# Safety, privacy and security across the mobile ecosystem

## Key issues and policy implications

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**

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

For more information or questions on this report, please email **publicpolicy@gsma.com**

A.T. Kearney is a leading global management consulting firm with offices in more than 40 countries. Since 1926, we have been trusted advisors to the world's foremost organizations. A.T. Kearney is a partner-owned firm, committed to helping clients achieve immediate impact and growing advantage on their most mission-critical issues.

For more information, visit **www.atkearney.com**

# Contents

# 1 Executive summary

In the last three decades, the market for mobile telecoms services has grown to represent more than 7.6 billion mobile connections,[1] serving 4.7 billion unique mobile consumers globally.[2] This growth is set to continue, and it is anticipated that by 2020, almost three-quarters of the global population will benefit from a mobile subscription.[3]

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 ubiquity of mobile services and smartphones in many developed economies 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 $3.1 trillion in economic value added.[4]

With the growing economic and social importance of the internet in general and mobile internet usage in particular, there is a corresponding need to protect consumers using these services and to ensure that they can continue to use them safely and securely. Without such protection, there is a risk that the benefits of modern communications could be undermined. If consumers cannot trust the integrity of an e-commerce service, or worry that sensitive private information may be intercepted when using communication services, then they are much less likely to use them and would have to resort to costlier and less efficient communication channels. In the most extreme cases, a service that was promoted in the 1990s as offering security (to car drivers, or vulnerable people travelling alone) and privacy (calls from a personal device instead of a fixed phone in the family living area), could be abused to damage those fundamental needs.

The mobile industry has worked to educate consumers and developed new features that have built trust in its services. Each new iteration of technology has introduced new features, such as encryption and user identification validation, which have made mobile services increasingly secure and minimised the potential for fraud, identity theft and many other possible threats.

The trust that underpins these services and allows people across the world to communicate, trade, share ideas and interact cannot be taken for granted. As more advanced and complex services are developed, so too 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. 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, it is important that any intervention is 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, 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.

1. Including machine-to-machine (M2M) connections
2. GSMA, 2016. "The Mobile Economy: 2016"
3. Ibid.
4. Ibid.

1

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. The GSMA plays a central role in coordinating activity and leading on initiatives such as IMEI (identifier codes to tackle mobile device theft) or Security Accreditation schemes for critical infrastructure components, and 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 faces a different challenge: with eight out of ten consumers reportedly uneasy with the degree of personal data being shared, there is a natural tendency 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, so that a mobile network operator can only commit to protect the user data it holds directly and to raise awareness that end users may be sharing far more data with organisations beyond its 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.

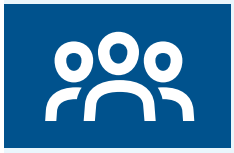
Some challenges to the provision of private and secure mobile services originate with governments and law enforcement agencies. Their legitimate and increasingly sensitive mandate to protect citizens has led them to sometimes seek wide-ranging powers to access and use personal data as well as intervene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

# 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 and 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 that 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 also needed from governments, law enforcement agencies, multilateral and nongovernmental organisations, and companies across the digital ecosystem, as well as individual efforts by consumers themselves. 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.

1



## 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 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**

# 2 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. At the individual level there are instances of fraud, identity theft, cyber bullying 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.

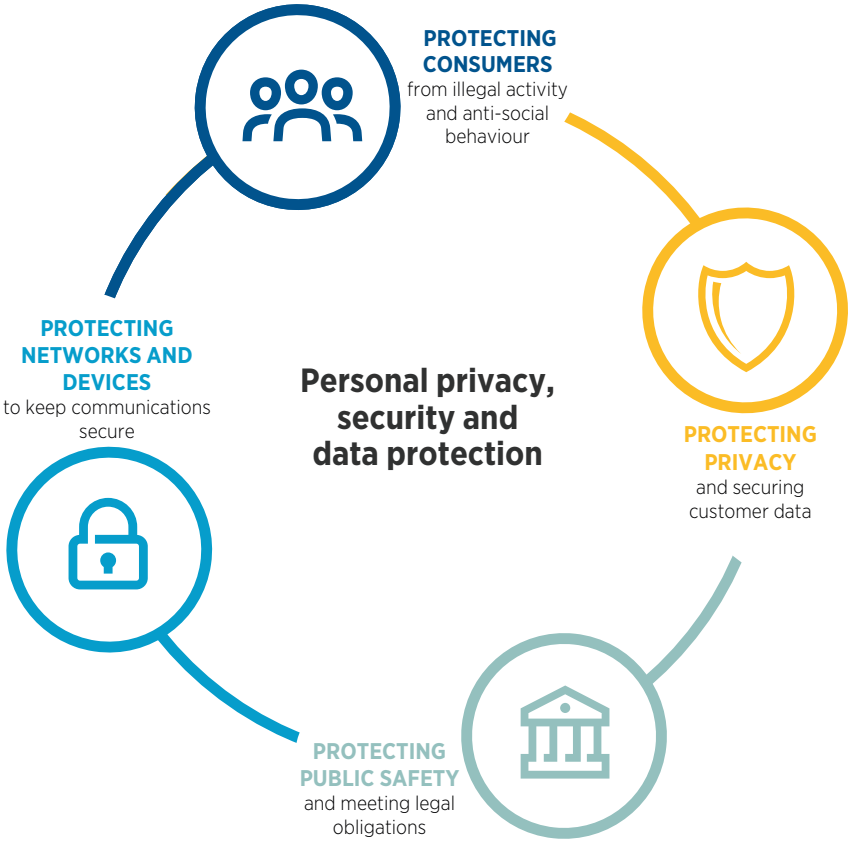
This report seeks to explain the major issues and challenges around safety, privacy and security in the mobile world, highlighting the complexities and trade-offs and demonstrating the industry initiatives and actions which are already taking place. Where there are opportunities to do more, the report 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, IETF and oneM2M, 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.

# 3 Protecting Consumers

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. Perhaps inevitably with something so widespread, there are people who seek to use mobile technology to harm others.

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. 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 antisocial 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.



## 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**

# Children and Vulnerable Individuals

For potentially vulnerable user groups, including but not limited to children and some women, mobile services offer many benefits helping them to be more connected, independent and safe. However, children and vulnerable individuals are also at risk of certain negative behaviours. For example, a GSMA study examining the gender gap in terms of mobile device ownership and usage found that 68% of women tend to perceive security concerns related to owning and using mobile devices, and harassment from strangers as a barrier.[5] 'Security and harassment' emerged as one of the top five barriers to mobile phone ownership and usage by women.[6] While it is important to note that only a subsection of women, like men, may be considered as 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 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.

### Supporting the inclusion and safety of women

On average, women are 14% less likely to own a mobile device then men, with this gender gap reaching 38% in some regions.[7] This translates to 200 million fewer women than men owning a mobile device.[8] In total, over 1.7 billion females in low- and middle-income countries do not own mobile devices.[9] 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 by some women, particularly in lower income countries.[10] The GSMA and its member organisations are currently launching an initiative that further builds on the Connected Women work, with a specific focus on security and harassment issues.

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,[11] thus improving their level of safety.

5. GSMA, 2015. "Connected Women - Bridging the Gender Gap: Mobile Access and Usage in low- and middle- income countries"
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. Banglalink Emergency: http://www.banglalink.com.bd/en/services/services/information-based-services/banglalink-emergency/

### Safeguarding young users and child online protection

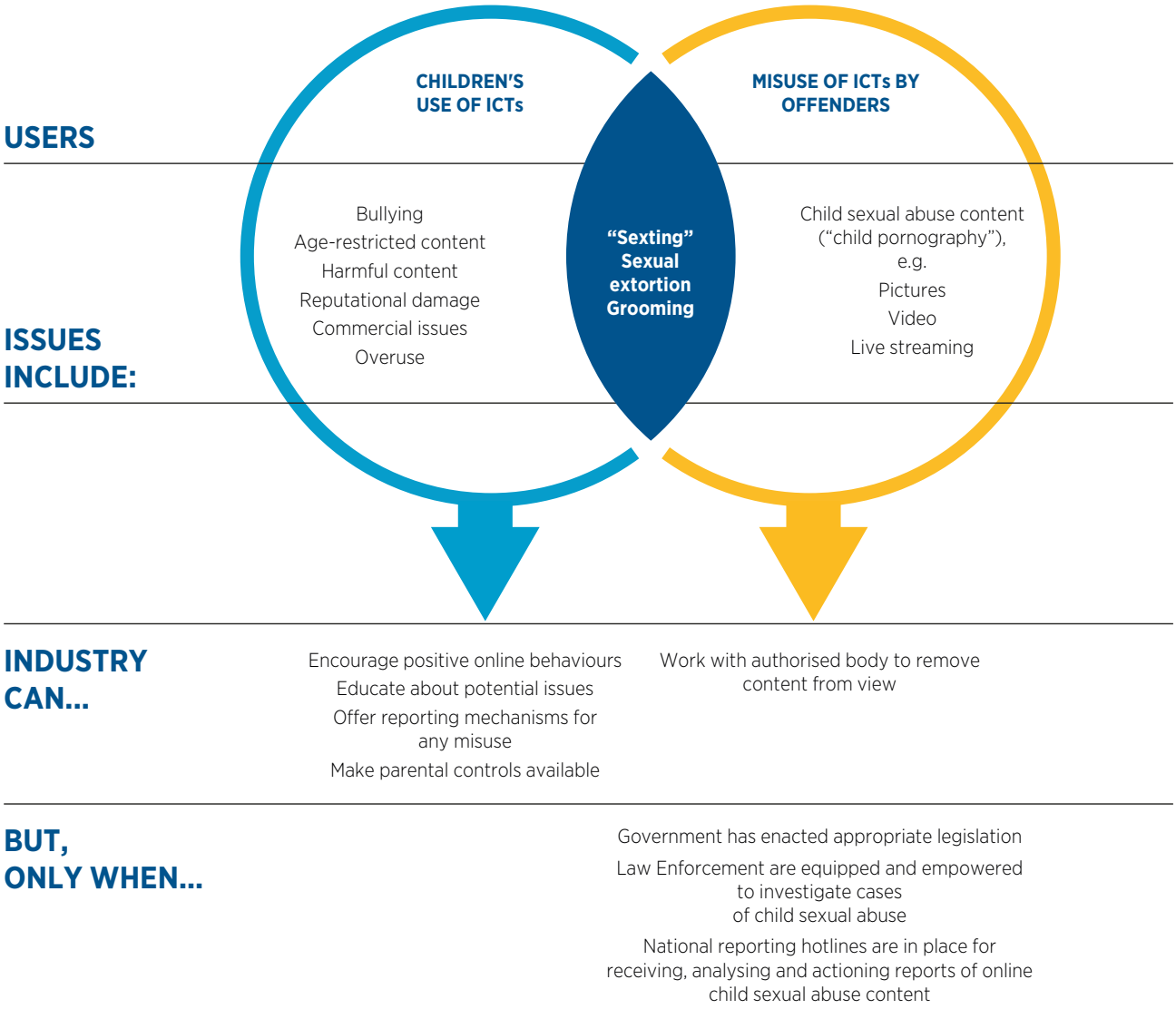
A second group of potentially vulnerable users of mobile services is children. In understanding the topic of child online protection, it is important to distinguish between two distinct issues:

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.

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.

### Encouraging children's safe and responsible use of mobile technology and services

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

By collaborating with stakeholders from across the mobile ecosystem, as well as NGOs and government organisations, the GSMA mYouth[12] programme is dedicated to helping young people make the most of their mobile experience. Along with other initiatives, the mYouth 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. The GSMA, through its partnership with Child Helpline International, 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]

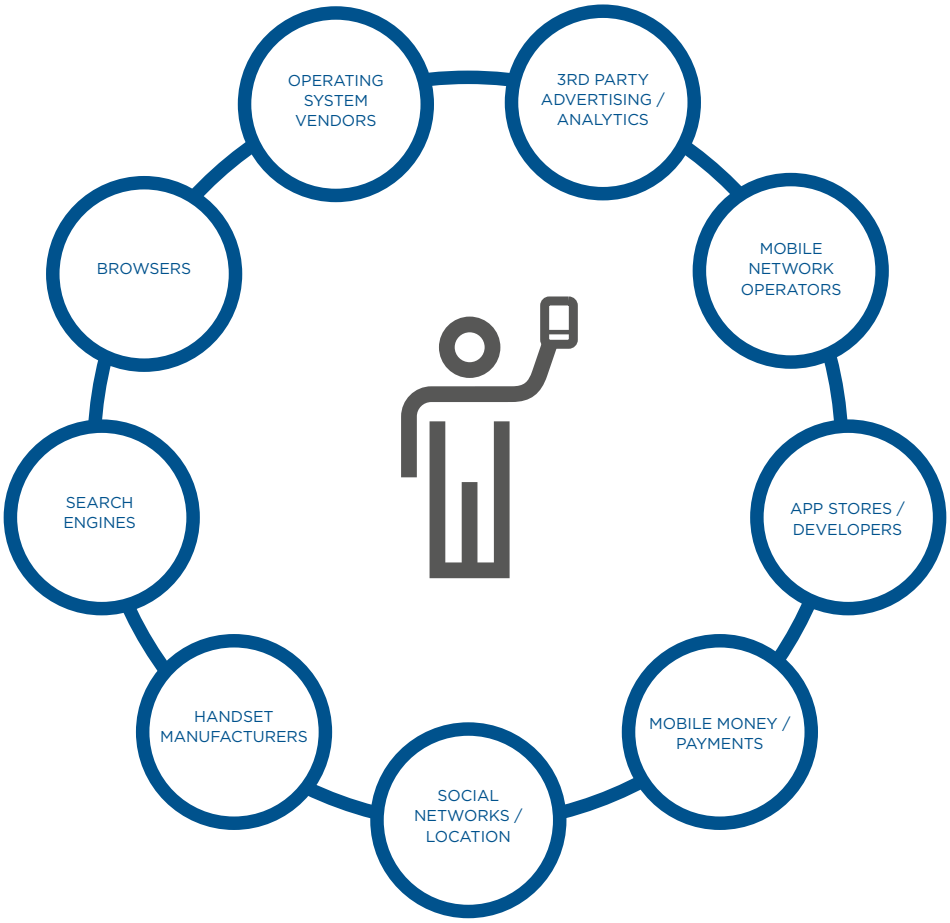
When it comes to protecting children's rights online, companies and other stakeholders have to strike a careful balance between children's right to protection and their right of access to information and freedom of expression. Therefore, companies must ensure that measures to protect children online 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 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.

12. The mission of the GSMA mYouth program is to promote the positive, safe and responsible use of mobile services by young people. This multi-stakeholder initiative includes partnerships with Child Helpline International and with UNICEF. For further detail, see: http://www.gsma.com/publicpolicy/customer-affairs/children-mobile-technology/myouth
13. For the guidelines, see: http://www.childhelplineinternational.org/resources/manuals-toolkits/internet-safety-guides/
14. ITU & UNICEF, 2014. "Guidelines for Industry on Child Online Protection"

Figure 3

## The mobile ecosystem






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.[15] 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 and UNICEF Guidelines for Industry on Child Online Protection. 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.

15. ITU & UNICEF, 2014. "Guidelines for Industry on Child Online Protection"

Deeper Dive

# ITU & UNICEF 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**
3. **Creating a safer and age-appropriate online environment**
4. **Educating children, parents and teachers about children's safety and their responsible use of information and communication technology (ICT)**
5. **Promoting digital technology as a mode for increasing civic engagement**



## Combatting online Child Sexual Abuse Content

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

As discussed above, tackling the misuse of technology with respect to child sexual abuse content (CSAC) 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 child sexual abuse content. 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 child sexual abuse content. 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 CSAC. 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. For example, the GSMA Mobile Alliance has already begun working with its external partners to understand, monitor and – if this becomes appropriate – address potential impacts of encryption on restricting access to known CSAC.

16. For further information on the Mobile Alliance, see: http://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance

Deeper Dive

# GSMA Mobile Alliance Against Child Sexual Abuse Content

The Mobile Alliance Against Child Sexual Abuse Content (Mobile Alliance) was founded by an international group of mobile 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 child sexual abuse content.

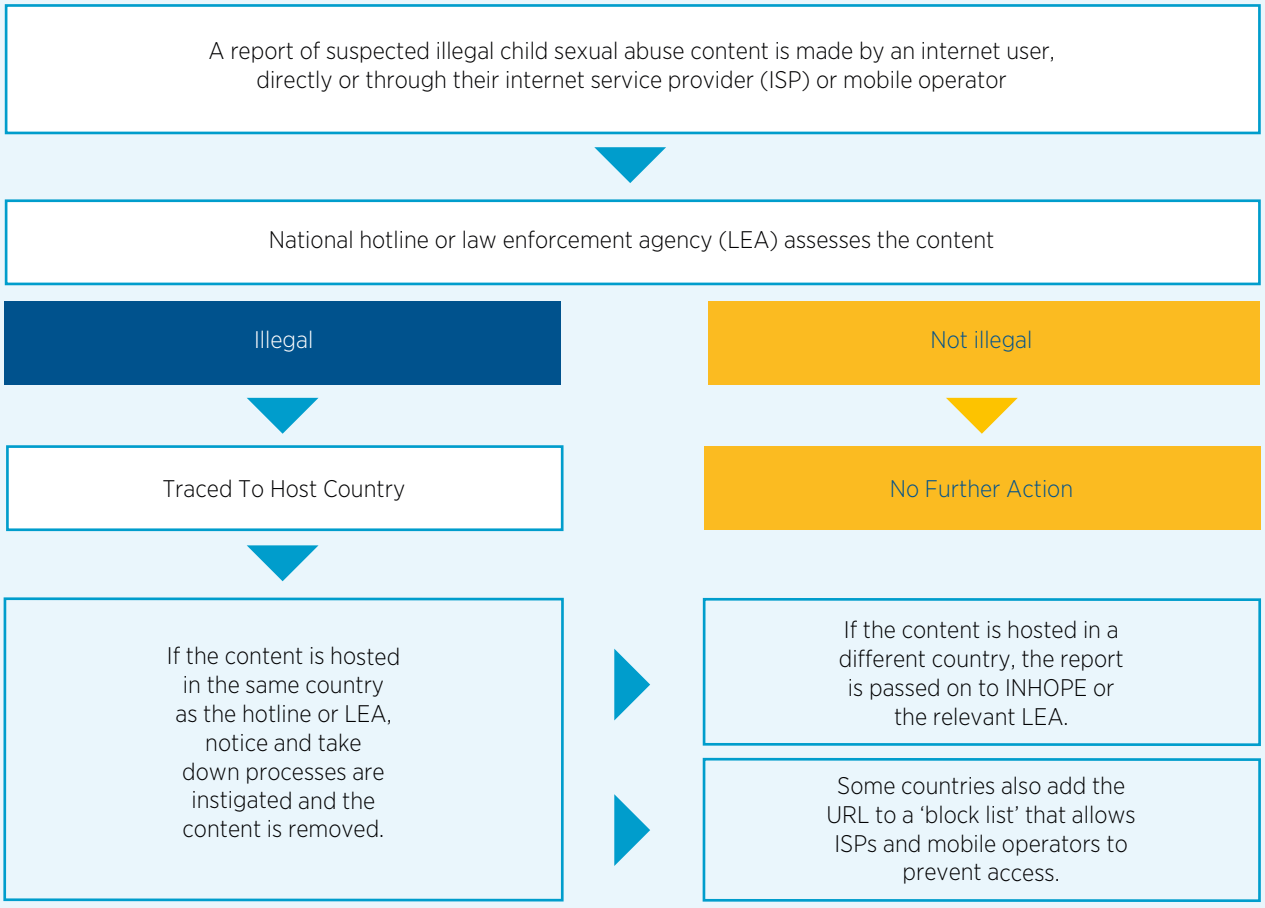
Alliance members have made the commitment to:

- **Implement technical mechanisms to restrict access to URLs or websites identified by an appropriate, internationally recognised agency as hosting child sexual abuse content**
- **Implement 'notice and take down' processes to enable the removal of any child sexual abuse content posted on their own services**
- **Support and promote hotlines or other mechanisms for consumers to report child sexual abuse content discovered on the internet or on mobile content services**

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

The Mobile Alliance also contributes to wider efforts to eradicate online child sexual abuse content by publishing guidance and toolkits for the benefit of the 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. It also collaborates with the European Financial Coalition and the Financial Coalition Against Child Pornography.

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



3

## Key implications for government, industry and other relevant stakeholders

Mobile devices and services enhance the lives of young people. This perspective needs to be embraced, encouraged and better understood by all stakeholders to ensure young people get the maximum benefits from mobile technology. 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.[17]

Furthermore, the full suite of responses to addressing and combating child sexual abuse content 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 child sexual abuse content.

- 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 child sexual abuse content[18]
- Mobile network operators use terms and conditions, notice and take down processes and reporting mechanisms to keep their services free of this content[19]
- 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,[20] including child sexual abuse content

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.[21] 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 as a useful tool to guide their response to online child sexual abuse content.[22]

17. GSMA, 2016. "Mobile Policy Handbook: Children and Mobile Technology"
18. GSMA, 2016. "Mobile Policy Handbook: Illegal Content"
19. Ibid.
20. Ibid.
21. Ibid.
22. For more information, see: http://www.weprotect.org/the-model-national-response/

# Stolen and Counterfeit Devices

## Mobile device theft and trade

The small, portable and high value nature of mobile devices, as well as the information stored on the device, unfortunately make them attractive to criminals. This has created an international black market for mobile devices obtained through theft. Policymakers in many countries are increasingly concerned about the incidence of mobile device theft, and also the involvement of organised crime in the bulk export and trade of stolen mobile devices.

## Creating barriers to mobile device theft and trade

The GSMA allocates unique identifiers, known as International Mobile Equipment Identifiers (IMEIs) to manufacturers of 3rd Generation Partnership Project (3GPP)[23] compliant devices. It records the ranges allocated, and information pertaining to the device models for which they have allocated, in its IMEI Database. The information recorded includes the manufacturer and model name of the device and its main network capabilities (e.g., frequency bands, radio interfaces and device types).

In 1996, the GSMA launched an initiative to block stolen mobile devices, based on a shared database of the unique identifiers of mobile devices reported as lost or stolen by consumers of GSMA member network operators. That central list — commonly known as the blacklist — is accessible by all GSMA members that have a connection to the IMEI Database for the purposes of sharing stolen device data. When mobile network operators detect a device connecting to their network that is registered on the blacklist, they are able to block its use. Once thieves learn that consumers are unlikely to buy stolen devices that are likely to be disabled soon after they have been stolen, it makes device theft much less attractive. To support this, the GSMA encourages its members to deploy a standards-based Equipment Identity Register (EIR) on their networks to block the connection of stolen devices, based on their IMEI identifier. IMEI blocking, based on the blacklist, has had a positive impact in many countries, but for an anti-theft campaign to be fully effective, additional measures must be put in place. The theft and sale of devices is an international problem. Even if an IMEI is blocked by all mobile network operators within one region, the mobile device could still be used in another region where mobile network operators have not connected to the GSMA IMEI Database.

The GSMA is working to connect as many mobile network operators as possible to the IMEI Database. The GSMA Database blacklist is currently (as at end 2016) used by over 140 mobile network operators across more than 40 countries worldwide to share information on stolen devices on a daily basis. Within the Latin American region where the issue of handset theft is highly prevalent, 18 countries have now connected to the IMEI Database to share stolen data and most mobile network operators in the region are now doing so. To further empower and help consumers and retailers, a Public IMEI Device Check service is available in some markets to check the status of devices that are offered for sale. This has been rolled out as part of the GSMA-led "We Care"[24] campaign, with more than 1.5 million searches having been conducted by the end of 2016.



23. 3GPP unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). 3GPP specifications are published - free of charge - up to four times a year. The term "3GPP specification" covers all GSM (including GPRS and EDGE), W-CDMA (including HSPA) and LTE (including LTE-Advanced and LTE-Advanced Pro) specifications. For more information, see: www.3gpp.org
24. For more information on the "We Care" campaign, see: http://www.gsma.com/latinamerica/wecare

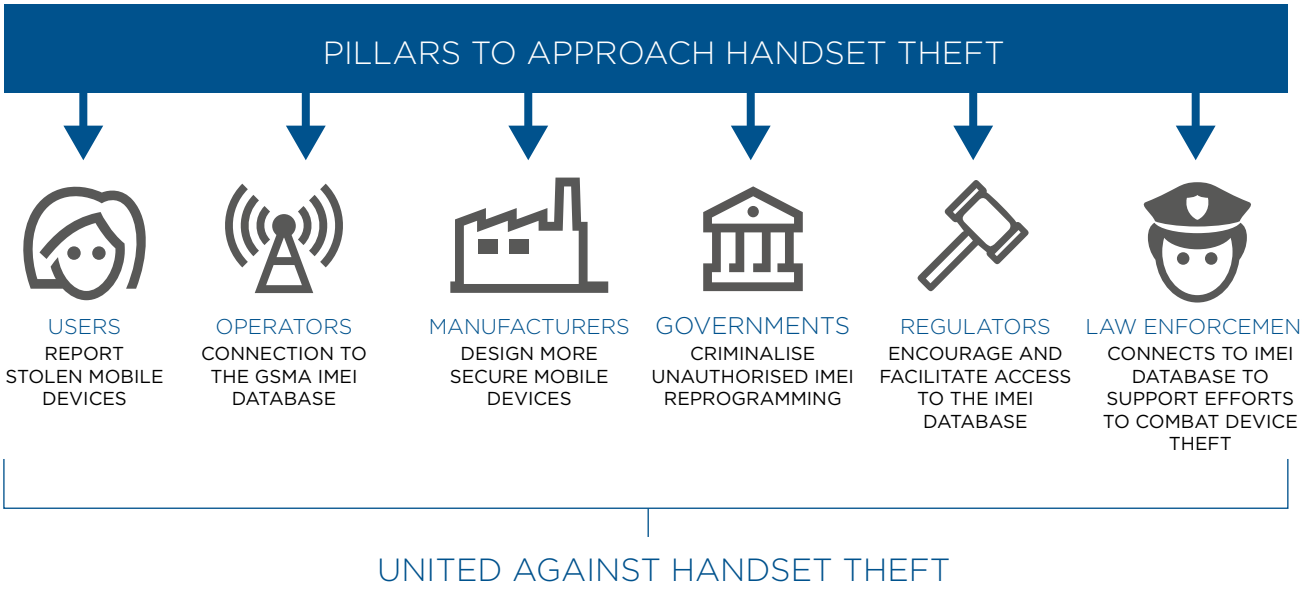
The success of the IMEI blocking approach depends on the secure implementation by manufacturers of IMEIs in all mobile devices. The world's leading device manufacturers agreed to support two key GSMA initiatives to strengthen IMEI security, including the definition of technical design principles for IMEI security implementations as well as participation in the GSMA's IMEI Security Weakness Reporting and Correction Process.[25] More could be done by some device manufacturers to enhance security levels relating to IMEI integrity, which is essential to effective device blocking. Mobile network operators and other large suppliers and retailers of mobile devices can make informed purchasing decisions when choosing which devices to sell on to their consumers, with the security of IMEI implementations in those devices and compliance with the technical design principles potentially becoming key considerations. It is important that all stakeholders – manufacturers, mobile network operators, governments and consumers – work together to ensure full IMEI integrity and the prompt remediation of problems that may arise. Additionally, governments need to recognise the central role IMEI integrity has to play in allowing stolen devices to be blocked, by criminalising the unauthorised changing of IMEIs in mobile devices (this is also referred to as IMEI reprogramming or adulteration). A number of countries have made it a criminal offence to change the IMEI of a mobile device following its manufacture and others are encouraged to follow suit and to actively identify and prosecute offenders to discourage the bypassing of security controls.

Another form of deterrence for mobile device theft is a "Kill Switch". A Kill Switch is a way to disable crucial functions of a mobile device. It is essentially a function within the mobile device operating system, so that when triggered the device will cease to operate as intended. It can only be reactivated or reused if the legitimate device owner authorises the reactivation of the device. The GSMA developed the Anti-Theft Device Feature Requirements document for device manufacturers, mobile network operators and governments defining a set of features that can be invoked by a device owner to locate, disable, and re-enable their device if it is misplaced, lost or stolen.[26]



**Figure 4**

## Pillars to approach handset theft




25. For the Security Weakness Reporting and Correction Process, see: http://www.gsma.com/publicpolicy/wp-content/uploads/2007/07/IMEI-Weakness-Reporting-and-Correction-Process-3.2.0.pdf
26. GSMA, 2016. "Anti-Theft Device Feature Requirements, Version 3.0"

## Key implications for government, industry and other relevant stakeholders

The GSMA seeks to assist external stakeholders to restrict the sale and use of stolen or lost devices. The GSMA and its members are able to offer expertise and resources to government and other stakeholders looking to develop local solutions in a collaborative way that are relevant and consumer focussed. For example, the GSMA suggests that:

- A collaborative approach among the main stakeholders is essential:[27]
  - Users can report stolen devices to their network operators, enable anti-theft features on their devices and, in countries where operators are connected to the IMEI Database, use the IMEI to check the status of devices they plan to buy
  - Mobile network operators can block stolen devices from their networks, connect to GSMA's IMEI Database to share blacklist 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 operators can obtain the IMEIs of stolen devices from 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 IMEI Database to share stolen device data, provide and/or facilitate the provision of IMEI checking services to allow users to check the status of devices before they buy and generally provide a regulatory environment that is supportive of consumer-friendly and effective solutions to combat device theft
  - Law enforcement agencies can ensure they have the ability to check the status of devices by obtaining free access to GSMA's stolen device data and increase their focus and resources on device theft ensuring offenders are identified and prosecuted
- It is important to avoid solutions which may be less effective and/or even have unintended negative consequences:
  - The optimal solution to prevent the use of lost or stolen devices at a network level is the use of blacklists. The use of whitelists for such purposes should be avoided. Whitelists were designed for other purposes, including to assist with combating counterfeit devices although the effectiveness of this approach has not been proven
  - Enforcing the use of non-standards based solutions to combat mobile device theft, as these are proprietary in nature and tend to be technically difficult and expensive to implement.

    Approaches that are contrary to the global mobile standards, such as tying specific devices to individual mobile users, as these tend to be difficult and onerous, or even disproportionate, for users and their service providers to comply with and they have the potential to raise a number of complex legal and competition-limiting issues
  - Building national device identifier databases represents an unnecessary expenditure and effort. The existing GSMA IMEI Database is 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



27. GSMA, 2016. "The Mobile Economy: Latin America and the Caribbean 2016"

Case Example

# Industry's contribution to combat handset theft in Latin America

In recent years, handset theft has grown strongly due to the expansion in the adoption of mobile phones, especially smartphones. Handset theft related offences are growing at a very fast pace in Latin America. For example, 1.2 million mobile phones were reported to be stolen in Peru within the first three months of 2014. This was a 34% increase from the same period in 2013. While occurrences are underreported, there were 14 million mobile phones listed as stolen in 2014 on the IMEI Database within the Andean countries of Ecuador, Colombia, Peru and Bolivia alone.

Stolen mobile phones are often transported across borders in order to exploit price arbitrage opportunities and/or to work-around country-specific initiatives to block devices using the IMEI. Therefore, to actually combat this issue, it is essential to share the information among operators within the same country as well as enabling the possibility to do so regionally and globally.

In 2011, the Inter-American Telecommunication Commission (CITEL) approved a resolution which, among other proposals, recommended: 'Regulating at the regional level the exchange of black-listing databases and blocking their unique identification codes (IMEI) to prevent the activation and use of cell phones stolen in other markets and helping to control illegal trafficking of devices among the region's countries'. In 2012, thirteen Latin American, GSMA member, mobile network operators pledged to work together, and to collaborate with regional governments across the region to block the use of stolen devices. This voluntary initiative allows the sharing of stolen mobile device information in order to block stolen devices and make their trafficking and reuse across the region more difficult.

The GSMA continues to work and to promote the adoption of these guidelines to all GSMA member companies in Latin America through the signing of memoranda of understanding among operators on a country-by-country basis but with the objective to ensure full data sharing across the entire region.

**1**

**HANDSET THEFT FROM USER**

**Samsung Galaxy**

24% 47%

**iPhone**

are the models which IMEIs are most uploaded to the database

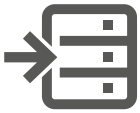
**2**

**USER REPORTS TERMINAL THEFT TO OPERATOR**

Units reported daily/per day

| | |
|---|---|
| **Argentina** | **5000** |
| **Columbia** | **4400** |
| **Brazil** | **8200** |
| **Peru** | **2800** |

**3**



**OPERATOR UPLOADS THE STOLEN HANDSET IMEI TO THE GSMA DATABASE**

**18 LatAm countries** connected to the GSMA database

**54 operators** in the region (106 worldwide)

**+38M** uploaded since the commitment signature in July 2012

**4**

**THE REST OF THE OPERATORS IN THE REGION DOWNLOAD THE BLOCKED IMEIS**

On average, Latin America operators download data from at least **34 operators of the GSMA database**

**5**

**THE HANDSET STOLEN FROM USER 1 CANNOT BE USED IN OTHER COUNTRIES**

Brazil (**6M**) Argentina (**4.1M**) Colombia (**3.2M**) Peru (**2M**)

represents

**76%**

of all IMEIs from the region uploaded to the GSMA database



## 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 on black markets globally, by organised criminal networks. As a result, there is limited awareness among consumers and governments about the true scale and impact of counterfeit mobile device trade. It is estimated that 143 million illicit mobile devices were sold in 2013 globally.[28]

While the production and distribution of counterfeit goods is a serious issue that breaches intellectual property and legitimate trading rules, with the subsequent loss of sales revenues for manufacturers and tax income for governments, counterfeit devices also have an impact on consumers. In many markets, the prevalence of counterfeit devices may be so high that consumers are unaware that the devices are even counterfeit and so are buying them unwittingly.

Quite aside from the poor service experience often associated with the performance and use of counterfeit devices, many have been reported to contain hazardous materials that pose a threat to the environment. A number of studies have demonstrated the presence of hazardous materials, such as lead in solder joints, within some counterfeit mobile devices at levels that are higher than globally acceptable limits.[29] These limits are defined within the regulations that legitimately manufactured mobile devices must adhere to. Counterfeit mobile devices with hazardous materials present 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 legitimate. It is now commonplace for counterfeiters to hijack IMEI number ranges allocated to legitimate device manufacturers for use in their products and this makes it more difficult to differentiate between legitimate and counterfeit products.

28. The Mobile Manufacturers Forum (MMF), 2014. "Counterfeit/Substandard Mobile Phones: A Resource Guide for Governments"
29. Ibid.

### Restricting the sale and use of counterfeit devices

To help address this issue, whitelist data (record of identification number ranges allocated to all legitimate device manufacturers) from the GSMA-managed IMEI Database can be used to detect, and if required deny network access to, devices with invalid or non-existent IMEIs. 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 and the World Customs Organisation (WCO) entered into a partnership in September 2016 to collaborate in the fight against counterfeiting and fraudulent trading of mobile devices. Integration with the IMEI Database will allow for cross-checking and the filtering out of identified counterfeit devices, based on the IMEI, at the point of import. However, this solution cannot be applied to mobile devices that are trafficked and imported outside of the customs process as contraband: here 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 limited effect as the counterfeit device distribution is typically international, with clampdown efforts in individual countries easily circumvented. Furthermore, creating national device whitelists is an unproven approach for which no evidence exists as to their effectiveness 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, networks, 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 local network operators to understand the extent to which counterfeit devices are in use in the local market and should work in consultation with those stakeholders to develop and agree measures to be taken that do not penalise legitimate device manufacturers or innocent users exploited by counterfeiters
  - Governments can help disrupt the device black market by reducing tariffs and duties on legitimate imported devices which will reduce the cost of ownership of legitimate devices and can support consumer awareness and education programmes to highlight the risks of buying counterfeit devices
  - Customs agencies can ensure they have the ability to verify if devices contain legitimate identifiers at the point of import by obtaining free access to GSMA's IMEI data and can increase 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 network operators can connect to GSMA's IMEI 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 which may be less effective and/or even have unintended negative consequences:
  - Enforcing the use of non-standards based solutions to combat counterfeit mobile devices should be avoided as these are proprietary in nature and tend to be technically difficult and expensive to implement.

    Approaches that are contrary to the global mobile standards such as tying specific devices to individual mobile users, should not be pursued as these tend to be difficult and onerous, or even disproportionate, for users and their service providers to comply with and they have the potential to 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[30] and, increasingly, "social engineering" fraud (e.g., Phishing, SMiShing or Vishing),[31] which tricks victims into revealing sensitive information about themselves and the services they consume, without realising they have compromised their own security.

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.

Social engineering 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, reported figures from the National Fraud Intelligence Bureau show reported incidents rose by 21% in the 12 months between October 2014 and October 2015.



### Addressing and minimising fraud

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 network operators have adopted GSMA recommended techniques for detecting and dealing with the international transmission of fraudulent mobile spam.

Although not very common, voicemail systems have been targeted in the past 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 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. 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 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 network operators in this, GSMA recommends three guiding principles[32] 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

30. '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)
31. See sidebar on Social Engineering
32. L. Gilman, 2012. "Mitigating the risk of fraud through consumer communication", GSMA

## 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



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. To reach M-PESA consumers, Safaricom uses a multi-pronged approach. SMS blasts, radio announcements in local dialects and newspaper ads are all part of their consumer awareness campaigns. Increasing consumer awareness through clear communication has been vital to Safaricom's success in managing fraud against M-PESA consumers.

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.

# 4 Protecting Consumer Privacy

This last decade has witnessed a huge increase in the richness of communication services. The very nature of these services means that the internet companies providing them gain access to considerable information about users, starting with their identity, who they communicate with, their location, through to an insight into their personal interests via the sites and services they access. Providers can analyse communications such as words typed into search engines or locations typed into map applications and combine these datasets to derive interests and intent.

Mobile network operators use 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.[33]

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, with acknowledgement of the need to consider national security concerns

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.

## 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**

33. For a more detailed discussion of such services, please refer to the GSMA document, produced in 2016 by A.T.Kearney, "The Internet Value Chain: A study on the economics of the internet", pg. 11

# Data Collection and Usage

The GSMA forecasts that the number of smartphones will grow from 2.6bn from the end of 2015 to 5.8bn by 2020. In parallel data traffic is expected to grow by a CAGR of 49% over the same period.[34] This proliferation of devices and data is allowing individuals, companies and governments to innovate in new and unexpected ways.[35]

However, research shows that while consumers are using these services ever more, they are also concerned about their privacy and seek reassurance that they can trust companies with their data. A GSMA study found that eight out of ten mobile users have concerns over sharing their personal information while using the mobile internet or apps, and further suggested that almost half of the mobile users with privacy concerns would limit their use of apps unless they felt sure their personal information was better safeguarded.[36]

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; there is no globally interoperable framework. Often, the organisations governed by these laws have an international footprint. This creates uncertainty around the appropriate legal baseline and raises the question of which country's laws on data usage should apply — that of the user or that of the service provider. This can be further complicated if the service provider stores and processes the data in a third country
- A second distinction is between the mobile network operator and the third party online services and apps that users can access over the network. Most mobile network operators are subject to laws and licence obligations relating to the protection of privacy that do not apply to other online services in the internet ecosystem.



Terminology

## Personal Data

**Personal data** – 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 the 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.

34. GSMA, 2016. "The Mobile Economy: 2016"
35. Ibid.
36. GSMA, 2014. "Mobile Privacy: Consumer research insights and considerations for policymakers"

The current misalignment between national and/or market-sector privacy laws, combined with global data flows, makes it virtually impossible for consumers' privacy expectations to be met in a consistent way by all parties. This inconsistent applicability of rules is likely to be exacerbated as more devices and sensors are interconnected through the 'Internet of Things' (IoT)[37] given that IoT services are often global and include multiple types of service providers across different sectors.

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. The GSMA's commissioned research shows that 82% of users agree to privacy notices without reading them because they tend to be too long or legalistic.[38] Because of the often misunderstood distinction between the mobile network 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

Increases in computing power, falling costs, and advances in analytics, 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 are often referred to as big data analytics techniques. This represents 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 network operators will increasingly be 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.

For example, to help fight the Ebola epidemic, Orange Telecom (West Africa) worked with the Harvard School of Public Health (HSPH) and Flowminder to predict the spread of the disease using mobile phone data. The data gleaned from cell phones in Ivory Coast (in 2011) and Senegal (in 2013) was anonymised and aggregated by Orange Telecom, who then authorised it for release to Flowminder. This was used to develop a model that provided a window into regional population movements, which then informed recommendations of where to focus health-care efforts (MIT Review, 2014. "Cell-Phone Data Might Help Predict Ebola's Spread").

Additionally, Telenor Group, Telenor Pakistan and HSPH have carried out the first-ever country-wide effort in Pakistan to understand and model the spread of dengue fever using anonymised mobility data. This project was not only the largest of its kind ever conducted, in terms of the number of subscribers analysed, but also represents the first attempt to conduct an analysis of dengue outbreaks using CDR analytics. The goal was to design prevention strategies rooted in data-driven methods, where Telenor leverages core internal competence on analytics and exclusive data sets to create shared value – for Telenor and society. The study demonstrated a privacy-conscientious way of utilising consumer data collected by mobile operators in solving and supporting societal problems. The approach operationalises dengue risk-maps that can serve as useful tools for health practitioners and government in Pakistan, and provided insight for designing better prevention strategies. (Telenor, 2017).

The mobile industry is determined to help realise the economic and societal benefits of big data analytics through good digital responsibility practices so that society can unlock the huge potential of big data analytics in a way that respects well-established privacy principles and fosters an environment of trust.

In collaboration with representatives from the mobile ecosystem, the GSMA is also working on privacy aspects of big data analytics, which are underpinned by the GSMA Mobile Privacy Principles.

37. Internet of Things is discussed in further detail within the chapter, "Protecting Network Security and Device Integrity".
38. GSMA, 2014. "Mobile Privacy: Consumer research insights and considerations for policymakers"

### Addressing consumer privacy when collecting and using data

The GSMA has developed a set of Mobile Privacy Principles, which describe the way in which 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.[39] 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

Figure 5

## GSMA Mobile Privacy Principles[40]

### 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.

### SECURITY

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

### ACCOUNTABILITY AND ENFORCEMENT

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

### 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.

### 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.

### 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.

### 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.

### USER CHOICE AND CONTROL

OPT IN OPT OUT

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

### EDUCATION

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

39. GSMA Mobile Privacy Principles (2016), see: http://www.gsma.com/publicpolicy/mobile-privacy-principles
40. http://www.gsma.com/publicpolicy/mobile-privacy-principles

## 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 and promote trust in mobile services. For services that they provide themselves to their consumers, mobile network 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[41] shows that mobile users want simple and clear choices to control the use of their information. The study found that over 80% of mobile internet users worldwide 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.

4

41. The GSMA has been working 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 all countries share similar attitudes and concerns about their privacy. 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 see, 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[42]
- 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

Guided by these principles, the GSMA also developed a set of Privacy Design Guidelines for Mobile Application Development in collaboration with representatives from the mobile ecosystem. These guidelines are designed to help application developers embed privacy into new applications and services.

However, these principles, even where fully enacted, can only go so far in providing consumers with the required level of choice. The mobile network operators have little 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 network 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. This commitment has resulted, among other initiatives, in the provision of leadership in this space through the GSMA Privacy Design Guidelines for Mobile Application Development, which emphasise that:

- Mobile network operators should ensure privacy risks are considered when designing new apps and services, and develop solutions that provide customers with simple ways to understand their privacy choices and control their data
- Developers of mobile device applications should embed industry-developed privacy principles and related design guidelines such as the GSMA mobile privacy principles
- Protection should be designed into new applications and services (i.e., privacy by design) to provide transparency, choice and control for the individual user, to build trust and confidence



42. Personal data is referred to as 'personal information' within the GSMA Privacy Principles

# 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 network 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.

Emerging 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.[43] Such localisation requirements can be found in a variety of sector- and subject-specific rules including for financial service providers, professional confidentiality or for the public sector and are sometimes imposed by countries in the belief that supervisory authorities can more easily scrutinise data that is stored locally.[44] While 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.

4

### Addressing the privacy and security of cross-border data flows

Running a mobile network generates large amounts of data on a daily basis. Every call and data transfer needs to be logged and then processed against tariff and account balance data in order to bill individual users for the services they use. Large batches of operational data are generated and stored regarding traffic loads, fault logs or customer enquiries (e.g., change of tariff, change of address). The net result of these demands is that mobile network operators are major users of global data centre storage and processing services. Consumers benefit from the wide range of services, innovation and advanced solutions that operators are able to offer, directly or via a third-party, by accessing and using these global services, either directly from the operator or a third-party.

Ensuring the integrity and security of such data is a major undertaking and requires complex solutions. Many mobile network 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 in multiple countries. Doing so allows them to build economies of scale and expertise by combining multiple countries' needs together to build a holistic and 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 network 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

43. Anupam Chander and Uyen Le, 2015. "Data Nationalism", Emory Law Journal; and Jonah Force Hill, 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", Hague Institute for Global Justice
44. European Commission, "Building a European Data Economy Communication", pg.5

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 network operators to develop privacy-enhancing technologies and services to protect consumers.

It is important to restate the distinction here between the personal data that mobile network 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 network operators, both in terms of what data has been transferred by users and how it can be accessed.

## 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 data flows 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
- Also, to the extent that governments need to scrutinise data for official purposes, they should achieve this through existing lawful means and appropriate intergovernmental mechanisms that do not restrict the flow of data

Mobile network 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

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.

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.

# 5 Protecting Public Safety

As providers of critical national infrastructure, mobile networks play an important role in protecting the general public and society as a whole. For example, mobile networks are used as a means of communication for the emergency services, particularly when responding to major incidents, while many incidents are reported by the public via mobile devices.

As part of laws and regulation, including licence obligations, and in accordance with local legislation, mobile network operators are required to assist law enforcement agencies in line with an overall objective 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)[45] and the International Covenant on Civil and Political Rights (ICCPR)[46] recognise that individuals worldwide have the right to communicate with each other

45. 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/

46 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

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 define that these rights can only be restricted in very limited pre-described 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 which 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 have a number of important implications for government, industry and other stakeholders and these are also outlined in detail later in this chapter.

## 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**

# 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[47] 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 that guide mobile network operators in how to respond to these requests. In November 2016 the United Kingdom (UK) passed new legislation[48] 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. Questions have also arisen as to the role that telecommunications network and service providers play in relation to such access. In light of this, in 2011 a group of mobile network operators and vendors formed the Telecommunications Industry Dialogue (ID) (see below) to jointly work on privacy and freedom of expression issues, 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.[49]

Legislation often lags behind technological developments[50] 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 is 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 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.[51] 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.

47. 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
48. For more information, see: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
49. 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.
50. GSMA, 2016. "Mobile Policy Handbook: Government Access"
51. 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.[52]

- 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[53]
- 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[54]
- 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[55]
- 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[56]

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[57] where possible.



52. GSMA, 2016. "Mobile Policy Handbook: Government Access"
53. Ibid.
54. Ibid
55. Ibid.
56. Ibid
57. Ibid.

Case Study

# Telecommunications Industry Dialogue — transparency (authority request disclosure) reporting

**Why report...**

The Telecommunications Industry Dialogue (ID), officially launched in 2013, is a group of telecommunications operators and vendors who 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. These companies have a global footprint, providing telecommunications services and equipment to consumers, businesses and governments in nearly 100 countries worldwide.

One of the key purposes of the ID is shared learning. Furthermore, to build on the notion of transparency, ID operators AT&T, Millicom, Orange, Telenor Group, Telia Company, and Vodafone Group regularly publish reports that disclose information about the law enforcement requests they have received. They hope this reporting will help the public understand the context in which they operate and interact with law enforcement agencies.

**What is reported...**

Typically, the 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

These operators do however believe that, although it is States that carry the main responsibility to be transparent, measuring the number of requests received from authorities, with all its flaws, is the most sensible measurement available, without making it too complex. They also emphasise that only the governments who make these requests to communications providers are able to give the full picture of the extent of requests. (Telecommunications Industry Dialogue, see: https://www.telecomindustrydialogue.org/ )

# 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. 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.

A recent example of this occurred in Brazil, where the messaging service, WhatsApp, was allegedly insufficiently supportive of various criminal investigations.[58] In response, the government required mobile network operators within Brazil to restrict access to the WhatsApp services on three separate occasions since December 2015.[59] 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 were 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.[60] 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 that services have been restricted pursuant to a government order.[61]



58. The Financial Times, 2016. "WhatsApp ban ignites Brazil censorship fears"
59. The Guardian, 2016. "WhatsApp officially un-banned in Brazil after third block in eight months"
60. Examples of shutdowns can be found within the Internet & Jurisdiction Retrospective Database. Please see: http://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTYtMTEifQ
61. For more information on the Telecommunications Industry Dialogue and Global Network Initiative joint statement, see: 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 as 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 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.

5

## 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.[62] 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[63]
- 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[64]
- 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 it has been approved by a judicial authority, 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)[65]
- 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[66]

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 operators have made to improve their coverage.[67]

- 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[68]
- 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[69]
- 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[70]

62. GSMA, 2016. "Mobile Policy Handbook: Service Restriction Orders"
63. GSMA, 2016. "Mobile Policy Handbook: Service Restriction Orders
64. Ibid.
65. Ibid.
66. Ibid.
67. GSMA, 2016. "Mobile Policy Handbook: Signal Inhibitors"
68. Ibid.
69. Ibid.
70. 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. This is the requirement for users to prove their identity at the point at which they purchase a prepaid or 'pay as you go', subscriber identity module (SIM) card to use mobile services.

It used to be common practice that mobile network operators,[71] especially new entrants into a market, would distribute free SIM cards to potential customers, sometimes quite literally handing them out on street corners. Customers would then purchase credit via a pre-pay coupon and be able to use the SIM card and its phone number.

Some governments have argued that this arrangement 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 customers.

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. Depending on the country and the availability of standard identity documentation this can be a major hurdle[72]
- The increase in mobile device theft and the emergence of a black market for fraudulently registered or stolen SIM cards,[73] based on the desire by some consumers, including criminals, to remain anonymous
- 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[74]

Case Study

## Industry Collaboration

In 2012 The Uganda Communications Commission announced that mobile network operators would have to block all SIM cards that remained unregistered by the (final) deadline of 31 August 2013.

In an effort to beat this deadline, mobile network operators Airtel and Warid launched innovative campaigns to encourage more people to register; in addition to sending their customers SMS reminders of the final registration deadline they also offered free minutes and texts to those who registered before the deadline. They also gave consumers an option to partially-register by texting their unregistered mobile number to a toll-free number in order to avoid having their SIM deactivated by the imposed deadline; This partial registration option enabled consumers to indicate that their SIM cards were active and were therefore given more time to register in person even if they missed the deadline.
(GSMA, 2013. "The Mandatory Registration of Prepaid SIM Card Users: A White Paper")



71. Within 'User Registration', mobile network operators include other operators that provide wireless communication services while not owning the network, such as mobile virtual network operators (MVNO) or mobile other licensed operators (MOLO)
72. GSMA, 2016. "Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice"
73. GSMA, 2013. "The Mandatory Registration of Prepaid SIM Card Users"
74. Ibid.

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.[75] However, to date, there has been no empirical evidence that mandatory SIM registration directly leads to a reduction in crime.[76] 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[77] 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.[78]

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.

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 on-going 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. (GSMA, 2016. "Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice")

5

75. GSMA, 2016. "Mobile Policy Handbook: Mandatory Registration of Prepaid SIMs"
76. GSMA, 2016. "Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice"
77. 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
78. 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.[79]

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



79. GSMA, 2016. "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

5

# 6 Protecting Network Security and Device Integrity

Underpinning safe and secure use of mobile services is the security of the network infrastructure. In its simplest form this means that mobile network operators safeguard the integrity of communications across the network by securing critical assets (hardware, software and data) and preventing unauthorised access or intrusion to any of the nodes or links making up their networks. 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 has recently emerged as an added 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.

Telecommunications network infrastructure was originally designed as a secure, closed-loop system. Where networks did interconnect, such as at country borders (the first network operators in most countries were usually state-owned national monopolies), this was done on a transparent, bilateral and trusted basis. These networks have since multiplied and evolved as the world has become increasingly interconnected and technology has advanced. Today, any phone call or data transmission is likely to traverse many networks and, in the case of data, will often also 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 industry ecosystem to be vigilant and to respond to them.

Figure 6 summarises a range of threats which have the potential to undermine the integrity of networks by enabling unauthorised interception, impersonation or service interruption. The mobile industry has been responding to these threats primarily by improving on strong 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 issues that affect networks and devices and that have the potential to compromise the security required to keep customer communications safe and secure:

- Securing the Network
- Mobile Device integrity
- Future Network Developments

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

## Protecting Network Security and Device Integrity

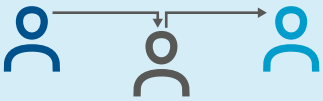
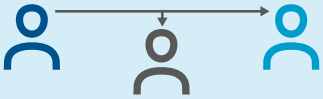
Industry players need to work together and coordinate with international law enforcement agencies to share threat intelligence to respond to malicious attacks on mobile networks and devices, as well as to identify perpetrators. This can be achieved through the engagement of existing security incident 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**

Figure 6

## 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)  |

6

# Network Security

## 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 currently developing recommendations to protect against the unauthorised use of these devices.[80] 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.

## Communications over the 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.

The launch of second generation networks (2G) in 1991 introduced the use of digital modulation which enabled robust protection and security to be implemented. The GSM standard, which underpins a large number of 2G networks, uses SIM (Subscriber Identity Module) technology to authenticate a user for identification and billing purposes, and to support encryption by the device to protect against attacks such as interception. The physical SIM concept, which has been based on smart card technology, has proved remarkably robust and continues to be a critical component of 4G networks today. This will continue in the future through innovations such as the embedded SIM.[81]

2G networks were primarily designed to support voice call communications but had basic data transmission capabilities and also, introduced the popular SMS text messaging service. 3G networks, launched in early 2000's, were the first to have data transmission built in as a core capability, introducing near-broadband web browsing and multimedia integration, and introduced additional security capabilities.



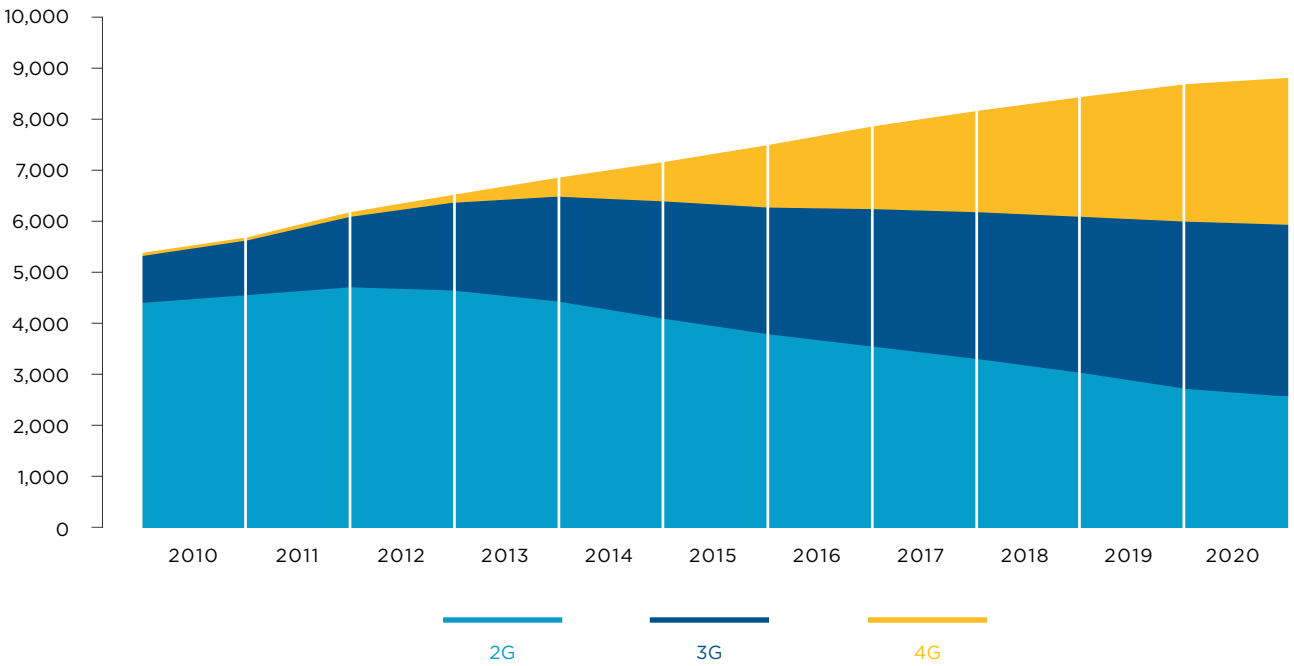
80. Committee on Oversight and Government Reform, 2016. "Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations"
81. The embedded SIM is a chip that is fitted into mobile devices, and provides the same level of security as the current SIM technology. It provides added flexibility by enabling operator profiles to be downloaded, so that users can change providers without the need to change the physical chip. This is particularly relevant for machine-to-machine (M2M) devices. See: http://www.gsma.com/newsroom/press-release/leading-m2m-alliances-back-the-gsma-embedded-sim/

However, security weaknesses in the ITU-defined Signalling System Number 7 (SS7) protocol, along with other interconnect protocols that are used to route voice calls and support services between and across networks can expose mobile networks and their customers to a range of vulnerabilities, such as eavesdropping, location tracking or data interception. Monitoring, detection and blocking capabilities exist to mitigate the threats posed to interconnect protocols and to messaging. The GSMA recognises the need for mobile network operators to respond in a comprehensive and collective manner to mitigate these risks. The GSMA's Fraud and Security Group has undertaken significant work to provide advice to network operators on how to mitigate SS7 security risks.[82] Furthermore, operators need to take all necessary precautions to protect against the interception of sensitive data, including subscriber credential details.

The fourth generation of mobile communication standards (4G) offers high-speed mobile broadband access to smartphones and other devices. The adoption of 4G wireless networks (see Figure 7) has introduced a switch to all-IP (Internet Protocol) which resolves the SS7 vulnerability when implemented between operators, but the adoption of new protocols can itself create fresh security challenges. Exploitation of vulnerabilities on these networks can be minimised by ensuring the security capabilities that are inherent in the standards are properly deployed and configured; advice is available from the GSMA on how best to achieve that.

**Figure 7**

## Global connections by technology (millions, excluding M2M)




82. For more information, see: http://www.gsma.com/newsroom/all-documents/ir-70-sms-ss7-fraud/

A more commonly reported challenge of communication relates to GSM Gateways, or "SIM Boxes" as they are commonly called. GSM Gateways can 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 with the result that services that depend on CLI become unavailable to users to which traffic has been routed by GSM gateways (e.g., service can be denied to prepaid service users who need to top up their credit levels). The absence of CLI can also have implications for lawful interception and the legal obligations network operators have to support law enforcement agencies in their licensed markets. Because of the impacts on service availability and general security, GSM gateways use is illegal in some markets. Where permissible, mobile network operators are encouraged to implement measures to prevent the use of gateways by third party carriers.

While mobile network operators continue to mitigate against the threat to their networks and their consumers, it is important to note that the same should be expected of operators of public wireless networks, such as public 'Wi-Fi Hotspots' or hotel Wi-Fi connections. The operators of these networks and customers should deploy appropriate safeguards (e.g., Virtual Private Networks) to help secure the wider communications ecosystem.

## Key implications for government, industry and other relevant stakeholders

While no security technology is guaranteed to be unbreakable, attacks on GSM-based networks and services are uncommon, as many would require considerable resources, including specialised equipment, computer processing power and technical expertise beyond the capability of most people or organisations.[83]

The barriers to compromising mobile security have been very high, and the GSMA considers that research describing possible vulnerabilities has generally been of an academic nature.[84] 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 the dissemination of information can be done promptly in response to incidents. Such an initiative could include regulators or other government authorities such as national Computer Emergency Response Teams (CERTs)
- 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. 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 brings the 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.

6

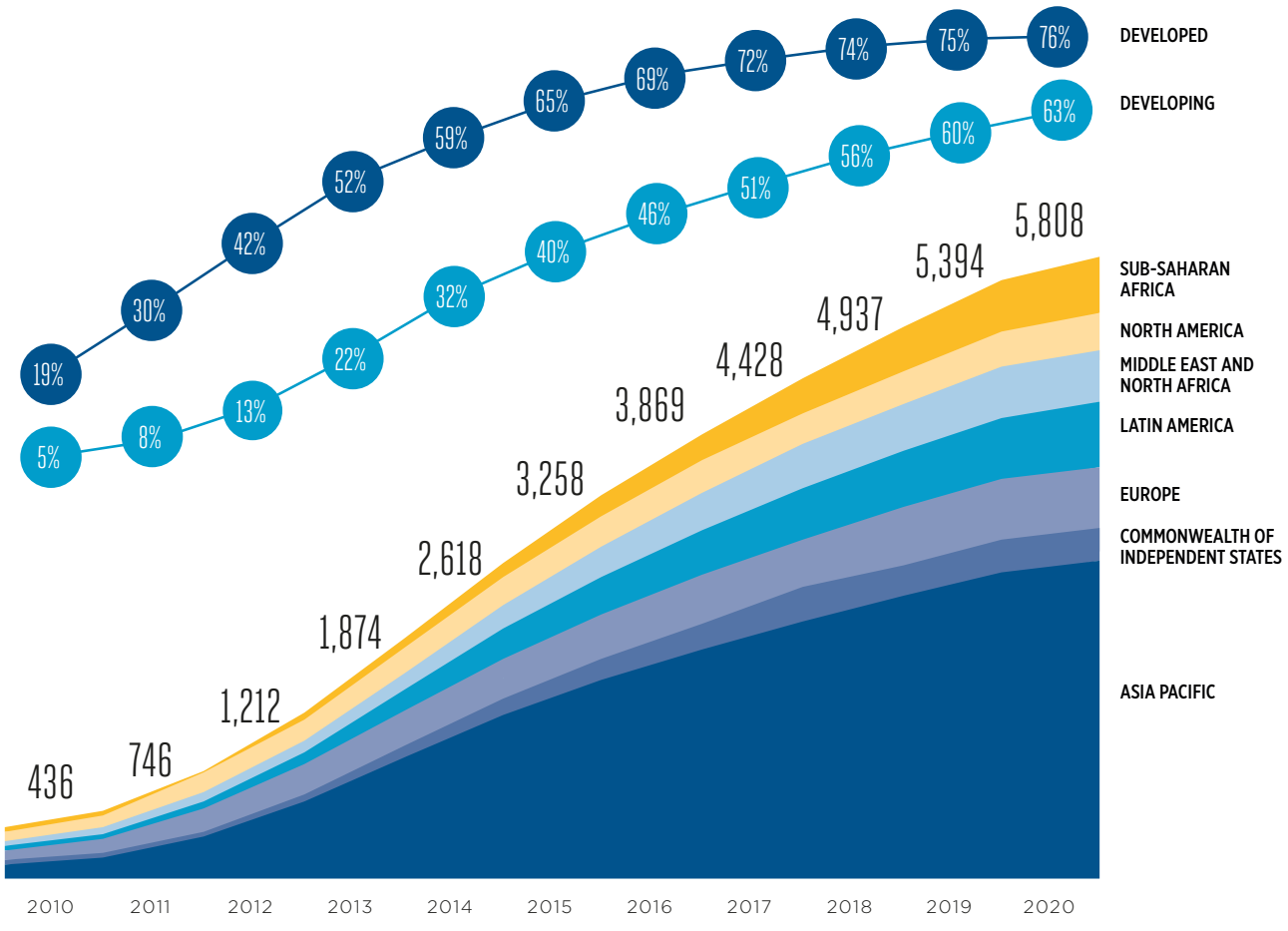
83. GSMA, 2016. "Mobile Policy Handbook: Mobile Security"
84. Ibid.

# Mobile Device Integrity

As 3G, 4G and, in the future, 5G networks are deployed, the adoption and use of mobile devices such as smartphones have increased. It is expected that by 2020 two out of three connections in emerging markets and three out of four connections in developed markets will be smartphone connections (see Figure 8). Application providers are considering how smartphones, perhaps with plug-in modules, can replace dedicated devices for use in hotspots or other highly sensitive environments. Furthermore, at least one billion machine-to-machine (M2M) connections are expected by 2020, impacting homes, factories, transportation, etc., and accounting for at least 10% of the global mobile market.[85]

**Figure 8**

## Global smartphone connections and adoption (millions)




85. GSMA, 2014. "Cellular M2M forecast and assumptions: 2010-2020"

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. As an attractive item for thieves (due to their relatively high value and small size), organised criminals often seek to change the IMEI[86] 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.[87]

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 to 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,[88] 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.[89] 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 has helped develop protection mechanisms such as those described in the GSMA IoT Connection Efficiency Guidelines[90] 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 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,[91] which provides certification of 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 current development of a programme for infrastructure OEMs.

The GSMA also seeks to support internet service providers or 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.[92]

6

86. The IMEI and the issues relating to theft of mobile devices is discussed in greater detail in Section 3. Protecting Consumers
87. These issues are discussed in further detail within the chapter, "Protecting Consumers"
88. 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. For their public statement, see: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
89. USA Today, 2016. "Hacked home device caused massive Internet outage"
90. For more information, see: http://www.gsma.com/connectedliving/gsma-iot-device-connection-efficiency-guidelines/
91. For more information, see: http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
92. GSMA, 2016. "Mobile Policy Handbook: Mobile Security"

# Future Network Developments

The Internet of Things (IoT) is a broad set of developments that involve connecting a whole range of new devices to the internet, from connected cars to household appliances. These devices will connect to a range of networks including Wi-Fi networks, dedicated low-power networks, as well as mobile networks, and using both licensed and unlicensed spectrum. The next generation of mobile networks technology, for example, network function virtualisation and 5G, will provide part of the IoT connectivity, and will usher in an era of even faster mobile broadband and pave the way for 5G-optimised services. These optimised services may include support for cutting-edge technologies such as tactile internet, virtual reality and enhanced broadcast services.

### Securing the Internet of Things

IoT presents huge growth opportunities for the mobile industry and many others, and with the advent of new business partners and new equipment suppliers, it is essential that security is forefront in the minds of those entering this commercial space. Many devices and equipment items which have previously not been connected to any form of network, need to have adequate security protections designed into equipment and services from the outset. This will require vendors and developers who have never previously had to consider such issues to include robust and sophisticated security quickly. The GSMA has produced IoT security guidelines[93] and an associated security self-assessment scheme[94] for a range of ecosystem players.

The development of the 5G standards and protocols, including those relating to network security, are being developed specifically for this technology. The GSMA is playing a leading role in capturing and prioritising requirements and ensuring that they are addressed and built in to the new standards. This on its own, however, only addresses a single link within the future IoT and considerable effort and attention is needed to ensure the security of the many other components and services within the highly interconnected infrastructure which will form part of the IoT as it evolves.

## 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, as well as the 5G ecosystem.[95]

- GSMA recognises that it has a key role to play in gathering and prioritising 5G security requirements for standardisation. Discussions are already underway and 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

6

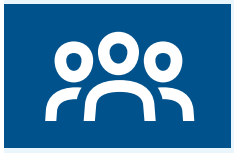
93. For further information about the GSMA IoT Security Guidelines, see: http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
94. For further information about the GSMA IoT Security Self-Assessment scheme, see: http://www.gsma.com/connectedliving/iot-security-self-assessment/
95. GSMA, 2016. "Mobile Policy Handbook: 5G – The Path to the Next Generation"

6

# 7 Mobile Industry Safety, Privacy and Security 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 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**

7


**GSMA HEAD OFFICE**
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601