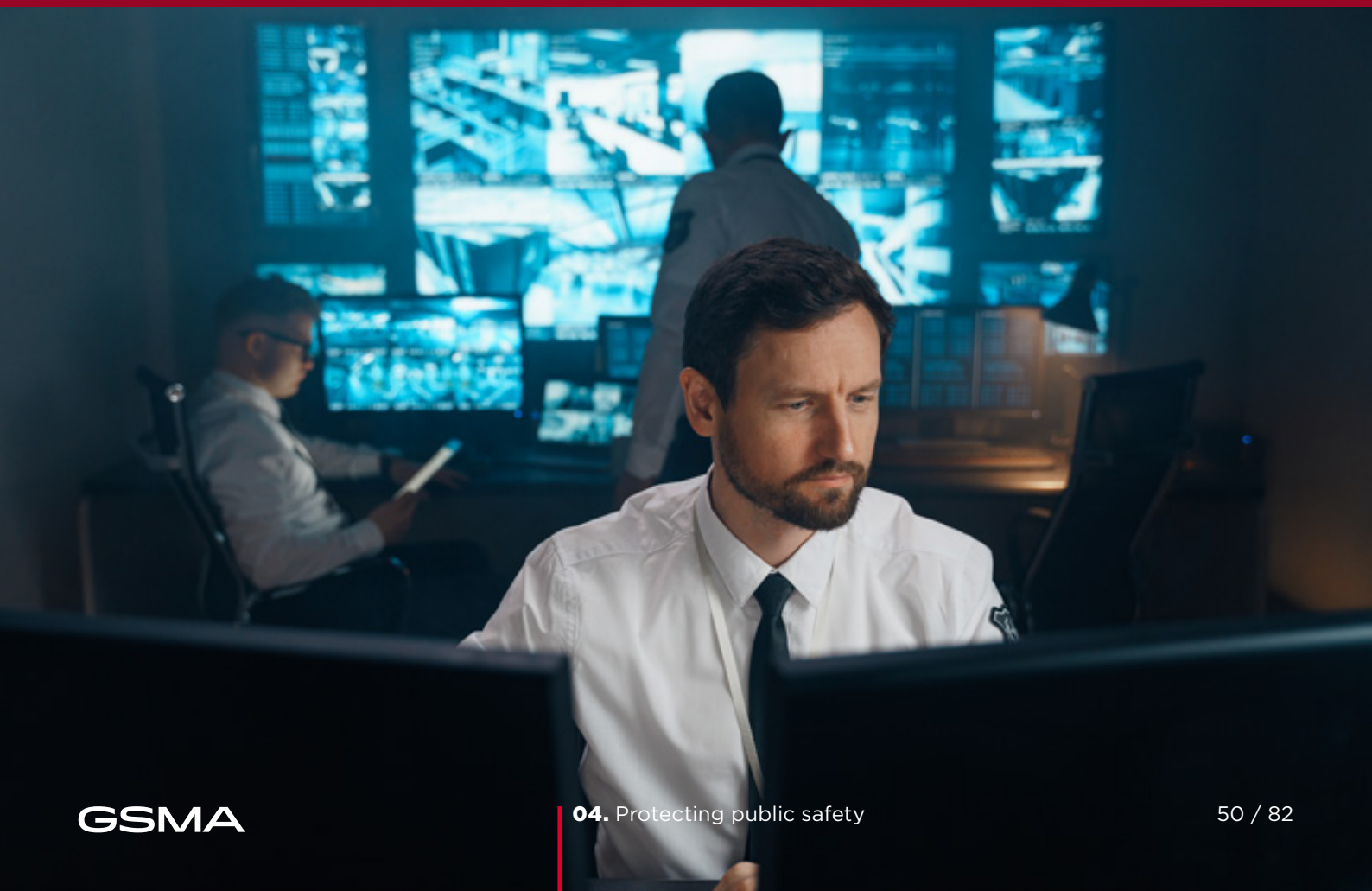
- Enable the digital economy to operate efficiently and deliver social and economic benefits more rapidly in multiple nations and regions;
- Provide people with access to a global range and high quality of services, overcoming national market constraints where they exist; and
- Permit established businesses, including telecoms operators, to adopt data-driven digital transformation strategies to reduce costs and consequently the prices for digital and physical goods in the marketplace.

56 In particular, be interoperable with APEC Cross-Border Privacy Rules (CBPRs), EU Binding Corporate Rules (BCRs) and the associated common reference model established by a joint APEC / EU working party

04

Chapter 4

Protecting Public Safety



Mobile networks are core to critical national infrastructure, playing an important role in protecting the general public and society as a whole.

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.

For example, emergency services responding to major incidents rely on mobile networks to communicate with each other, while members of the public use mobile devices to report incidents as they occur.

In accordance with local legislation, as well as mobile licence obligations, mobile network operators are required to assist law enforcement agencies in their work to protect to protect public safety. For example, law enforcement agencies may be granted court orders to monitor communications to, from or between specific suspects as part of criminal investigations. Therefore, as a standard feature of most licences, mobile network operators are required to provide the technical means to meet their legal obligations to assist law enforcement. In most countries, such interventions are limited and subject to due legal process.

The Universal Declaration on Human Rights (UDHR)[57] and the International Covenant on Civil and Political Rights (ICCPR)[58] recognise that individuals worldwide have the right to communicate with each other privately and also the right to freedom of expression within the confines, boundaries and public morals of any given nation state. International human rights instruments also specify that these rights can only be restricted in very limited predefined circumstances and that any limitation should always be necessary and proportionate to the perceived threat.

There can be tension between national security and law enforcement objectives to protect public safety and the rights to privacy, freedom of expression and access to information. These potentially conflicting needs, in most countries, result in the default position that individuals should be able to communicate freely and in private and that interventions and interruptions should only be by necessary and proportionate exceptions, and subject to due legal process. Most countries have safeguards to prevent abuse and overuse of the powers that are capable of undermining privacy of communication.

This section highlights three typical examples of public safety interventions and the issues that arise when the various parties seek to address them in practice, specifically:

- **Law enforcement assistance requests, with a focus on the need for transparency and safeguards**
- **Service restriction, with a particular focus on the use of mobile signal inhibitors**
- **User registration, with a focus on prepaid SIM card consumer registration**

Each of these issues has a number of important implications for government, industry and other stakeholders and these are also outlined in detail later in this chapter.

Law Enforcement Assistance Requests

Complying with law enforcement assistance requests

Mobile network operator licences generally set out the obligations of network operators to support law enforcement and national security activities of the issuing country. Where they exist, such laws and licence obligations typically require mobile network operators to retain data[59] about their consumers' mobile service use and disclose it to law enforcement agencies on lawful demand, and also to have the ability to intercept live consumer communications on lawful demand.

Laws typically define the conditions, and at times the process, under which law enforcement agencies can request mobile network operators to provide access or information about communications over their network and provide the legal reference point

57 The Universal Declaration of Human Rights (UDHR) was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected. The right to privacy is captured in Article 12 and the right to freedom of expression in Article 19. For the UDHR, see: http://www.un.org/en/universal-declaration-human-rights/

58 The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty adopted by the United Nations General Assembly on 16 December 1966 and has been in force since 23 March 1976. The right to privacy is captured in Article 17 and the right to freedom of expression in Article 19. For the treaty, see: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en

59 Annulling the Directive in 2014, the European Court of Justice (CJEU) ruled that "general retention of personal data" as ordered by the EU Data Retention Directive violated the right to privacy outlined in the Charter of Fundamental Rights of the European Union. In December 2016, the CJEU confirmed its position and ruled that national laws which are corresponding to the Data Retention Directive are in breach of the EU acquis

that guide mobile network operators in how to respond to these requests. In November 2016, the UK passed new legislation[60] that clarifies these boundaries. While there are differing views on the acceptability of the powers the new legislation gives to UK law enforcement agencies, it is important that the rules were debated and enacted publicly. In some countries, there can be a lack of clarity in the legal framework to regulate the disclosure of data or lawful interception of consumer communications. This creates challenges for industry in seeking to protect the privacy of customers' information while honouring their licence obligations to assist law enforcement.

Over the last few years there has been an important global public debate about the scope, necessity and legitimacy of the legal powers that government authorities use to access the communications of private individuals. Telecoms networks and service providers have worked together for over ten years on the privacy and freedom of expression issues that arise from this type of access. For example, in 2011 a group of mobile network operators and vendors formed the Telecommunications Industry Dialogue (ID) and defined principles outlining the responsibility of telecommunications companies in safeguarding freedom of expression and privacy. One outcome of the work of the ID has been that a number of the company members have decided, wherever possible, to proactively disclose information on the nature and volume of government access requests they received in each country where they have operations.[61] The ID existed until 2017 when many of its members joined the Global Network Initiative.[62]

Legislation often lags behind technological developments[63] and misunderstandings can arise about the level to which mobile network operators have the technical capacity to intercept communications. Intercepting standard phone calls or SMS messages to and from specific users is technically possible and lawful interception requirements and capabilities have been described in the global mobile standards for decades.

However, communications between users using an internet-based platform are generally beyond the reach of mobile network operators, even if their networks are transporting the traffic. Some popular services, such as WhatsApp, WeChat, and Signal are encrypted, with messages not stored by the mobile network operators nor decryption keys made available to them. This means that, even on receipt of lawful requests, the network operators cannot access, and therefore cannot provide, the content of the messages (see example of WhatsApp service restriction in Brazil in the next section).

Mobile network operators recognise the importance of the sovereignty and legitimacy of governments in the defence of their citizens' safety. In their pursuit of this objective, the interception of communications for law enforcement or security purposes should take place only under a clear legal framework, compatible with human rights principles of necessity and proportionality, and using the proper process and authorisation specified by that framework.

Finally, the responsibility and often also the cost of activities undertaken by mobile network operators in support of public safety needs are increasingly being absorbed by the operators. An extreme example is El Salvador, where a 5% tax on telecommunications services was approved in November 2015 to finance general government security plans.[64] While fiscal policy is a matter for governments to decide, taxing the operators of the very mobile network infrastructure that supports security is counterproductive in that it diverts funding away from the one of the parties already investing in public safety.

60 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

61 However, many countries expressly forbid mobile network operators from making public even high-level details about the nature or volume of intercept requests they have received.

62 About GNI – Global Network Initiative

63 GSMA Mobile Policy Handbook: Government Access

64 Telecompaper, 2016 El Salvador introduces 5% telecoms tax

Key implications for government, industry and other relevant stakeholders

Mobile network operators have a responsibility to ensure that they only respond to lawful requests (i.e., judicial mandates) received from government agencies that are legally authorised and have followed due process, with appropriate safeguard mechanisms. Therefore, governments should ensure they have a proportionate legal framework that clearly specifies the surveillance powers available to national law enforcement agencies.[65]

- Any interference with the right to privacy must be in accordance with the law, i.e., the retention and disclosure of data and the interception of communications for law enforcement or security purposes should take place only using the proper process and authorisation specified by that framework.[66]
- There should be a legal process available to telecommunications providers to challenge requests which 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.[67]
- 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 and the withdrawal of network access and services.[68]
- In addition, the costs of complying with all laws covering the interception of communications, and the retention and disclosure of data, or access restriction to networks or services should be borne by governments, as is the case in some countries today. Such costs and the basis for their calculation should be agreed in advance.[69]

The GSMA and its members are supportive of initiatives that seek to increase government transparency and the publication by government of statistics related to requests for access to customer data[70] where possible.

65 GSMA Mobile Policy Handbook: Government Access
66 ibid
67 ibid
68 ibid
69 ibid
70 ibid

Transparency (authority request disclosure) Reporting

Why report...

The Telecommunications Industry Dialogue (ID) was founded by a group of telecommunications operators and vendors to jointly address freedom of expression and privacy rights in the telecommunications sector in the context of the UN Guiding Principles on Business and Human Rights..

One of the key purposes of the ID was shared learning and to build on the notion of transparency, ID operators AT&T, Millicom, Orange, Telenor Group, Telia Company, and Vodafone Group were some of the first mobile network operators to regularly publish reports that disclose information about the law enforcement requests they received.

What is reported...

Typically, transparency reports seek to:

- Explain the legal frameworks and law enforcement capacity within the markets of operation.
- Explain the policies and processes followed when responding to demands from agencies and authorities.
- Where possible, disclose statistics on the number of law enforcement requests received for consumer data in certain countries or regions.

What are the limitations...

Law enforcement and national security legislation often includes stringent restrictions preventing operators from disclosing any information relating to agency and authority demands received, including disclosure of aggregate statistics. In many countries, operators are also prohibited from providing the public with any insight into the means by which those demands are implemented. These restrictions can make it very difficult for operators to respond to public demand for greater transparency.

Operators do however believe that measuring the number of requests received from authorities, with all its flaws, is the most sensible measurement available, without making it too complex. Additionally, it should be emphasised that only the governments that make these requests to communications providers are able to give the full picture of the extent of requests.

Since the original launch of the ID in 2013 many mobile network operators have published transparency reports. Access Now, a global digital rights organisation, updates a database called the Transparency Reporting Index, which includes links to reports of mobile network operators and other companies.[71]

71 https://www.accessnow.org/transparency-reporting-index/

Service Restriction Orders and Signal Inhibitors

Service restriction orders

In addition to requests to intercept communications, from time to time mobile network operators receive orders from government authorities to restrict services on their networks ('service restriction orders' or 'SROs'). These orders require them to shut down or restrict access to their mobile network, a specific network service or a third-party service accessed via their network. Orders may include blocking particular mobile or internet services or content, restricting data bandwidth and degrading the quality of SMS or voice services. As well as being obliged by law to comply, in some cases mobile network operators would risk criminal sanctions (including imprisonment of senior staff) or the loss of their licence if they were to disclose that they had been issued with the SRO or refuse to carry out such orders.

SROs can have a number of serious consequences. For example, national security can be undermined if the powers are misused (i.e., relying on network restrictions to prevent terrorist attacks deprives both citizens and law enforcement alike the opportunity to use communication tools in the fight against terrorism) and public safety can be endangered if emergency services and citizens are not able to communicate. Freedom of expression, freedom of assembly, freedom to conduct business and other human rights can be impacted. Service restriction orders can affect the ability of society to function, individuals to transfer funds to friends and family and businesses to transact, pay 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 due to the suspension of services, as well as damage to their reputation, but their local staff can also face pressure from authorities and possibly even retaliation from the public.

An example of this occurred in Brazil, where the messaging service, WhatsApp, was allegedly insufficiently supportive of various criminal investigations.[72] In response, the government required mobile network operators within Brazil to restrict access to the WhatsApp services on three separate occasions since December 2015.[73] The primary impact of this action was to prevent the 100 million users in Brazil from using the country's most popular mobile messaging app. Each of the rulings was reversed after appeals to higher courts due to their disproportionate impact. WhatsApp and its parent company, Facebook, maintain that cooperation would be technically impossible as no communications are stored or, even if they were, they could not be accessed due to the use of end-to-end encryption. However, many of the impacted users often blame mobile network operators for the disruption to the service.

More extreme examples of network shutdowns have taken place in certain countries, sometimes to restrict the ability of political opponents of governments to organise.[74] As a first step, mobile network operators urge governments to be transparent with their citizens about the government role in shutting down or restricting networks and services, and the legal justifications for any restrictions. Importantly, shutdown orders should permit companies to disclose in a timely manner to their customers those services that have been restricted pursuant to a government order.[75]

72 Financial Times, 2016: "WhatsApp ban ignites Brazil censorship fears"

73 The Guardian, 2016. "WhatsApp officially un-banned in Brazil after third block in eight months"

74 Examples of shutdowns can be found within the Internet & Jurisdiction Retrospective Database. http://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTYtMTEifQ

75 The Telecommunications Industry Dialogue and Global Network Initiative joint statement: http://www.telecomindustrydialogue.org/global-network-initiative-telecommunications-industry-dialogue-joint-statement-network-service-shutdowns/

Use of signal inhibitors

Another form of restriction to mobile communication is to use signal inhibitors, also known as jammers. These are devices that generate interference in order to intentionally disrupt radio-based communication services by interfering with the communication between the mobile terminal and the base station. Typically, these crude tools are used to prevent communications in penitentiary centres, or between terrorists or groups deemed as politically subversive, often where there are mass public gatherings. Signal inhibitors at times are also used a tool to prevent the use of mobile devices in prohibited areas. For example, in Latin America, signal inhibitors are used to prevent the illegitimate use of mobile devices in sensitive locations, such as prisons. However, blocking the signal does not address the root cause of the problem — mobile devices illegally ending up in the hands of prison inmates. Furthermore, the nature of radio signals makes it virtually impossible to ensure that the interference generated by inhibitors is confined. Consequently, the interference caused by signal inhibitors affects citizens, services and public safety organisations. It has a knock-on effect for many other users, such as those who live and work in the vicinity of prisons, who are unable to use mobile services. There is a negative impact for mobile network operators due to the cost of the jammers, the loss of legitimate revenue, and, not infrequently, the negative reputation caused by service disruptions.

Any disruption of communications networks, network services, or internet services (such as social media, search engines, or news sites) has the potential to undermine public safety and restrict access to vital emergency, payment and health services. For example, service restrictions can limit the ability of mobile users to contact emergency services via numbers such as ‘112’ or ‘911’, and they can interfere with the operation of mobile connected alarms or personal health devices. For these reasons service restrictions should be kept to a minimum and consideration needs to be given to the subsequent negative side-effects for all users.

Key implications for government, industry and other relevant stakeholders

Whereas the GSMA understands and supports the appropriate use of lawful interception to enhance public safety, the GSMA discourages the use of SROs and signal inhibitors.

Governments should only resort to SROs in exceptional and pre-defined circumstances, and only if absolutely necessary and proportionate to achieve a specified and legitimate aim consistent with internationally recognised human rights and relevant laws.[76] There are further points that should be observed:

- In order 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 judicial or other authority in accordance with administrative procedures laid down in law. They should allow mobile network operators to investigate the impacts on their networks and customers and to communicate freely with their customers about the order. If it would undermine national security to do so at the time when the service is restricted, citizens should be informed as soon as possible after the event.[77]
- Governments should seek to avoid or mitigate the potentially harmful effects of SROs by minimising the number of demands, the geographic scope, the number of potentially affected individuals and businesses, the functional scope and the duration of the restriction. For example, rather than block an entire network or social media platform, it may be possible for the SRO to target particular content or users. In any event, the SRO should always specify an end date. Independent oversight mechanisms should be established to ensure these principles are observed.[78]
- Mobile network operators can play an important role by raising awareness among government officials of the potential impact of SROs. They can also be prepared so that if they receive an SRO they can work swiftly and efficiently to determine the legitimacy of the SRO, whether a judicial authority has approved it, whether it is valid and binding and whether there is opportunity for appeal and they can work 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 (e.g., escalate to senior company representatives).[79]
- All decisions should first and foremost be made with the safety and security of mobile network operators' customers, networks and staff in mind and with the aim of being able to restore services as quickly as possible.[80]

76 GSMA Mobile Policy Handbook: Service Restriction Orders
77 ibid
78 ibid
79 ibid
80 ibid

The GSMA and its members are committed to working with governments to use technology as an aid for keeping mobile devices out of sensitive areas, as well as cooperating on efforts to detect, track and prevent the use of smuggled devices. However, it is vital that a long- term, practical solution is found that does not negatively impact legitimate users, nor affect the substantial investments that mobile network operators have made to improve their coverage.[81]

- Signal inhibitors should only be used as a last resort and only deployed in coordination with locally licensed mobile network operators. This coordination must continue for the total duration of the deployment of the devices to ensure that interference is minimised in adjacent areas and legitimate mobile device users are not affected.[82]
- Furthermore, regulatory authorities should ban the use of signal inhibitors by private entities and establish sanctions for private entities that use or commercialise them without permission from relevant authorities.[83]
- 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. In addition, strengthening security to prevent wireless devices being smuggled into sensitive areas, such as prisons, is the most effective measure against the illegal use of mobile devices in these areas, as it would not affect the rights of legitimate users in the vicinity of mobile services.[84]

81 GSMA Mobile Policy Handbook: Signal Inhibitors
82 ibid
83 ibid
84 ibid

Deeper dive

Mitigating the impact of service restriction orders

In emergency situations, government authorities in some countries are within their powers to demand extreme responses from network operators, such as complete or partial shutdowns of network and/or services for any period of time. When national security is cited as the reason for such requests, strong sanctions for non-compliance are likely to apply. However, some network operators work diligently on government requests to minimise the potential impact on freedom of expression and privacy. **The following are three examples of this:**

1. On June 1, 2014, government authorities contacted Orange by telephone in one of its African markets and requested that it suspend SMS services throughout the country. In order to verify the legal basis for this request, Orange asked that the order be submitted in writing. On the following day, the country's four telecommunications operators received a written order, which cited the pertinent law, was signed by the authority with jurisdiction, and indicated that sanctions could result from non-compliance. The order was subsequently published in a pan-African newspaper. The companies complied with the order, resulting in the suspension of SMS services until July 24. The company learned several lessons as a result of this event, including the importance of cooperation among peer companies in responding to government demands that present irregularities, and that transparency can aid a company in responding to these demands. (Telecommunications Industry Dialogue, 2016. "Input to UN Rapporteur David Kaye")
2. At AT&T, such requests are evaluated by employees (including AT&T lawyers and, where necessary, local counsel familiar with applicable law) who are trained to confirm that requests are duly issued by an appropriate entity, under valid legal authority and are otherwise in compliance with applicable requirements. The company rejects government demands that do not satisfy these requirements. Where appropriate, it will seek clarification or modification of a request or object to a government demand or court order in the appropriate forum. These efforts help minimise the potential impact that government requests may have on AT&T customers' privacy and on their ability to communicate and access information of their choice. (Telecommunications Industry Dialogue, 2016. "Input to UN Rapporteur David Kaye")
3. The security situation in the Central American operations for Millicom was challenging in 2015. Since the previous year, authorities in Guatemala, El Salvador and Honduras have laws that oblige all telecom operators to shut down services or reduce signal capacity in and around prisons, as authorities suspect that crime gangs continue to operate from inside prisons by using mobile devices that have been smuggled onto the premises. Telecom operators were originally requested to shut down base station towers that serve large areas, also affecting populations living in the vicinity of the correctional facilities as well as disrupting everyday activity, such as the use of ATMs.

   The company actively engaged with the authorities and industry peers, focusing on finding alternative solutions that would address the issue in ways that would not affect the population living in the vicinity of prisons. These included everything from new network coverage design around prisons to third party solutions that work similarly to jammers to restrict signals in specific physical areas, to the relocation of prisons outside of densely populated areas.

   As a result, by the end of 2015, in Guatemala and Honduras, all restrictions of mobile device signals within prisons were implemented in a more targeted manner, affecting only the inside of the prison buildings. (Millicom, 2016. "Law Enforcement Disclosure Report 2016")

Mandatory Prepaid SIM Card Registration

The third area of public safety that has been the subject of much debate in recent years is mandatory prepaid mobile SIM registration, a policy that a number of governments have adopted in recent years which requires consumers to provide proof of identity in order to activate a prepaid mobile SIM card. Many governments continue to perceive this policy as an important way to address national security concerns, despite the lack of published empirical evidence showing a direct link between the introduction of such policies and a reduction in crime-related activities. Some governments have argued that non-registration enables criminals to take advantage of anonymity for a variety of illegal activities e.g., demanding ransom following a kidnapping, or to plot terrorist attacks. Such anonymity is perceived as offering a lower risk of tracing the use of a mobile SIM back to the actual user. In response, a number of governments have mandated the need for mobile network operators to register both existing and all future pre paid customers.

Governments take very different approaches to applying proof-of-identity policies, which means that locally licensed mobile network operators are subject to different requirements in each country.

At the end of 2020, 72 per cent of mobile subscriptions were prepaid[85] and the number of countries where mandatory pre paid SIM registration policies are in place increased to 157. When implemented, such exercises have had a number of unintended consequences, including:

— The exclusion of users without the necessary identity documentation, often the poorest and most vulnerable, from being able to access mobile services. Around one billion people globally who do not have the means to prove their identity, accessing SIM cards and mobile services in one's own name remains a challenge, particularly in the countries where SIM registration requirements are mandatory. Depending on the country and the availability of standard identity documentation this can be a major hurdle.[86]

— The potential for fraudulent registration by criminals wishing to remain anonymous leading to an increase in mobile device theft and the emergence of an illegal market for stolen SIM cards.

— Increased concerns of consumers related to the access, security, use and retention of their personal data, particularly in the absence of national laws on privacy and freedom of expression. Although many of the countries mandating SIM registration maintain a data protection and/or privacy framework (64 per cent), there is still a significant proportion of countries that are either considering introducing a data protection and/or privacy framework or do not have one at all.[87]

85 GSMA Intelligence, prepaid penetration (prepaid connections, Q3, 2020)

86 GSMA report 'Access to Mobile Services and Proof of Identity 2021. Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19' April 2021 (https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf)

87 ibid

Case Study

Industry Collaboration

In 2020, many governments relaxed regulations during the COVID-19 pandemic to facilitate digital and financial inclusion. One of these regulatory changes, flexible Know Your Customer (KYC) and on-boarding, was the focus of GSMA Digital Identity programme research due to the link between ID requirements and access to mobile services (i.e., mobile money) through mobile wallets. The purpose of flexible KYC and on-boarding was to encourage more people to use digital financial services rather than cash, thus reducing contact between mobile money users, agents and merchants. The GSMA conducted exhaustive research with an array of stakeholders from organisations including mobile network operators, central banks and telecom regulators in five countries to understand how the regulatory changes came about and the early impacts on individuals and the private and public sectors. Examples of good outcomes include: in Columbia, existing mobile financial services and remote on-boarding processes accelerated Colombia's response to COVID-19. In Jordan, policy relaxations highlighted the importance of digitisation and faster adoption of digital financial services. Online platforms also became more robust. In Senegal some mobile network operators supported the UN World Food Programme (WFP) to digitise their food assistance, providing an estimated 40,000+ families with aid to their mobile wallets.

An increasing number of governments have introduced mandatory registration of prepaid SIM card users, primarily as a tool to counter terrorism and improve law enforcement.[88] As of January 2020, GSMA research found that the governments of 155 countries mandated SIM registration policies.[89] However, to date, there has been no empirical evidence that mandatory SIM registration directly leads to a reduction in crime.[90] Despite the lack of any empirical evidence, many governments believe mandatory SIM registration does help in the fight against crime and terrorism. Typically, where a mandate to shift to the registration of prepaid SIM users is in place, the implementation cost is passed on to the mobile network operators. This can be significant and may impact mobile network operators' ability to invest in serving lower spend customers. A number of countries, including the UK, have looked[91] in detail at such programmes and concluded that the costs to society (in the form of bureaucratic burden and registration databases) outweigh the benefits and have decided not to adopt this policy. These are national decisions and are dependent on national circumstances and may also be dependent on the issues the registration is targeted to address.[92]

On the positive side, SIM registration can allow consumers to access value-added mobile and digital services that would otherwise be unavailable to them as unregistered users (such as mobile money, digital identity and e-Government services). In order to facilitate these benefits and create valuable outcomes for consumers, mobile network operators and governments need to offer services that encourage customers to register voluntarily.

It is important not to confuse the unintended negative consequences of a mandatory registration policy in a given country with the potential benefits that voluntary SIM user registration can deliver for individual consumers. None of these benefits and positive outcomes depends on SIM registration being mandated by governments. Instead, they can be achieved through the voluntary registration of customers who choose to register their prepaid SIM card in order to access services they consider valuable, such as mobile money, m-commerce or e-Government services. Voluntary registration does however still depend on those consumers having access to the required proof of identity documents.

88 GSMA Mobile Policy Handbook: Mandatory Registration of Prepaid SIMs
89 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf
90 GSMA, 2016: Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice
91 Lord West of Spithead in response to a parliamentary question from Viscount Waverley on the mandatory registration of SIM card users: https://www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones
92 GSMA, 2016 Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice

Case Study

Alternatives to registration – Mexico

In 2009 Mexico introduced mandatory SIM registration ('RENAUT') with the objective of addressing criminal activities.

When the 'RENAUT' rules came into effect, there were significant ongoing concerns over privacy and data security and problems registering large portions of the population who lacked official ID papers, against very short implementation timescales. The solution also failed to address criminal activity and drove up handset theft.

Following consultation with the industry, academics and NGOs, the RENAUT registration programme was stopped in 2012. The database was decommissioned and the significant financial investment by all the mobile network operators and the authorities was written off. An alternative programme was introduced into the Telecommunications and Broadcasting Law to address the unique Mexican market situation, which has been in effect since 2014.

The new Telecommunications and Broadcasting Law, and other regulatory provisions do not require a user to provide registration details to use pre paid services. Rather, the law leverages the several obligations on mobile network operators (e.g., lawful intercept) to help the government and security services address criminal activities.[93]

93 GSMA, 2016 Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice

When SIM registration is mandated, existing customers should be notified about the need to register their SIM cards, how to do so and the consequences if they do not (e.g., that their SIM card may be deactivated if they fail to register). In this case, SIM registration must be implemented in a pragmatic way that takes into account local market circumstances. The relevant local market factors include whether citizen access to national identity documents is widespread throughout the country, whether the government maintains robust citizen identity records and whether mobile network operators are able to verify customers' identity documents.

Key implications for government, industry and other relevant stakeholders

While registration of prepaid SIM card users could offer valuable benefits to citizens and consumers, it should not be made mandatory. Where a decision to mandate the registration of prepaid SIM users has been made, governments should take into account global best practices and allow registration mechanisms that are flexible, proportionate and relevant to the specific market, including the level of official identity documentation penetration in that market.[94]

If these conditions are met, the SIM registration exercise is more likely to be effective and lead to more accurate consumer records. Furthermore, a robust consumer verification and authentication system can enable mobile network operators to facilitate the creation of digital identity solutions empowering consumers to access a variety of mobile and non- mobile services. Given the large existing customer bases in all countries, careful consideration needs to be given to the magnitude of the task and how long it would take to register users in order to minimise the burden on the customers and the potential disruption to services.

The GSMA urges governments that are considering the introduction or revision of mandatory SIM card registration to take the following steps prior to finalising their plans:

- Consult, collaborate and communicate with mobile network operators before, during and after the implementation exercise.
- Balance national security demands against the protection of citizens' rights, particularly where governments mandate SIM registration for security reasons.
- Ensure there are appropriate privacy safeguards and effective legal oversight to protect customers' data and privacy.
- 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 administratively 'light' registration processes.
- Allow and/or encourage the SIM-registered customer to access other value-added mobile and digital services.
- Support mobile network operators in the implementation of SIM-registration programs by contributing to joint communication activities and to the operational costs.

94 GSMA Mobile Policy Handbook: Mandatory Registration of Prepaid SIMs

Deeper dive

Private-public partnerships to registration in Latin America

During 2009 in Ecuador and December 2016 in Argentina, the National Regulatory Authorities (CONATEL and ENACOM respectively) requested that the SIM registration procedure of all consumers be cross-checked and validated with a national or private identity register agency. In each case, Telefónica worked closely with government to deploy a solution suitable to consumers, government and their own needs.

In Ecuador, Telefónica implemented the registration process using an automated system called "Interactive Voice Response" (IVR). The voice service improved upon the previous procedure, which required a cross-check of the consumer's identity against the "Registro Civil."

In Argentina, Telefónica developed an app that is triggered once a SIM card is inserted into the mobile device. This app is used to collect the SIM information along with the mobile user's personal ID. This digital system is being used to create a database that captures the unique link of the owner to the SIM and mobile device SIM and mobile device.

Through these experiences of working in partnership with the relevant national authorities, Telefónica took away the following three key lessons:

1. There are several ways to validate the SIM registration process. Mobile network operators should develop the one that they consider most appropriate.
2. The planned schedule is critical to achieve a successful implementation. For example, in Ecuador the mobile network operators and the regulator worked together to implement a "statistical phase" that allowed the real needs to be assessed in order to avoid over-regulation.
3. A close private-public partnership and collaboration between mobile network operators and government is required to consider implementation alternatives and develop the one that best meets the needs of all stakeholders in a balanced way.

05

Chapter 5

Protecting Mobile Network Security and Device Integrity

Underpinning safe and secure use of mobile services is the security and resilience of the network infrastructure.

Protecting Mobile Network Security and Device Integrity

Industry players need to work together and coordinate with international law enforcement agencies and national security authorities 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 source network equipment that is securely designed, developed and supported and 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

Mobile network operators safeguard the confidentiality, integrity and availability of communications across the network by securing critical assets (hardware, software and data) and preventing unauthorised access or intrusion to any of the constituent nodes or links. Since the end-user mobile device is the primary access point to the network from a user's perspective, protecting the integrity of mobile devices is a critical requirement. By necessity, mobile networks are accessible to a very wide range of users, via a variety of devices and connection protocols. They must also interconnect with many other communications networks around the world (fixed, mobile, internet service providers and enterprise) in order to offer the anywhere-anytime functionality of modern networks. Protecting networks and devices is therefore highly complex in practice.

The rapid evolution of mobile communications over the past decade has led to not only convergence of mobile and fixed network connectivity but also the exposure of mobile networks to new interfaces outside a network operator's control. 5G is ushering in an era in which connectivity is more fluid and flexible, with 5G networks adapting to applications and performance tailored precisely to the needs of users.

By 2030, most markets will have at least one 5G network and mobile 5G connections are expected to surpass five billion, accounting for more than half of total connections.[95] The mobile industry is enhancing network and service security through network function design as well as through deployment strategies. New authentication capabilities and enhanced subscriber identity protection are resulting in significant security improvements compared with legacy generations. However, 5G capabilities are likely to co-exist with previous generations of mobile infrastructure for some time, in which case, both existing and new infrastructure will need to be secured.

Different types of threats (Figure 5) have the potential to undermine the integrity of networks through unauthorised interception, impersonation or service interruption. The mobile industry has been responding to these threats primarily by strengthening security hygiene, encouraging transparent debate on the balance between convenience and security, and building ever more sophisticated security functionality into the technical standards and protocols as each new generation of mobile network has been developed and deployed.

This section of the report addresses a number of security considerations that affect networks and devices and that have the potential to compromise the security required to keep customer communications safe and secure:

- Network security, including physical security and signalling, interconnect and operational security
- Mobile device security and integrity, including malware and software (both proprietary and open source code)
- 5G, IoT and future network developments, including cloud and virtualisation as well as supply chain

Each of these has important implications for government, industry and other stakeholders, outlined later in this chapter.

Figure 5
Protecting networks

SAFEGUARD OBJECTIVE	DESCRIPTION OF THREAT	EXAMPLE ATTACK
Integrity avoid data being altered	Unauthorised tampering	MAN-IN-THE-MIDDLE (MITM)
Confidentiality keep data private	Unauthorised access	EAVESDROPPING
Availability keep network and data available to genuine users	Destruction, theft, removal, or loss of data, or networks become unavailable	DENIAL OF SERVICE (DOS)

95 GSMA report '5G in Context, Q4 2021 Data-driven insight into areas influential to the development of 5G' (March 2022)

Physical network infrastructure

The first step in securing mobile networks is the physical infrastructure itself, such as the cell sites, the backhaul network transmission and core network assets.

For example, there are key functions within a network, such as the register of authorised users, which need to be secured since they represent single points of vulnerability, whether exposed to malicious attack or technical failure. Mobile network operators and equipment vendors continue to develop and deploy new solutions to make these more robust, and have been largely successful to date, but this requires ongoing investment in the development and deployment of new functions and features.

The use of false mobile base stations, or IMSI (international mobile subscriber identity) catchers, is a vulnerability due to the absence of mutual authentication on 2G technologies and functionality that can automatically configure 3G and 4G devices to use the 2G network. False base stations trick mobile devices that are within range to connect to them rather than the real network to which the false base station operator can then relay the call. Such a "man in the middle" attack creates a range of exposures to interception, location tracking, denial of service, and fraud. Lawmakers, such as the US Committee on Oversight and Government Reform, are developing recommendations to protect against the unauthorised use of these devices. Mobile network operators can deploy standard network and security measures to help mitigate against this risk and the GSMA has developed guidance to assist operators.

In addition to telecoms infrastructure, there are a range of corporate IT services that enable broader business operations as well as software for supporting customers, including billing systems and enterprise client dashboard and control systems. Internal corporate systems include intranet, email, instant messaging and staff systems such as accounting and sales systems. These systems are accessed by a range of employee devices and used by the full range of staff functions including the system administrators for the operational network.

The technology used within mobile networks is regularly upgraded with the latest enhancements rolled out on a planned basis. The high levels of investment in new infrastructure on a periodic basis have gone a long way to ensuring that the network infrastructure is as robust as reasonably possible. Maintaining confidence in this ability to invest as legislation and regulation changes in response to evolving threats will be increasingly important for success.

Some legacy 2G and 3G networks make use of unsecure signalling protocols, which were developed many years ago when security needs were lower, and as a result are subject to fraud and security threats on a regular basis. The GSMA's Fraud and Security Group has undertaken significant work to provide advice to network operators on how to mitigate signalling security risks. Several of the known attacks have been mitigated with security enhancements introduced in 4G and 5G. Exploitation of vulnerabilities on 4G networks can be minimised by ensuring the security capabilities that are inherent in the standards are properly deployed and configured. However, due to the backward compatibility of 4G with 3G/2G they will not disappear until the legacy technology or backward compatibility ceases to exist.

5G includes security controls to address many of the threats faced in legacy 4G/3G/2G networks. These controls include new mutual authentication capabilities, enhanced subscriber identity protection and additional security mechanisms. GSM Gateways (or "SIM Boxes") can also allow unauthorised third parties to interfere with the routing of calls to mobile networks and their customers, and this can raise safety and security concerns. Calling line identity (CLI) is generally not supported by GSM Gateways, and its absence has implications for services that rely on CLI (e.g. prepaid SIM account top up) as well as for network operators' lawful interception obligations to support law enforcement.

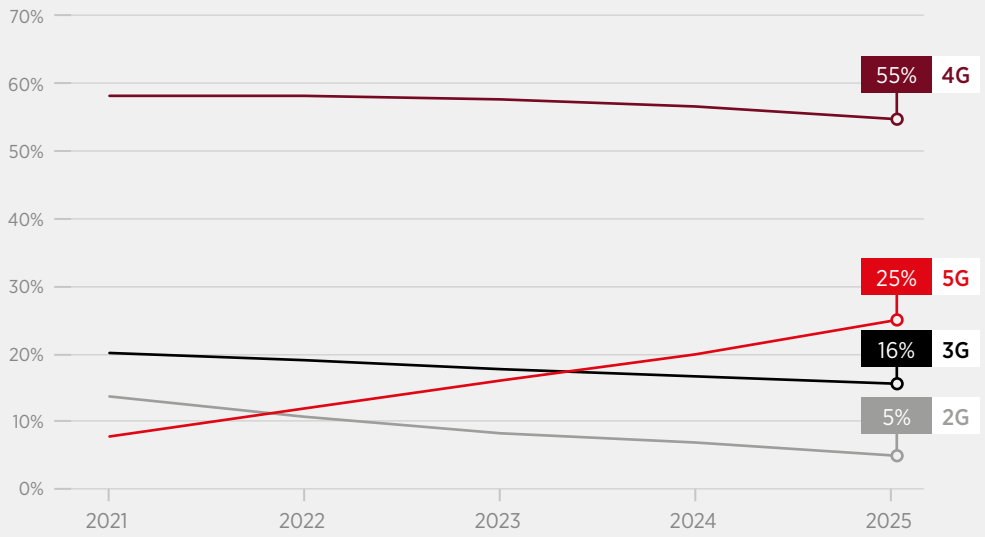
While mobile operators continue to mitigate the threats to their networks and their consumers, the same should be expected of operators of public wireless networks, such as public Wi-Fi Hotspots. The operators of these networks and customers should deploy appropriate safeguards, for example virtual private networks (VPNs) to help secure the wider communications ecosystem.

Figure 6

Percentage of Connections

5G will account for a quarter of total mobile connections by 2025, more than three times the figure for 2021

Percentage of connections (excluding licensed cellular IoT)



Source: GSMA Intelligence

Key implications for government, industry and other relevant stakeholders

While no security technology is guaranteed to be unbreakable, attacks on mobile networks and services are less common, as many would require considerable resources, including specialised equipment, computer processing power and technical expertise beyond the capability of most people or organisations. The barriers to compromising mobile security have been very high, and understanding of possible vulnerabilities has been greatly enhanced thereby enabling a prompt industry response to new security issues. However, the changing technology landscape and the emergence of new threats and sources of attack requires industry to take an even more proactive approach to protecting networks in future:

- It is important that the mobile industry ensures adequate mechanisms, tools and opportunities are in place to facilitate the sharing of threat and attack information and to ensure information is promptly disseminated in response to incidents. Such an initiative could include regulators or other government authorities such as national Computer Security Incident Response Teams (CSIRTs).
- Collective industry action is required to protect connected networks and consumers through consistency and consensus in the development of standards and the proportionate use of monitoring, detection and blocking capabilities.
- Securing mobile networks and services is complex, with multiple decisions to be taken by mobile network operators and their suppliers to implement the security standards properly and to deploy and configure a range of features. The GSMA offers advice and guidance to its members on how to achieve optimal security levels and continues to work on defining baseline security requirements to be committed to by all mobile network operators.
- The ongoing security challenge will expand with the evolution of 5G, but that also creates an opportunity to rethink security and how it can be provided.
- 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.

Mobile device security and integrity

By the end of 2021, 5.3 billion people subscribed to mobile services, representing 67% of the global population.[96] Over the period to 2025, there will be an additional 400 million new mobile subscribers, taking the total number of subscribers to 5.7 billion (70% of the global population).[97] It is expected that there will be 5.2 billion 5G connections by the end of 2030.[98]

A mobile phone call or data transmission will traverse several networks and, in the case of data, will often take multiple paths as part of a single communication. As a result, a range of potential vulnerabilities has emerged, requiring all network operators and the broader mobile industry ecosystem to be vigilant and to respond to them. Malware attacks can cover a range of targets including mobile devices, device applications and infrastructure. However, with increasing broadband access and a range of malware attacks on devices, protection must be also considered against device-based network attacks (e.g., signalling 'storms,' Denial of Service (DoS) attacks, IoT compromises back into the network).

Perhaps the most serious threat is a premeditated and systematic large-scale attack designed to render a whole network inoperable, affecting all users. There is a risk that breaches of mobile devices (e.g., by malware from phishing emails) could be used as an entry point to spread to other connected devices and then exploited to attack IP-based networks. For example, the 21 October 2016 attack on a major controller of domain name system infrastructure, Dyn[99] originated from malware on a computer, which spread to other devices, creating a botnet, which was then used to carry out a DDoS (distributed denial of service) attack. On an even larger scale, a similar approach could be used to inundate an IP-based mobile network with traffic that causes it to be overwhelmed and become unusable. Preventing such an attack requires close cooperation between mobile network operators and national law enforcement agencies as part of an overarching security plan, since attacking mobile networks is only one such possible route of attack by hostile parties.

The GSMA plays a central role in coordinating activity and leading on initiatives such as the Network Equipment Security Assurance Scheme (NESAS)[100] which is a global security assurance framework that facilitates improvements in security levels across the mobile industry for network equipment vendors. The scheme reflects the security needs of the entire ecosystem, including governments, mobile network operators and regulators, as it has been defined by industry experts through GSMA and 3GPP.

Security threats can come in many guises. Mobile devices require a SIM application to connect to a cellular network, either in a traditional UICC (SIM Card) or in an eUICC (eSIM). SIM swap is a normal business process to issue and provision new SIMs for customers that require replacements. The emergence of SIM swap fraud is an example where a legitimate service offered by mobile operators to allow customers to replace their existing SIM with a new one, has provided an opportunity for fraudsters to obtain and use the replacement SIM card to gain access to users' financial and wider service accounts. Mobile operators are implementing best practice to defend against such attacks. Phasing out legacy methods of authentication (such as usage of secret information and user-selected passwords that need to be spoken) is just part of the solution. Some mobile operators are now providing APIs for services such as banks to be able to connect to in order to establish whether a SIM swap has occurred recently.

96 https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf Mobile Economy Report 2022
97 ibid
98 5G in Context, Q1 2022 Data-driven insight into areas influential to the development of 5G (May 2022)
99 Dyn is a domain name system (DSN) provider for internet service providers, including Twitter, Amazon, AirBnB and Spotify. The organisation was able to restore their services after each attack while avoiding a system-wide outage, and mitigate against a third attack without consumer impact.
100 https://www.gsma.com/security/nesas-network-equipment-vendors/

Alongside the opportunities for consumers and businesses to use such services is the risk that mismanagement of these devices can create vulnerabilities that have the potential to breach networks and impact a wider set of users. Security attacks threaten all forms of technologies, including mobile. Mobile devices are targeted for a variety of reasons. For example, as an attractive item for thieves (due to their relatively high value and small size), organised criminals often seek to change the IMEI number of a stolen mobile device in order to re-activate it after it has been reported stolen. Other criminals use malware to perform functions that have the potential to cause harm to users, typically via identity theft and related fraud.

The GSMA has helped develop protection mechanisms such as those described in the GSMA IoT Connection Efficiency Guidelines[101] to protect mobile networks from the mass deployment of inefficient, insecure or defective IoT devices. Furthermore, the GSMA encourages its members to deliver security critical device patches to vulnerable devices as quickly as reasonably possible.

Key implications for government, industry and other relevant stakeholders

Good security practice and policy by industry suppliers is essential. Programmes such as the GSMA Security Accreditation Scheme, which certifies SIM suppliers, ensures that a commitment to security levels is encouraged and can be evidenced. Security assurance of suppliers and their products has been performed by the GSMA for some time with the Security Accreditation Scheme for SIM suppliers and the Network Equipment Security Assurance Scheme (NESAS) for network infrastructure product vendors.

The GSMA also seeks to support internet service providers and app developers which operate on the network and need to be accountable for preventing their exploitation as a channel to breach the integrity of a mobile network.

The GSMA supports global security standards for emerging services and acknowledges the role that SIM-based secure elements can play, as an alternative to embedding the security into the mobile device or an external digital card (microSD), because the SIM card has proven itself to be resilient to attack.

101 https://www.gsma.com/newsroom/wp-content/uploads//TS.34-v8.pdf

5G, IoT and future network developments

5G gives the mobile industry an unprecedented opportunity to uplift network and service security levels. The GSMA regularly explores a range of security considerations including secure by design, 5G deployment models and 5G security activities. This analysis is collated into a GSMA 5G Cybersecurity Knowledge Base[102] to provide useful guidance on a range of 5G security risks and mitigation measures. The GSMA's 5G Security Task Force (5GSTF) is responsible for monitoring work on 5G security, within the GSMA and across the wider industry and the standards development community, with a view to ensuring all necessary enablers are in place to deliver secure and resilient operational networks. In particular, the task force focuses on potential gaps between standards and operational implementations and the resolution of those.

With the implementation of 5G comes the migration to cloud computing, resulting in security considerations that were once the responsibility of the network equipment vendor becoming increasingly that of the operator. Virtualised networks bring a range of opportunities and benefits, including network slicing, network scalability and greater flexibility of vendor choice. But they also introduce a range of potential security threats. The transition of operator network environments to the cloud creates significant changes to the security operations and management of these networks, as well as to the type and capabilities of security controls. Assets are no longer placed at a fixed location (physical box) with planned capacity and long lifecycles. Instead, the solution stack relationship changes dynamically, and with it, the network traffic of the physical and virtual switches. This increases the complexity of monitoring the compute, storage and network properties of each component as they are no longer statically bound. Furthermore, the lifespan of such entities gets shorter to serve a workload for a few minutes after which it is decommissioned. In case of compromise there is a need to track not only the alignments of virtual/physical assets, but also the relationship between assets as well as the historic allocations of these assets as they moved within the platform.

5G is needed to capture the huge opportunity presented by IoT. As the ecosystem grows, the mobile industry will be expected to support bespoke services across industry verticals, where data is exchanged and insightful decisions using AI are made. According to the latest GSMA Intelligence IoT market update[103] the total number of IoT connections will more than double by 2030, reaching 37.4 billion.[104] Consumer IoT connections will almost double between 2020 and 2030 to 13.8 billion.

IoT services present security challenges, not only due to the scale and breadth of the services, but also due to the critical functionality that they provide and the private information they leverage. These factors make IoT services high-value targets for potential attackers who wish to exploit these services, for example, to launch DDoS attacks or extract sensitive data. Additionally, there exists a relatively large legacy estate of older IoT devices with limited in-built security protections. The GSMA has produced IoT security guidelines and an associated security self-assessment scheme for a range of ecosystem players. The GSMA's IoT security guidelines,[105] provide a comprehensive guide to IoT service providers.

As the industry moves from the traditional approach of dedicated hardware to a cloud-orientated approach, the number of options for infrastructure grows. Typically, modern infrastructure options can be classified into one of four groups: Software as a Service (SaaS); Infrastructure as a Service (IaaS); Platform as a Service (PaaS); and on-site infrastructure.

102 https://www.gsma.com/security/5g-cybersecurity-knowledge-base/
103 https://data.gsmaintelligence.com/research/research/research-2021/IoT-market-update-assessing-disruption-and-opportunities-forecasting-connections-to-2030
104 GSMA Intelligence report 'IoT market update: assessing disruption and opportunities, forecasting connections to 2030' (December 2021)
105 https://www.gsma.com/IoT/IoT-security/IoT-security-guidelines/

The move from the traditional approach of dedicated hardware to a cloud-orientated approach presents a range of opportunities and benefits such as network slicing, network scalability and greater flexibility of vendor choice. Cloud computing software can run on a range of non-proprietary platforms ranging from the entire product being hosted in the cloud, through to every element being owned and managed by the operator. The GSMA's Network Function Virtualisation Threats Analysis (FS.33)[106] provides a comprehensive overview of the threats related to network function virtualisation (NFV) and the underlying infrastructure and platforms hosting the NFV. It also includes extensive guidance on appropriate risk controls.

Virtualised infrastructure and more open interfaces deliver significant benefits but also make the 5G supply chain more complex and multi-party compared to 4G and earlier. This enables significant flexibility, scalability and potential cost savings but it is a more complicated supply chain. The need for increased resilience in network infrastructure has resulted in many regulators placing requirements on all operators to increase the levels of diversity, security and controls.

The GSMA encourages suppliers to participate in industry-recognised security assurance schemes, such as the GSMA Network Equipment Security Assurance Scheme (NESAS)[107] and encourages operators to source equipment from suppliers that participate in these schemes. The GSMA Supply Chain Toolbox outlines a number of services and guidelines to help operators and their suppliers to better understand security and to access best practice.

106 https://www.gsma.com/security/resources/fs-33-network-function-virtualisation-nfv-threats-analysis/
107 https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Key implications for government, industry and other relevant stakeholders

The GSMA aims to play a significant role in helping to shape the strategic, commercial and regulatory development of IoT and the 5G ecosystem.

— GSMA recognises that it has a key role to play in gathering and prioritising 5G security requirements for standardisation. The GSMA and its members invite other subject matter experts and law enforcement agencies to engage to ensure all needs are clearly understood.

— Government should support the global nature of future network markets and the wide variety of devices which will connect to the internet in future, and work across jurisdictions to ensure consistency and clarity on regulation and network security obligations for all players involved in this complex and rapidly evolving area.

— The mobile industry will continue to engage with the wider ecosystem and foster appropriate investment, directly or via vendors and ecosystem partners, in securing networks and devices as technology develops, especially in relation to the transition to network function virtualisation and 5G.

The GSMA has also conducted a comprehensive threat analysis involving industry experts from across the ecosystem, regulators as well as public sources such as 3GPP, the European Union Agency for Cybersecurity (ENISA) and the National Institute of Standards and Technology (NIST). These threats have been mapped to appropriate and effective security controls, and this analysis has been collated into a 5G Cybersecurity Knowledge Base providing useful guidance on a range of 5G security risks and mitigation measures.

The 5G Cybersecurity Knowledge Base makes available the combined knowledge of the 5G ecosystem to increase trust in 5G networks and make the interconnected world as secure as possible. The GSMA constantly monitors the activities of hacker groups, as well as researchers, innovators and a range of industry stakeholders, to improve the security of networks from one generation to the next.

GSMA security initiatives

The GSMA leads a range of industry initiatives (see Figure 7) to make operators aware of the risks and mitigation options available to protect their networks and customers and its work is acknowledged by regulators around the world as being sufficient to eliminate the need to formally regulate on a range of security matters.

Figure 7
GSMA Fraud and Security Services

GSMA Coordinated Vulnerability Disclosure (CVD)
A way for researchers to disclose vulnerabilities that could impact the mobile ecosystem

GSMA Device Check™
Protect against the risk of handling stolen or fraudulent devices, with this instant look-up service

GSMA Device Registry
Deter device crime, by exchanging device status information across the global ecosystem

GSMA eUICC Security Assurance (eSA)
Instil confidence that eUICC chipsets have reached rigorous industry security standards

GSMA Network Equipment Security Assurance Scheme (NESAS)
Security assessment of vendors' product development/lifecycle processes and infrastructure products

GSMA Security Accreditation Scheme (SAS)
Security audit and certification of SIM/eSIM production and subscription management sites

Services for GSMA Members only:

GSMA (FASG)
Share threat intelligence in a confidential forum and collaborate to maintain the security of operators' and their customers' assets

GSMA Telecommunications-Information Sharing and Analysis Center (T-ISAC)
Share timely and actionable information on cybersecurity threats in a trusted environment

Annex:
Mobile industry principles

As part of the GSMA's ongoing work on the safety, privacy and security topics identified in this report, the GSMA and its member operators recognise the need for a flexible and evolving approach to find a balance between the rights of the consumer/citizen, public safety needs and the role of mobile network operators in supporting both. The best responses will accommodate local market needs and variations rather than simply follow what may have been done elsewhere, but it is clear that there should be collaboration and shared learning between different stakeholder groups.

The GSMA and its member organisations have established the following principles, which guide how they continue to develop solutions to the issues raised within this report.

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 are 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 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