GSMA

etno

The Proposed European ePrivacy Regulation

Use cases for enabling privacy-protective innovative products and services

April 2018

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 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, Mobile World Congress Americas and the Mobile 360 Series of conferences.

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

For more information on this topic, please visit **www.gsma.com/policies_for_a_digital_europe**

Follow the GSMA on Twitter: **@GSMAEurope** and **@GSMAPolicy**

ETNO has been the voice of Europe's telecommunication network operators since 1992 and has become the principal policy group for European electronic communications network operators. Its 39 members and observers from Europe and beyond are the backbone of Europe's digital progress. They are the main drivers of broadband and are committed to its continual growth in Europe. ETNO members are pan-European operators that also hold new entrant positions outside their national markets. ETNO brings together the main investors in innovative and high-quality e-communications platforms and services, representing 70% of total sector investment.

For more information, see ETNO's website at **www.etno.eu**

Follow ETNO on Twitter: **@ETNOAssociation**

The GSMA and ETNO are committed to reinforcing the role of telecom operators as the “backbone of the Digital Single Market,” as noted by European Commission Vice-President Ansip. Connectivity is the lifeblood of innovation and economic growth.[1] As telecom operators endeavour to build the networks critical to Europe’s digital future, we must consider the broader regulatory environment in the EU. We envision an enabling regulatory environment that supports individuals’ fundamental rights, while permitting technological developments and spurring investment. To manifest this reality, we urge policymakers to consider the impact of the ePrivacy Regulation (ePR) on both existing and future products and services that are critical to Europe’s digital growth, including the Internet of Things (IoT) and 5G.

This document highlights use cases impacted by the currently proposed ePR, and (on page 11) outlines how the proposed legislation could be amended to better align with the GDPR and enable such use cases.

[1] See ‘World Development Report 2016: Digital Dividends’, available at: http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf on page 4.

We recognise the importance of the confidentiality of communications, and appreciate continued focus on this issue in the draft ePR. However, when it comes to the processing of communications metadata, including location data, we believe that the ePR's corresponding rules are overly restrictive. In contrast, the General Data Protection Regulation (GDPR) enables the processing of personal data based on a number of legal grounds and following a thorough risk-based approach. The GDPR thereby strikes the right balance between the ability to innovate and the protection of people's personal data, through the application of data protection by design, data protection impact assessments, and technical safeguards such as pseudonymisation[2] and encryption. Processing of personal data under the GDPR is guided by the overall principles of accountability, purpose limitation, data minimisation, storage limitation, and integrity and confidentiality among others.

The described risk-oriented principles underpinning the GDPR should therefore also be applied to processing metadata, in order to reflect the balanced approach not only horizontally, but also in sector-specific privacy regulation, to allow telecoms operators, and other electronic communications service (ECS) providers, to equally compete in a responsible way with market players along the digital value chain.[3]

As one of the key arguments for imposing strict obligations on the processing of metadata, the ePR refers to the Court of Justice of the European Union (CJEU) Tele2 judgment, which contains statements related to the sensitivity of metadata "as a whole". The CJEU states therein that the general, systematic and indiscriminate retention of metadata as a whole for purposes of crime prevention is not proportionate. What matters for the CJEU therefore is not the nature of the data alone, but also the scope, purpose, and (lack of) safeguards and context of the processing.

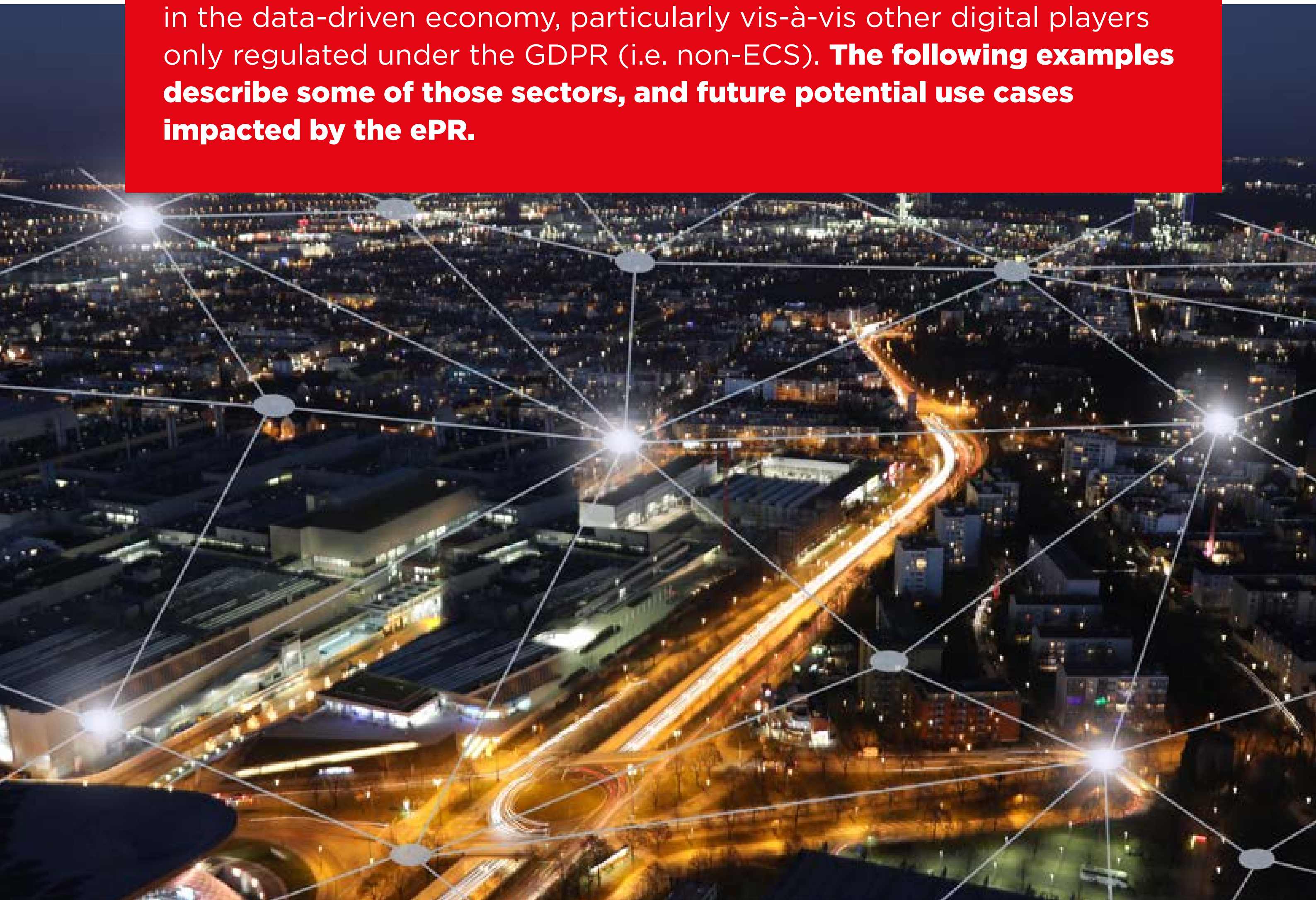
[2] For more information on pseudonymisation and its application as a privacy-protective safeguard, see 'White Paper on Pseudonymization Drafted by the Data Protection Focus Group for the Safety, Protection, and Trust Platform for Society and Businesses in Connection with the 2017 Digital Summit – Guidelines for the legally secure deployment of pseudonymization solutions in compliance with the General Data Protection Regulation', available at: https://www.eprivacy.eu/fileadmin/Redakteur/News/2017_Data_Protection_Focus_Group-White_Paper_Pseudonymization.pdf.

[3] Electronic communications service providers include those providers offering interpersonal communications services, consistent with the proposed definition of ECS in the Electronic Communications Code.

These considerations lead to the conclusion that not all metadata can be defined, from the outset and per se, as sensitive. The processing of metadata should therefore be subject to a risk-based analysis, to determine in a case-by-case assessment whether processing could result in high risks for the end-users concerned. The ePR should thus be aligned with the GDPR to create a coherent regulatory framework for the protection of privacy and personal data.

The current ePR proposal only allows the use of metadata under very limited circumstances. This will prevent various legitimate, unobtrusive uses of data across a number of sectors for the benefit of society and the European economy. The European Commission has repeatedly emphasised the importance of big data for innovation, and Europe should encourage the development of big data across different sectors, including telecommunications.

The telecommunications industry believes that big data can flourish, while also respecting individual privacy, in a consistent and coherent regulatory environment. The additional obligations imposed by the ePR will negatively impact the ability of some sectors to participate in the data-driven economy, particularly vis-à-vis other digital players only regulated under the GDPR (i.e. non-ECS). **The following examples describe some of those sectors, and future potential use cases impacted by the ePR.**



Impact on IoT: Industrial IoT

The continued growth of IoT is critical to the Digital Single Market. Industrial IoT represents a significant part of this market. While there are numerous different industrial IoT sectors, according to the European Commission (EC), manufacturing is Europe's largest IoT market, growing from €88 billion in 2014 to €287 billion in 2020.[4] The EC found that companies harnessing new technologies, including big data and IoT, can perform 10 times better than their peers.[5] Using this technology also creates a wide range of other benefits, such as reducing workplace accidents.[6]

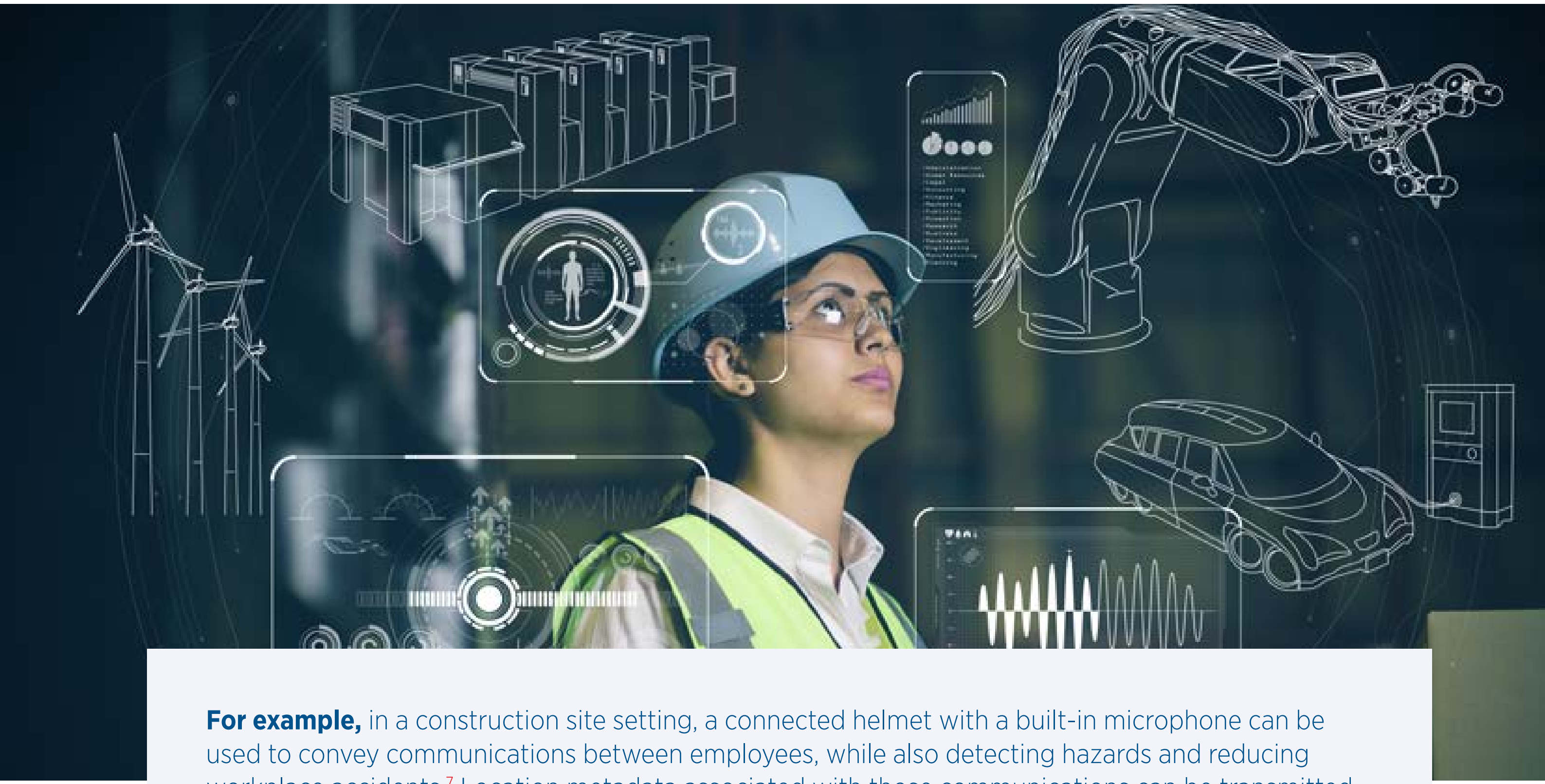
As currently drafted, the ePR will impact the implementation of industrial IoT. According to recital 12, the ePR should apply to the transmission of machine-to-machine (M2M) communications, and the principle of confidentiality enshrined in the ePR should also apply to the transmission of M2M communications. We would argue that this should be clarified, and that the recital should instead note that the ePR applies to the transmission of M2M communications to the extent necessary to protect the confidentiality of communications, and as far as the pure conveyance of signals is concerned.

The ePR will also impact IoT because the ePR's narrowly defined legal bases for processing require consent in circumstances where other legal bases such as legitimate interest would be more appropriate.

[4] See 'Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination', available at: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

[5] See 'Final report Strategic Policy Forum Digital Entrepreneurship', available at: http://ec.europa.eu/DocsRoom/documents/9462

[6] See 'Wearable devices aim to reduce workplace accidents', available at: https://www.ft.com/content/d0bfea5c-f820-11e5-96db-fc683b5e52db; According to the International Labour Organization, every 15 seconds, 151 workers suffer a work-related accident. See http://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_211627/lang--en/index.htm



For example, in a construction site setting, a connected helmet with a built-in microphone can be used to convey communications between employees, while also detecting hazards and reducing workplace accidents.[7] Location metadata associated with those communications can be transmitted in real time to other heavy machinery such as cranes, to assist with logistics and to help avoid accidents.

Under the ePR, the employee must provide consent to this use of location metadata. If the factory adds new heavy machinery such as a forklift, and wants the connected helmets to share location metadata with the machinery, a new consent would have to be obtained from the employee.

The data cannot be anonymised because the identity of the employee must be known to assist with logistical elements and to quickly identify the individual in the case of an accident.[8] Asking for consent every time a new device connects to the smart helmet will not lead to better privacy - it will lead to box ticking.

[7] See 'Engineering Safety with Smart Helmets,' available at: https://www.asme.org/engineering-topics/articles/manufacturing-design/engineering-safety-with-smart-helmets

[8] Note that the proposed ePR does not include a basis for processing data to protect the vital interest of the data subject. If the addition of this legal basis is considered, it should mirror the basis in the Art. 6(1)(d) and Recital 46 GDPR. This will allow operators to process data to protect the lives of users, without having to first determine whether they are "physically or legally incapable of giving consent" per Art. 9(2)(c) GDPR. Vital interest processing under Art. 6 GDPR would enable more efficient emergency services in connected cars, etc.

Network Planning and Optimisation: Building Europe's Future Networks

Investment in network infrastructure is critical to Europe's digital economy. According to a European Commission supported study, 5G deployment costs are forecast to be approximately €56.6 billion, and that is likely a conservative estimate.[9] 5G will be able to deliver much higher throughput, lower latency, reliability, and a massive number of connections, all tailored to the users' needs through the network slicing concept. To better allocate network resources, telecom operators are working to develop innovative network optimisation and planning methods. Using big data, operators could collate data from different network sources to identify problems and better understand network usage. This saves time, money, and supports a more robust network for consumers. Increased intelligence about network usage and optimisation is particularly important as Europe moves towards 5G, because this analysis enables the creation of network slices that meet customer needs.

The ePR allows processing of metadata to meet "mandatory quality of service requirements" (in accordance with the proposal for an Electronic Communications Code), which is not broad enough to enable network efficiencies and improvements beyond mandatory requirements. The ePR instead requires that telecom operators rely on anonymised data, or ask for specific, opt-in consent. This approach will lead to consent fatigue for customers and inefficiencies for telecom operators, and ultimately lower service quality for customers.

Alternatively, analytical tools applied to pseudonymised network data can be used to learn more about network usage and problems while preserving confidentiality. This is true both for existing networks and future 5G networks.

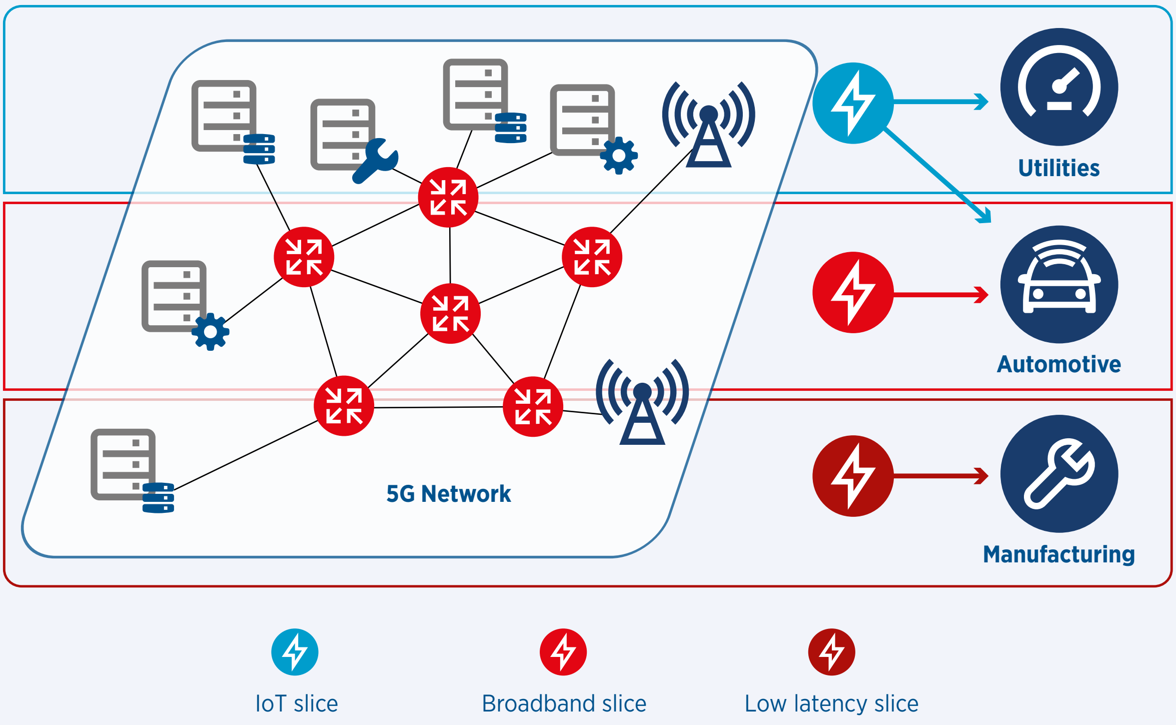
For example, in the context of existing telecom networks: if a telecom operator identifies problems at a certain location but is not able to detect the root cause based on simple aggregated statistics, it may be necessary to analyse pseudonymised personal data from the customers at that location to ascertain the nature of the problem. In general, the more narrow the group of customers affected (for instance a group with a particular model of phone), the larger the risk that the sample size will not be sufficient to render the data legally anonymous.

Also, anonymised data will not always convey enough information to the operator, because the operator needs specific information about the problem. The aim is not to learn about individual users, but only to learn about general network functioning and solutions, sometimes for only a small group of affected end-users. Where anonymised data is sufficient to solve the problem, the general principles of data protection in any case require anonymised data to be used (see data minimisation principle of the GDPR).

[9] See 'Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe', available at: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=17802

For example, in the context of 5G network planning: to determine where to locate the antennas and processing power needed to realize the variety of tailored 5G services, telecom operators must understand the needs of users of different network slices.[10] In this respect, network planners could generally rely on anonymised data, but since the user needs must often be known and optimised for small geographical areas, the number of users contributing to the aggregated data will in some particular situations be small, which would, by some regulators, no longer be defined as anonymous. For 5G, this challenge will be even larger than today since antennas will be located closer to each other in the future, requiring higher geographical granularity in the analysis. Furthermore, analysis will have to be done on each network slice, and each slice will have fewer data subjects as users compared with today's general purpose 4G network.

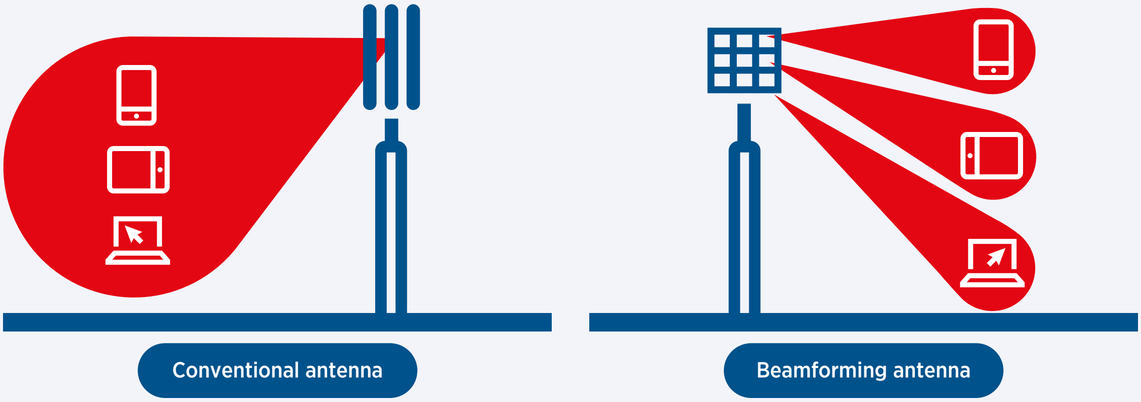
Network Slicing



[10] A network slice is a part of the end-to-end network delivering a set of services tailored to a given set of properties like data rate, mobility, latency, quality of services, etc. Different use cases like massive mobile broadband, Internet of Things, ultra-reliable low latency communications or fixed wireless access will require a different set of service capabilities delivered by the network.

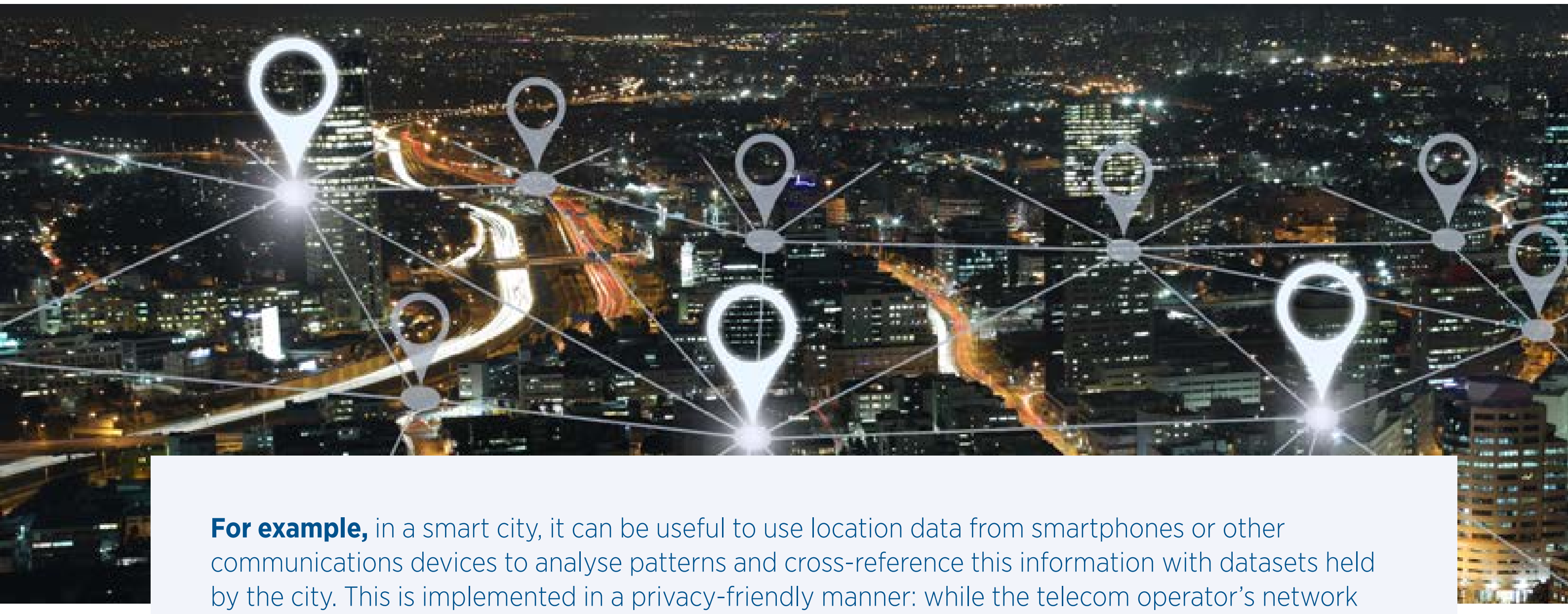
For example, 5G networks will be self-optimising. The “beamforming” antennas used in 5G networks make much better use of spectrum by allowing the same spectrum to be used in different beams from a single antenna-site, at the same time compensating for the limited range of 5G due to the use of higher frequency bands. The antenna may for instance beam the connection to a moving bus, delivering signals optimised for the need and the movement of the receiving end. A beam may theoretically even be directed to a single house or a single individual user. An example could be an ambulance in need of a high reliability, low latency, semi-high bandwidth connection while moving at high speed through the city.

It is important to keep in mind that the technology is not yet production ready and the precise functioning is accordingly unknown. However, since the antenna will be self-optimising in real-time, the antenna will need to know information about usage needs, and while the telecom operator may want to rely on aggregated data as far as possible, the level of aggregation necessary to achieve anonymisation may not be possible to achieve, particularly not if the beam is directed to a single moving vehicle containing few users. It may be possible to introduce directional antennas, but their full capacity could not be utilised without self-optimisation that might require the processing of pseudonymised data. If a user would not consent to the use of beamforming antennas, inter-site distance would shrink due to shorter range of higher frequencies. In such a case, 5G would be far too costly to deploy due to the increased number of sites to be established.



Creating Smarter Cities

Cities and regions across Europe are embracing connected technologies, big data and continually improved network infrastructure to become "smarter". This generates significant benefits for many stakeholders, including citizens, local governments and industry. As the EU has noted, smart cities are also linked to important societal goals such as ensuring sustainable development.[11] Municipalities and cities are keen to advance their relationships with telecom operators through new, innovative uses of data to better understand and plan. However, as illustrated in the following examples, the ePR could frustrate some of these ambitions.



For example, in a smart city, it can be useful to use location data from smartphones or other communications devices to analyse patterns and cross-reference this information with datasets held by the city. This is implemented in a privacy-friendly manner: while the telecom operator's network generates metadata (including location data), this data can be effectively pseudonymised and subject to other safeguards, and third parties would only be given access to general knowledge at the aggregate level (graphs, pie charts). In this manner, significant societal gains could be realised, while eliminating the link with the individual and without necessitating prior consent from each potentially concerned individual, which would be required under the current ePR, and which would also be difficult to obtain to achieve a critical mass of data necessary for sound data analysis.

[11] See 'Horizon 2020 : Work Programme 2018-2020 - 10. Secure, clean and efficient energy', available at: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-energy_en.pdf

For example, during snowstorms, city governments need to issue warnings to drivers in neighbourhoods to move their cars so that the roads can be plowed. A connected car's telematics system can provide network information identifying the location of the car in the path of the snow plow, and a network could provide aggregate information about the number of users in a particular area to better plan snow removal routes. Alternatively, the city could provide an open data API including information regarding snow removal routes. Using pseudonyms, the network can send a message to the owners of cars in the respective area requesting that they park their cars elsewhere. While the city will never know the identities of the car owners, the network would be able to generally notify the car owners, based on their location, before the snow removal. This will create significant improvements in snow removal speed, resource and energy allocation, and would prevent the forced towing of cars. This cannot be achieved using anonymised data as the connecting identifier would be missing.

Enabling Europe’s Digital Economy: Amending the ePrivacy Regulation to Align with the GDPR

To enable these use cases, one approach would be to allow processing based on the **legitimate interest** of the electronic communications services provider. Drawn on Art. 6(1)(f) GDPR, legitimate interest would allow ECS providers, including telecom operators, to use metadata responsibly, on a case-by-case basis, weighing the rights of the end-users, the interests of the provider and, for example, broader societal interests. This is consistent with the principle of accountability enshrined in the GDPR that requires a thorough assessment of the data processing operation concerned. Introducing such a legal basis would also significantly incentivise the development of European networks and IoT, where complex relationships between multiple actors intervene in processing data, often with little privacy impact.

For example, an operator offers enhanced services to a customer based on their usage measurements. According to legitimate interest, the operator should also be able to use these usage measurements to make smart network investments, provided it considers the interests of the customer carefully, considers safeguards for the data, and communicates effectively with customers. This is a far more effective tool to change and embed privacy culture within a company than merely collecting consent.

To further align with the GDPR, the ePR should embrace the concept of **further compatible processing** established in Art. 6(4) GDPR, which provides that further processing should be allowed, also without prior consent, if a new processing purpose is compatible with the initial purpose for which the data was collected. This compatibility test provides for the need to carefully weigh the interests of the individual, taking into account the context and nature of the collected data as well as the consequences of processing, including whether appropriate safeguards like pseudonymisation have been used to reduce risks. In order to more strongly align with the provisions of the GDPR, further processing should be allowed, if the new processing meets the compatibility test.

For example, an operator collects metadata to transmit a call. Under further compatible processing, the operator could use that data to analyse usage patterns for the purpose of network planning and optimisation, provided that the processing is subjected to the compatibility test and is protected through the implementation of safeguards such as pseudonymisation, which eliminates the direct link between data and individual.

The telecoms industry believes that pseudonymisation can play a significant role when considering whether further processing is compatible. We note that the European Commission embraced pseudonymisation as a privacy-friendly technique in the GDPR, "to reap the benefits of big data innovation while protecting privacy." We want the ability to use this technique to develop innovative new products and services for consumers, while protecting their privacy, and avoiding the inevitable "consent fatigue" that would result if no alternatives to user consent are recognised in the ePR. Additionally, using pseudonymisation helps operators avoid unnecessary identification of individual users. For many types of processing, operators only need to know the pattern of movement of unidentified individuals over a period of time. In this case, requiring consent from individuals – who would need to be identified as opposed to pseudonymised – may actually contravene the data minimisation principle of the GDPR.[12]

The more flexible approaches of both Art. 6(1)(f) and 6(4) GDPR to process metadata would enable the use cases highlighted in this paper in a privacy-protective way that is aligned with the robust, risk-based approach embodied by the GDPR. For these use cases, end-users would be prior informed about the purpose of processing, safeguards would be provided and the possibility to opt-out would be given in line with the GDPR, *see* Art. 12, 13 and 14 GDPR as well as Art. 21 GDPR. In addition, the basic principles enshrined in the GDPR continue to apply: data minimisation, purpose limitation and storage limitation (Art. 5 GDPR).

Other legal bases, such as allowing for the processing necessary for scientific research or statistical purposes as suggested by the Estonian Presidency of the Council in December 2017, are a welcome step but do not offer the same applicability as legitimate interest and further compatible processing. Mere statistics – numerical or quantitative measurements – are not sufficient to enable smart cities or urban planning, where a qualitative assessment of the data needs to be made and where the purpose is to investigate and understand movement patterns in time and space, without aiming to identify and/or track individuals. Additionally, in some jurisdictions, "statistical purposes" has been interpreted very narrowly, even as narrowly as "statistics for the purpose of statistics". If such narrow interpretation is applied, such legal basis applied to metadata would only enable very few of the opportunities we see. Consequently, it is necessary to introduce a broader reference to processing based on legitimate interest (Art. 6 (1)(f) GDPR) and further compatible processing (Art. 6(4) GDPR).

Conclusion

The telecommunications industry is working to fulfil the digital goals identified by the EU to realise the Digital Single Market. Doing so will continue to require investment in networks and commitment to research, development and innovation. Our industry is committed to achieve these goals in a privacy-protective way that respects confidentiality of communications, while also being afforded the flexibility to process data under a regulatory approach better aligned with the GDPR.

[12] See also Art. 11 and Recital 57 GDPR.

For more information, please visit the
GSMA Europe website at
www.gsma.com/policies_for_a_digital_europe

GSMA EUROPE
Park View, 4th Floor,
Chaussée d'Etterbeek 180
B-1040 Brussels, Belgium
Tel: +32 2 792 0550