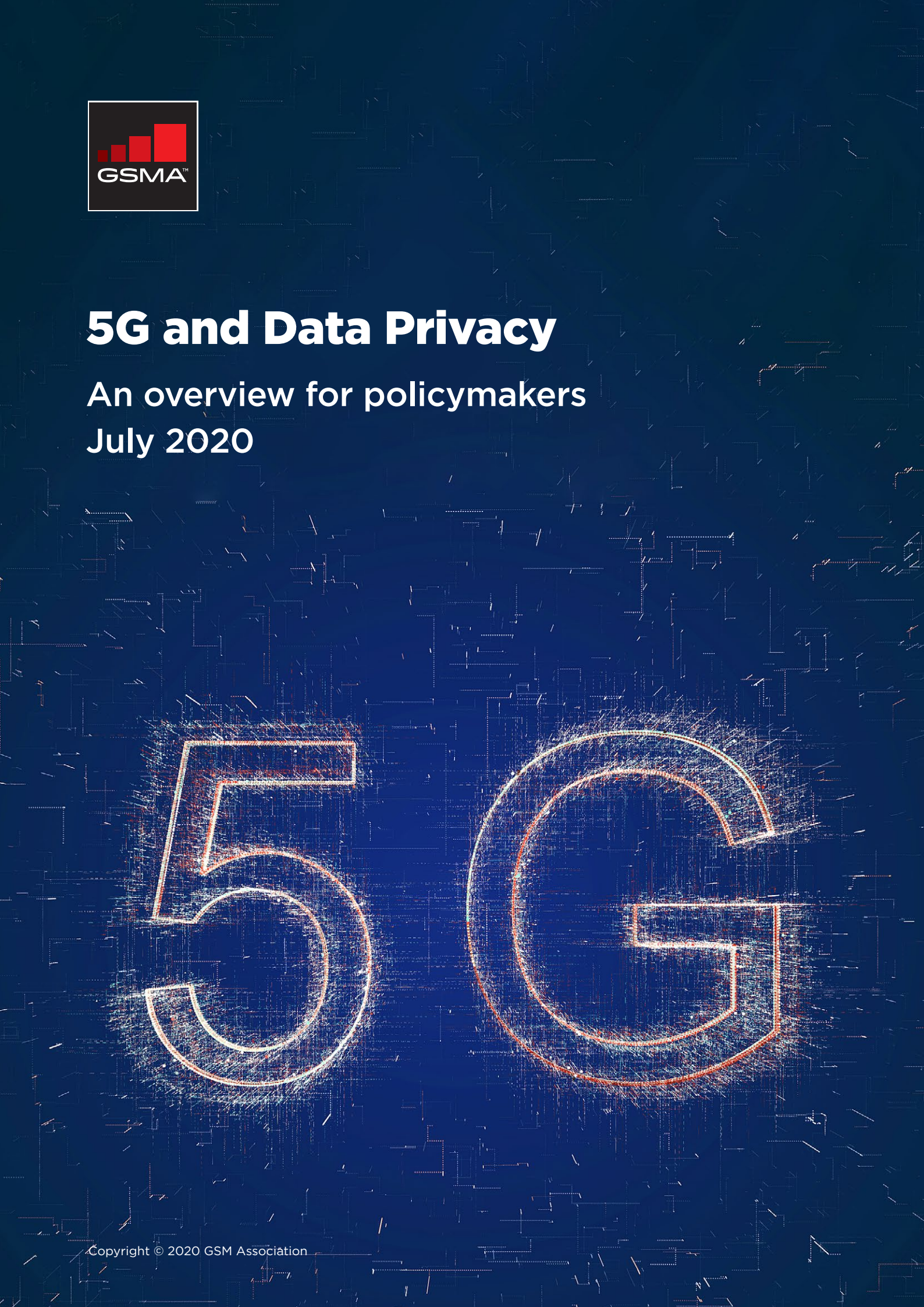
5G and Data Privacy

An overview for policymakers
July 2020



About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 750 operators with almost 400 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 and @GSMAPolicy

Contents

The new world of 5G

5G is rolling out around the world and promises to provide seamless connectivity to support diverse innovations such as smart homes, driverless cars, industrial automation, 3D films and augmented reality. 5G will enable billions of Internet of Things (IoT) devices to be deployed and a vast number of new applications to be conceived. These innovations have the potential to improve people's lives, for example, by facilitating remote surgery or enabling a blind skier to ski without human assistance.

5G is not just faster mobile networks and it is not just a matter for telecom operators. As connectivity becomes increasingly fluid and flexible, 5G will change the types of service and business models that are possible in unpredictable ways; much in the same way as the sharing economy and apps have changed the way we interact with organisations, government and each other. The volume and granularity of traffic and location data generated during 5G communications will increase, organisations will be able to customise their virtual network requirements for specific use cases and an explosion of novel data-driven applications that leverage 5G could lead to a greater volume and variety of personal data usage.

This flexibility will help industry to meet and continuously respond to a variety of businesses and consumer needs including:

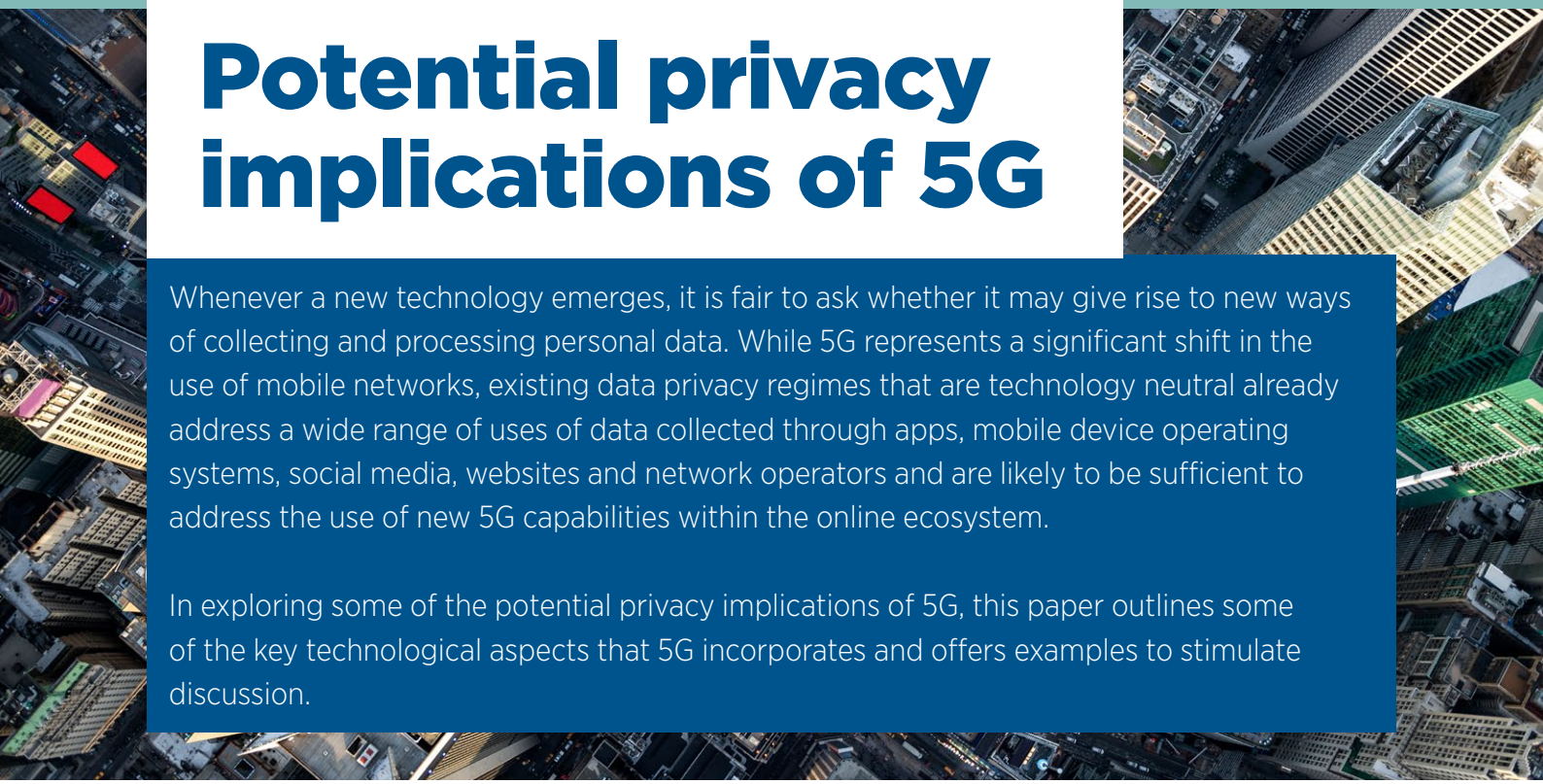
- **Enhanced mobile broadband** e.g: enables fast 3D video and 4K screens;
- **Low latency**[1] e.g: enables vehicle automation and self-driving cars;
- **Massive connectivity** e.g: enables a low volume of data to be transmitted from a large number of IoT devices like smart meters;
- **Wider coverage** to ensure seamless service experience across networks and country boundaries;
- **High density** of devices and Device to Device (D2D) connectivity e.g: in factories;
- **Seamless mobility** for uninterrupted service delivery and stable quality in scenarios with medium to high velocity e.g. high-speed train, aviation;
- **Mixing licensed and unlicensed networks** that may also belong to multiple different service providers e.g: 5G and WiFi;
- **Energy efficiency** e.g: when IoT devices need very long battery life.

1. 'Latency' refers to the time it takes for a packet of data to traverse the network. Low latency is extremely important for applications such as driverless cars that will require on-board computers to take extremely quick decisions, VR applications, precision agriculture and drones control.

Enhanced connectivity will bring with it new business models, innovations and a greater convergence of sectors and technologies. Countries that have already adopted a smart data privacy law approach should be well-placed to deal with the risks considered in this paper. A smart data privacy laws approach[2] is characterised by rules that are risk-based, technology and sector-neutral and promote the concept of 'Accountability'.[3] Under the principle of Accountability, organisations are encouraged to not only comply, but also be able to demonstrate how they comply through effective data governance policies and processes, for example, to conduct data privacy impact assessments, to be transparent and to avoid or mitigate the risk of harm to individuals through good 'Privacy-by-Design' practices. Such data privacy regimes have always acknowledged that the context of data processing, taking all relevant circumstances into account, is what determines risk rather than the particular technology or type of data viewed in isolation.

While the current rules and guidance are sufficiently flexible, a more nuanced understanding of how 5G works will help anticipate and evaluate the range of circumstances that could influence risk. As new business models and uses of personal data begin to emerge, this paper explains some of the relevant features of 5G to help industry, authorities and consumer groups to explore the data privacy aspects of the evolving 5G landscape.

2. Smart Data Privacy Laws Achieving the Right Outcomes for the Digital Age, June 2019 www.gsma.com/publicpolicy/resources/smart-data-privacy-laws
3. For further information on 'Accountability', please see GSMA's Smart Data Privacy Laws. The Centre for Information Policy Leadership (CIPL) also has numerous resources explaining the concept that can be found at www.informationpolicycentre.com



Potential privacy implications of 5G

Whenever a new technology emerges, it is fair to ask whether it may give rise to new ways of collecting and processing personal data. While 5G represents a significant shift in the use of mobile networks, existing data privacy regimes that are technology neutral already address a wide range of uses of data collected through apps, mobile device operating systems, social media, websites and network operators and are likely to be sufficient to address the use of new 5G capabilities within the online ecosystem.

In exploring some of the potential privacy implications of 5G, this paper outlines some of the key technological aspects that 5G incorporates and offers examples to stimulate discussion.

1. Higher frequencies, smaller cells

Context

A mobile network consists of three conceptual parts: radio access network allowing devices within a certain area (a cell) to connect to an antenna on the cell tower, a core network and a transfer network between the radio and core elements.

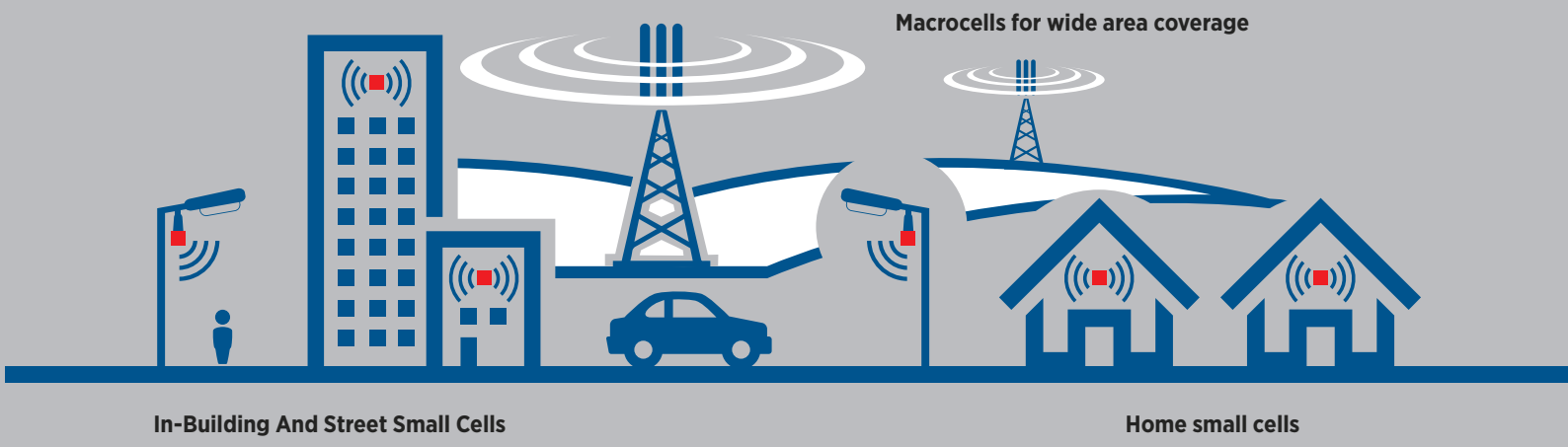
To achieve higher speeds, 5G networks will use higher radio frequencies, sometimes referred to as mmWave[4]. However, signals transmitted over higher frequencies degrade faster and hence, travel a shorter distance. The signals are also less capable of travelling through buildings or trees, thus, requiring smaller cells, many of which will be at ground level or within buildings (like WiFi is today).

Privacy Considerations

The smaller cell size in 5G does imply that more accurate geolocation data will be generated on the networks. However, satellite positioning systems such as GPS or Galileo, which drive numerous location-based consumer services such as for navigation or fitness tracking, will continue to provide a far higher degree of accuracy. If anything, this reemphasises the need for horizontal rules that protect consumers consistently regardless of the technology or business sector.

When network location data is used for purposes such as the planning of smart cities or reducing carbon emissions, this is typically done using insights or dashboards showing only the mobility of people at a non-identifiable aggregated level. Smaller cell sizes in 5G do not reduce this protection. Data from 5G networks will continue to be aggregated and rendered non-identifiable. Organisations involved in such projects should continue to follow a risk-based approach and consideration of available safeguards.

Representation of a 4G/5G Mobile Network



2. Massive MIMO, beamforming and bouncing

Context

MIMO (Multiple Input Multiple Output) simply means that more than one antenna is used to transmit and receive a radio signal thus improving the quality of the communication channel. In 5G networks we can expect to see a growth in the number of antennae allowing many more signals to be sent.

Rather than pushing out the same signal in all directions, 5G will use different combinations of antennae at cell sites to send a focused beam in the direction of the receiver (often referred to as 'beamforming'). Boosting the power of the signal increases the distance the signal can travel before it degrades so that it can reach the device. In a process referred to as 'bouncing' a signal can reach a user via an indirect route by bouncing off surfaces such as walls or roads. Typically, a communication will comprise multiple packets of information that may bounce off different surfaces before reaching the user.

Privacy Considerations

Some of these technologies have already been implemented in non-5G networks and so are not entirely new with 5G. The system does not know and does not need to know precisely where a particular device is geographically. It simply pushes the signal out in a way that works for the device to receive the signal. No data is generated or stored regarding which antennae are used, their inclination, or the power used for a particular signal. As the multiple packets comprising a communication will likely have bounced off multiple unknown surfaces it would, in any event, be virtually impossible to infer anything from such parameters regarding the direction of the device or the distance between the base station and the device.

4. mmWave is generally considered to be frequencies between 30GHz and 300GHz due to the wavelength.

3. 'Network slices' and an adaptable 'system of systems'

Context

5G is designed to be flexible. It will be able to support new applications with very different requirements such as Gigabit data rates, low latency and high reliability. It achieves this by allowing the key components of the physical telecommunications networks to be configured virtually in a way that suits the particular needs of industry verticals and individual organisations. These configurations are often referred to as 'network slices'.[5] For example, a network slice could provide efficient support for large numbers of connections, enabling the IoT. An in-car infotainment system, for example, will have very different requirements from assisted driving devices that send data at an ultra-low latency to nearby traffic. An engineer using an augmented reality headset has very different needs than a public safety camera.

From a mobile operator's point of view, a network slice is an independent end-to-end logical network that runs on a shared physical infrastructure, capable of providing a negotiated service quality. It could span across multiple parts of the network (e.g. terminal, access network, core network and transport network) and could be deployed across multiple operators. A network slice comprises dedicated and/or shared resources, e.g. in terms of processing power, storage, and bandwidth and has isolation from the other network slices.

Network slicing results in a more efficient use of communications infrastructure for everyone: mobile network operators can use the same physical infrastructure to serve their business customers in flexible ways; consumers benefit from a greater variety of services that optimise performance for whatever activity they are engaged in; and organisations can configure their virtual networks to suit their specific needs on demand (e.g. dimensioning, configuration) by means of Application Programming Interfaces (APIs) offered by the mobile operators. For example, an organisation may provide smart meters and smart home devices that have low bandwidth and speed requirements, but may also deliver video streaming, gaming and VR/AR equipment.

Privacy Considerations

Organisations that configure their virtual networks may demand more detailed information about users' behaviour patterns derived from network data in the same way that an over-the-top service does with non-network data. Such services must be treated equally under data protection and privacy laws rather than creating a distinct set of rules for different sectors.

Some virtual network slices may be configured exclusively to manage machine-based processes without any impact on individuals (e.g. manufacturing, pollution monitoring etc.). Clarification that laws for the protection of personal data would not apply to such configurations could enable data analytics and B2B sharing of non-personal data.

Network slicing also means that certain data can be isolated from the rest of the network. For example, a financial institution may deploy hardware (non-virtual) components of the network that are completely dedicated to their customers so that sensitive data can be stored at the financial institution premises for maximum privacy and security.

4. Edge computing and network resources

Context

Mobile network operators could make 5G network resources, such as edge computing, storage and analytics capabilities, available to business customers. Mobile edge computing (MEC) is essential to the low-latency use cases that form an integral part of 5G. For example, organisers of a sports event may want to provide slow motion videos or augmented reality content to people in the stadium. This could be achieved by storing the content related to the game in MEC servers closest to the stadium. Similarly, a factory may collect data from sensors, vehicles, wearable devices and drones used in the factory and process these locally helping it to operate more efficiently.

Privacy Considerations

While the servers used in mobile edge computing may reside closer to network elements to reduce latency, they are essentially providing a cloud or hosting service.

The ability to process data in the network edge in which it has been generated, could obviate the need to send the data further into or outside the network, reducing wider circulation of personal data than is necessary.

It may be important to distinguish between the content data which is stored locally by the MEC provider to provide the service and the communications data which would remain subject to the usual licence conditions and legal requirements.

5. More devices, more applications

Context

5G may lead to a plethora of novel ideas for the collection and use of personal data at the device operating system or application level. These could represent a significant expansion of existing use cases or they could be entirely new use cases. These new applications and devices may provide fresh channels for the generation of personal data that sit 'on top' of the network itself in the same way that mobile phone apps do in the 4G world and are not created by the mobile network operators.

Privacy Considerations

This 'over-the-top' activity is flagged here as a consideration as it may lead to a significant increase in the volume of data privacy work requiring more staff, resources, training and awareness for both organisations and regulators.

As 5G may be deployed in wealthier cities before it is deployed poorer cities or rural areas, any insights from 5G network data or data from applications that are only viable in an area of 5G deployment may contain an inherent bias reflecting wealthier metropolitan populations. This is not a barrier to using such insights or data, but merely something organisations should be aware of when developing products and services or leveraging machine learning algorithms.

5. For further introductory information on network slicing, please visit www.gsma.com/futurenetworks/resources/an-introduction-to-network-slicing-2/

6. Security

Context

Information security will be enhanced in 5G including the implementation of the 'Subscription Concealed Identifier' (SUCI) to encrypt the subscriber identity number (which is part of the international mobile subscriber identify or 'IMSI').[6] Authentication and encryption protocols designed to prevent some of the better-known threats such as 'IMSI catchers' and 'man-in-the-middle attacks and more extensive encryption and authentication throughout the networks ensure that sender and receiver have an established trust and the end-to-end relationship is secured.

Having virtual network components means that core network operations may be performed through functions outside the operator network e.g. the cloud which can complicate the supply chain and liability chain, but can also present an opportunity. A virtualised, software-driven architecture can also mean that elements of the network can be isolated or containerised and vulnerabilities can be remediated quickly and remotely.

Privacy Considerations

If the physical infrastructure of 5G networks is constantly repurposed for new virtual configurations that are provided by numerous operators and potentially managed by business organisations, it could create complexity concerning who is ultimately responsible for security at any given point and who is liable for the consequences of data breaches. This could, therefore, require a much more collaborative approach to security across the entire 5G ecosystem.

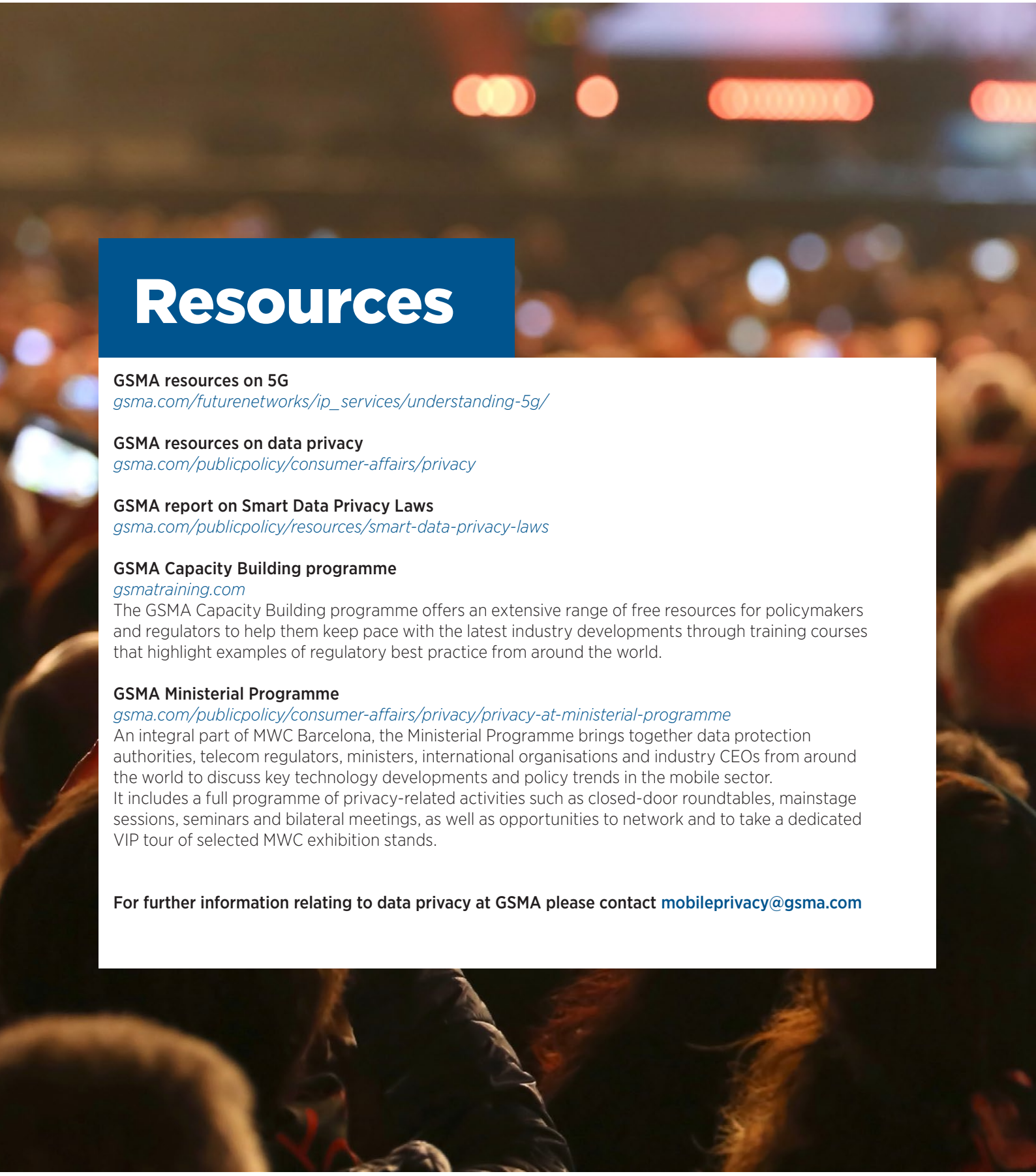
5G will enable the deployment of a vast number of IoT devices that could be manufactured by anybody. Security assurance mechanisms and industry guidelines such as the GSMA IoT Security Guidelines[7] will become increasingly important.

6. For further information regarding security in 5G please visit www.gsma.com/security/securing-the-5g-era/
7. The GSMA IoT Security Guidelines and Assessment www.gsma.com/iot/iot-security/iot-security-guidelines/

Conclusion

5G will open up exciting new opportunities that will benefit individuals in all kinds of ways, but, as with any new technology, innovations involving personal data will need to be considered carefully. Smart data privacy laws that embrace the concept of 'Accountability', encourage Privacy-by-Design, are based on the identification and mitigation of risks and are sector and technology neutral will be in a good position to accommodate novel use cases and deal effectively with new privacy risks.

Evaluating new risks as 5G develops will require interests to be balanced and judgments to be made within organisations and as a society. To this end, it is hoped that an open, inclusive discussion regarding 5G and data privacy will benefit everyone, most of all the individuals whose data may be processed.



Resources

GSMA resources on 5G
gsma.com/futurenetworks/ip_services/understanding-5g/

GSMA resources on data privacy
gsma.com/publicpolicy/consumer-affairs/privacy

GSMA report on Smart Data Privacy Laws
gsma.com/publicpolicy/resources/smart-data-privacy-laws

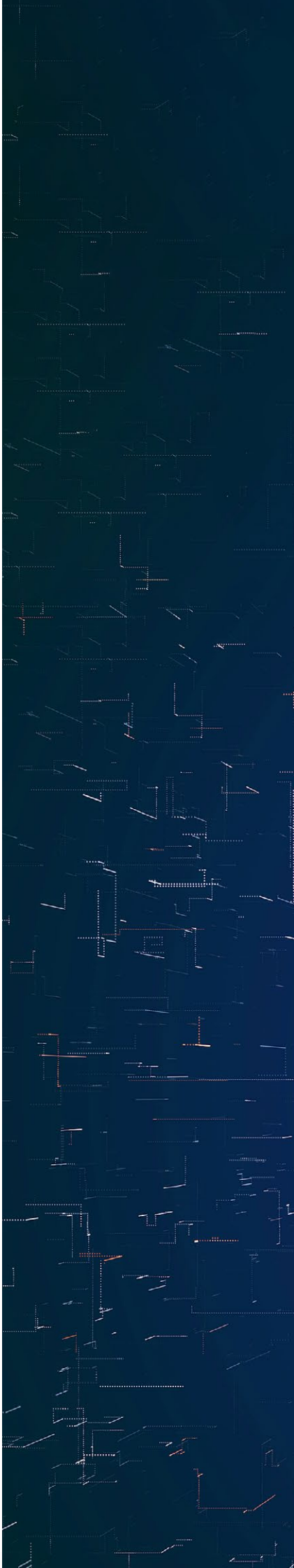
GSMA Capacity Building programme
gsmatraining.com
The GSMA Capacity Building programme offers an extensive range of free resources for policymakers and regulators to help them keep pace with the latest industry developments through training courses that highlight examples of regulatory best practice from around the world.

GSMA Ministerial Programme
gsma.com/publicpolicy/consumer-affairs/privacy/privacy-at-ministerial-programme
An integral part of MWC Barcelona, the Ministerial Programme brings together data protection authorities, telecom regulators, ministers, international organisations and industry CEOs from around the world to discuss key technology developments and policy trends in the mobile sector.
It includes a full programme of privacy-related activities such as closed-door roundtables, mainstage sessions, seminars and bilateral meetings, as well as opportunities to network and to take a dedicated VIP tour of selected MWC exhibition stands.

For further information relating to data privacy at GSMA please contact mobileprivacy@gsma.com


gsma.com/publicpolicy

To download the report please visit the GSMA website at
gsma.com/5g-and-data-privacy



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