A new IoT regulatory framework for Europe

White Paper
June 2019

vodafone

Contents

A note from Joakim Reiter and Stefano Gastaut

Few think of Europe as a frontrunner in the internet age. Yet as the digital transformation of societies and economies gathers pace, a window of opportunity has opened for Europe to re-establish itself as a global technology leader.

The reason for this opportunity is the growth of the Internet of Things (IoT), which provides the crucial link between the data economy and the physical economy. As everything and everyone becomes connected, IoT will be the foundation of Europe's future competitiveness and its digital society.

IoT has risen quickly on the agenda of policymakers across Europe, especially given the crucial role it can play in addressing pressing societal and economical challenges. For example, IoT can improve the environment and support energy transition. It can deliver preventive healthcare, increase agricultural yields while using less water and make smarter use of fertilisers. It can help with more efficient planning of public transport, improving congestion and reducing pollution. In fact, an analysis by the World Economic Forum found that an estimated 84% of IoT deployments are currently addressing, or have the potential to advance, the UN's Sustainable Development Goals.

As the EU's largest mobile company and a market leader in IoT, with over 85 million IoT-connected devices across many different sectors and industries, Vodafone wants to play its part in this digital transformation.

Europe represents an enormous opportunity when it comes to the development of IoT applications and services. IoT is a technology that plays to Europe's strengths as the world's largest integrated market, with a sophisticated industrial sector underpinned by excellent educational institutions.

Yet, as set out in this White Paper, there are already indications that Europe runs the risk of falling behind. These reports are an early warning for policymakers. Current policies and regulations are not adequately adapted for a world of machine-to-machine (M2M) communications and data. Scale is hindered by fragmentation between regulatory frameworks, between EU member states and between sectors. These are self-imposed handicaps that Europe can ill afford.

The EU needs to learn from past mistakes and successes. European institutions have already taken welcome and positive steps to ensure the free flow of non-personal IoT data between EU Member States. But, as explained in this report, more is needed: Europe needs an ambitious 'designed-for-IoT' regulatory framework that gets rid of unnecessary and unintentional barriers, ensures technological neutrality and builds on the successful experience of promoting world-class manufacturing prowess through European scale by leveraging its internal market.

The time to act is now. The USA and China are making strides with IoT technology. But Europe still has the chance to take the lead. A newly designed policy framework that reflects the needs of IoT will open up digital opportunities for people and businesses, and position Europe as a world leader in the next phase of the journey towards a digital society.

Joakim Reiter
Group External Affairs Director, Vodafone Group Plc

Stefano Gastaut
Internet of Things Director, Vodafone Business

Executive summary

The value IoT could bring to Europe is well recognised – from increased GDP growth from the sharing of machine-generated non-personal data to improved lives through smart applications. If the regulatory landscape is right, realising these benefits could transform Europe's standing in terms of global competitiveness and 5G connectivity.

However, studies show that the EU is already falling behind other global regions in relation to IoT adoption and sophistication and that urgent action is needed to address this.

On 29 April 2019, Vodafone brought over 100 stakeholders together in Brussels[1] to discuss Europe's future policy approach to IoT. This included speakers from the European Commission, the Body of European Regulators for Electronic Communications (BEREC) and the Organisation for Economic Co-operation and Development (OECD), and from the agricultural, automotive, aviation, energy and healthcare sectors.

Following from this event, we have prepared this White Paper to set out our multi-sectoral assessment of IoT applications in Europe. We find that the absence of an IoT-designed regulatory framework is significantly impacting the potential of IoT across the EU. The White Paper also incorporates input from the industry speakers who attended our 29 April event.

Our analysis reveals a number of issues with the existing regulatory regime, and its application, that are acting as significant obstacles to the development of IoT in the EU:

1. **uncertainty over how rules apply to IoT, meaning that rules primarily designed for human communications are being applied, thus raising the cost of doing business and introducing delays;**
2. **a fragmented application of rules across Member States, thus hindering the ability to operate seamlessly across the single market;**
3. **an undue difference in the treatment of different technologies; and**

   a. for historic reasons, rather than as a result of an objective analysis of the risk of harm, often different rules apply to IoT applications according to whether they are connected via cellular or non-cellular technology; while

   b. some EU industry-specific policies have explicitly favoured non-cellular technologies.

   Both significantly distort investment choices and hinder Europe's ability to keep up with its competitors on IoT innovation and adoption.

4. **limited adoption of other best practices in relation to IoT, including the voluntary sharing of non-personal machine-generated data, the use of IoT security measures and a contractual emphasis on resolving potential issues around IoT liability, that could promote European competitiveness and end-user trust in IoT.**

We believe that a new cross-sectoral IoT regulatory framework for Europe is needed, which would take the form of a new Recommendation under EU law. This would enshrine the principles (already established within the EU Treaty) that are particularly important to the development of IoT, codifying them into a 'designed-for' IoT framework that would provide clarity on the application of existing regulation, and therefore address the obstacles that have been identified.

By promoting these best practices, removing significant and unnecessary burdens, and by ensuring consumer and business confidence through effective regulation, the new framework will promote the data economy, foster growth and further the interests of European businesses, citizens and consumers.

Vodafone welcomes questions or comments on any of the proposals set out in this document. They should be directed to robert.macdougall@vodafone.com or oltion.xhezo@vodafone.com.

Event video accessible at
www.vodafone.com/iotpolicy

1 www.vodafone.com/iotpolicy

1. Background and context

In this section, we describe the IoT market and identify the EU regulations relevant to IoT. We also set out important recent policy learnings from the European Commission, the OECD and BEREC, and conclude by summarising some of the difficulties IoT investors and innovators in specific industry verticals have experienced as they seek to navigate the existing regulatory framework.

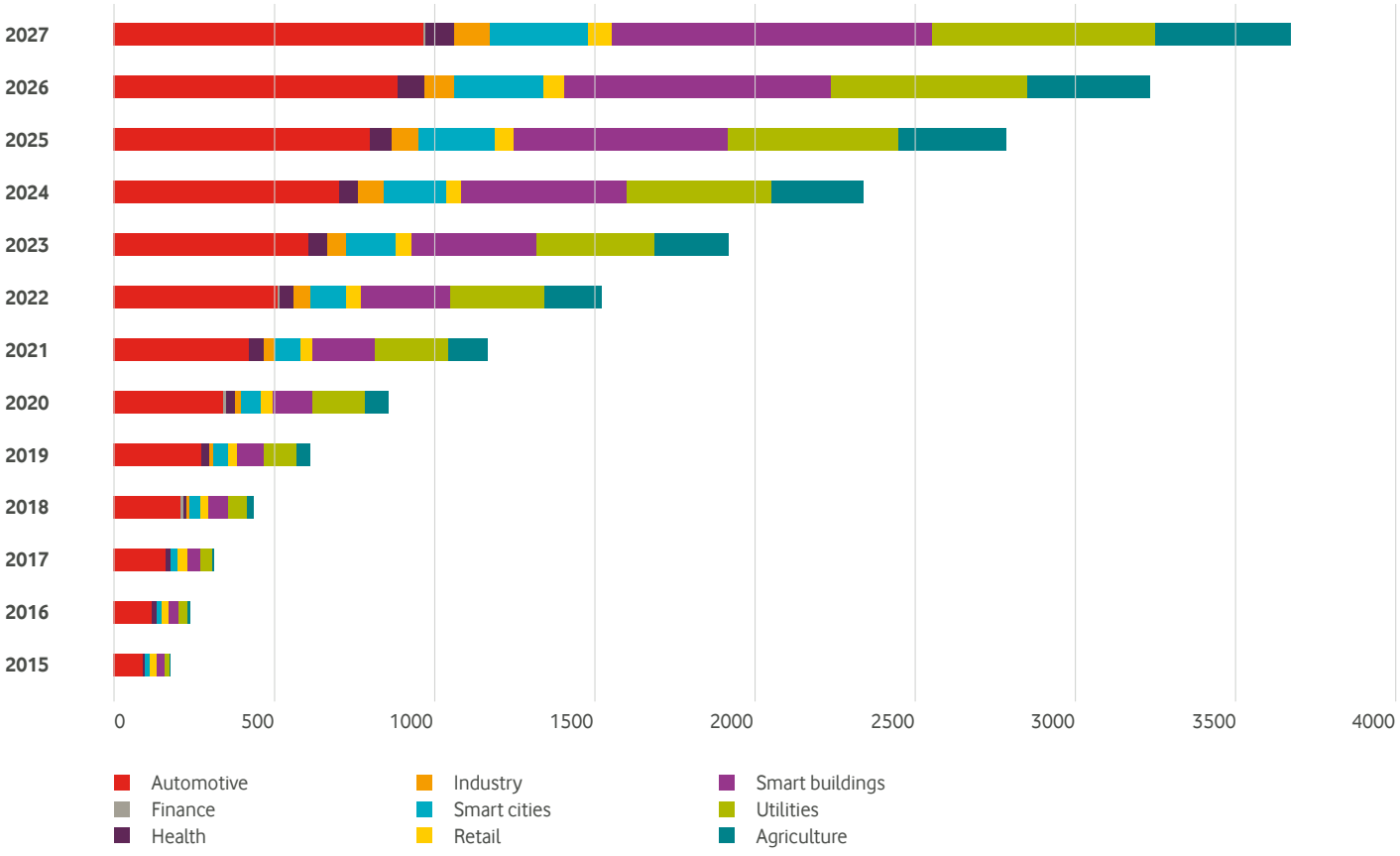
This overall context helps to frame our discussion later in the White Paper, where we:

- describe the significant regulatory obstacles to IoT's success in Europe (Section 2);
- identify how the IoT regulatory framework needs to be improved (Section 3); and
- propose a new cross-cutting IoT regulatory framework, in the form of a Recommendation, to ensure IoT realises its full potential for the EU economy and for its businesses and citizens (Section 4).

1.1 IoT cuts across a wide variety of market sectors, emphasising the need for a cross-sectoral regulatory approach

IoT is a very diverse market with a distribution of connections across many different sectors of the economy, as set out below. Although outside the scope of Figure 1, consumer IoT is also an important market segment, with IDC estimating that spending in this sector will reach $108 billion (€96 billion) worldwide in 2019, making it the second largest industry segment, with a focus on smart home, personal wellness and connected vehicle infotainment[2].

Figure 1: IoT connections worldwide share by sector



Source: Analysys Mason, IoT forecast: connections, revenue and technology trends 2018–2027, March 2019

2 IDC, Customer Insights and Analysis, 2019, available at https://www.idc.com/getdoc.jsp?containerId=prUS44596319

1.2 IoT also cuts across a range of connectivity technologies, emphasising the need for a technology-neutral regulatory approach

IoT is also diverse from a connectivity perspective. The variety of connectivity solutions, including cellular, satellite and private networks, enables providers to address diverse and evolving customer requirements, across a wide range of uses in different vertical sectors.

In summary, and as set out in Figure 2 below, Ericsson estimates that for 2018, approximately 12% of the total IoT devices were connected through mobile networks (cellular IoT)[3], while the rest were enabled through short-range[4] communication protocols, satellite connectivity or alternative Low Power Wide Area private networks.

Figure 2: Worldwide connected devices across different technologies

IoT	2018	2024
Wide-area IoT (including Cellular IoT)	1.4	4.4
Cellular IoT	1.0	4.1
Short-range IoT	9.3	17.8
Total	**10.8**	**22.2**

Source: Ericsson Mobility report, June 2019[5]

1.3 There is a complex web of regulation and policy relevant to IoT

Existing EU regulations relevant to IoT

One of the key characteristics of IoT is that it is inherently cross-cutting in nature. There is, therefore, a wide range of different regulations and policy initiatives that are relevant to the development of IoT in the EU.

For convenience, we group a number of these key initiatives into three broad categories: rules relating to the regulation of electronic communications services and networks, horizontal consumer protection rules and industry-specific rules. This non-exhaustive list includes:

Regulation relating to electronic communications networks and services

European Electronic Communications Code (EECC) (consolidating the Access Directive, Authorisation Directive, Framework Directive and Universal Service Directive), net neutrality (part of the Connected Continent Legislative Package), Roaming Regulation and ePrivacy Directive.

Horizontal law and regulation

The Regulation on the free flow of non-personal data, Cybersecurity Act, GDPR, Tangible Goods Directive, Directive on security of network and information systems, Consumer Rights Directive, Product Liability Directive and Unfair Commercial Practices Directive.

Industry-specific regulation

Automotive (e.g. Intelligent Transport Systems Directive, Type Approval Regulation, eCall Regulation), agriculture (Common Agricultural Policy), energy (e.g. Energy Performance of Buildings Directive), aviation (EU Basic Regulation for Drones) and healthcare (Medical Devices Directive).

European Commission activity on liability for emerging digital technologies and data sharing, interoperability, (re-)usability and access to data.

The European Commission has taken a variety of active steps to accelerate the take-up of IoT and unleash its potential in Europe for the benefit of its citizens and businesses. A particular focus has been to ensure a thriving IoT ecosystem, a human-centred IoT approach and a single market for IoT.

For example, the European Commission's Staff Working Document on liability highlighted challenges posed by the complex ecosystem of market operators which enables the roll out and functioning of the emerging digital technologies[6].

Also, it has been highlighted that contractual barriers are impeding the sharing, access and (re-)use of data in the EU, with issues that are more important for 'data users' than for 'data producers'[7].

Guidance has also been issued on sharing private sector data in the European data economy[8]. The Expert Group on Business to Government (B2G) data sharing is also examining non-personal data, which may include IoT devices.

OECD study on IoT measurement and applications confirms the diverse nature of the IoT market and the need for a joint policy approach.

In its October 2018 study[9], the OECD identified a variety of definitions that can be observed across National Regulatory Authorities, regions and actors in the value chain. The OECD proposes a taxonomy with a breakdown of IoT into categories, based on a 'case by case' approach, given that many connected devices will have different network and quality of service requirements (e.g. critical IoT applications such as remote surgery and automated vehicles will require high reliability and low latency connectivity).

3 The figures for cellular IoT are also included in the figures for wide-area IoT.

4 Short range largely consists of devices connected by unlicensed radio technologies, with a typical range of up to 100 metres, such as Wi-Fi, Bluetooth and Zigbee. This category also includes devices connected over fixed-line local area networks and powerline technologies.

5 Ericsson Mobility Report, June 2019, available at https://www.ericsson.com/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf

6 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51633

7 https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and

8 https://eur-lex.europa.eu/legal-content/EN/TXT PDF/?uri=CELEX:52018SC0125&rid=2

9 IoT measurement and applications, OECD Digital Economy Papers, October 2018 no. 271 accessible at https://www.oecd-ilibrary.org/science-and-technology/iot-measurement-and-applications_35209dbf-en

The study further recognised that *"New policy and regulatory challenges may emerge in some areas...Thus, creating indicators to inform policy making in these areas, is a priority"*.

BEREC Report on IoT indicators acknowledges the challenges in mapping the IoT ecosystem.

In its March 2019 report[10], BEREC acknowledged the challenges in mapping the ecosystem and proposed that a third-party study be commissioned during the second half of 2020.

In this document, BEREC recognised the need to take a proactive role to ensure technology neutrality and educate stakeholders.

BEREC further set out the need to build on its initial categorisation of IoT, based on a limited number of verticals, by classifying IoT services based on connectivity technologies (for example, cellular versus non-cellular connectivity), different spectrum usage (licensed or unlicensed), or network performance requirements.

1.4 A variety of industries have articulated concerns with the current framework, highlighting the need for urgent measures

Given the cross-cutting nature of IoT, a number of different industries have highlighted specific challenges relevant to the growth of IoT in the EU (a number of which were highlighted at the 29 April event).

AUTOMOTIVE MANUFACTURING

Uncertainty in the EECC

Opportunity

According to the European Automotive Manufacturers' Association (ACEA), connected and automated driving promises to revolutionise individual mobility within the space of just a few years. It will offer new mobility solutions that are cleaner, safer and more consumer-focused than ever, while also creating new areas of business for the automotive industry[11].

Challenge

ACEA believes that clarification of the EECC is required to ensure that electronic communication service (ECS) providers and M2M service providers can engage in the development of intelligent transport solutions and promote EU leadership in this domain without either side being subject to inappropriate and disproportionate regulatory obligations. This is also due to the definition of 'conveyance of signals' service, which ACEA and the European Automotive Telecoms Alliance (EATA) believe is confusing. This is troublesome in newly connected service areas with M2M communication without necessarily being able to unbundle the transmission layer from the service layer (e.g. V2V and V2I direct communication). It is also troublesome when the services are embedded in one contract towards the consumer (bundled services).

10 BEREC Report on Internet of Things indicators, BoR (19) 25, accessible at https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8464-berec-report-on-internet-of-things-indicators

11 https://www.acea.be/industry-topics/tag/category/connected-and-automated driving

Need for technological neutrality

Challenge

EATA has highlighted that technology neutrality is critical for the development of computer-aided manufacturing. As roll out will continue to be a priority, a technology-neutral regulatory framework that stimulates the adoption of new technologies will be key. This implies that any new policy initiative should not favour one technology over another but let market forces be a leading force in innovation and deployment[12].

Appropriate sharing of machine data

Opportunity

The sharing of machine-generated data can generate significant socio-economic benefits, amounting to €1.4 trillion in the EU by 2027[13].

Challenge

ACEA has taken active steps to promote appropriate sharing of machine data across the automotive ecosystem. Sharing of vehicle-generated data from sensors, components, systems and other devices requires a safe and (cyber)secure architecture and data flows. The automotive industry has fostered a dialogue at the International Organization for Standardization (ISO), where a vehicle-sharing model is standardised, called the Extended Vehicle. ACEA has launched a new educational website, www.CarDataFacts.eu, which provides a fact-based overview on everything related to the sharing of vehicle-generated data with third parties[14]. First applications are now seeing the light, e.g. in the framework of V2I sharing of data for road safety purposes[15]. However, such sharing is not yet widespread in the market as a whole.

AVIATION

Need for technology neutrality

Opportunity

Within 20 years, the European drone sector is expected to directly employ more than 100,000 people and have an economic impact exceeding €10 billion per year, mainly in services[16].
As has been highlighted by Copa-Cogeca – the EU employers' group of professional agricultural organisations – in combination with other 'smart' techniques, drones can contribute to enhanced resource efficiency, productivity and profitability, as well as greater sustainability, and provide reassurance for farmers. As the farming community is ageing rapidly, drones can help ease hard work, reduce working time and increase efficiency. They also have tremendous potential to involve young entrepreneurs in agriculture.
Airbus has tested the use of a mobile network to connect drones. As part of its ongoing trials in conjunction with the European Union Aviation Safety Agency, Vodafone has also carried out successful beyond visual line of sight drone trials in Spain and Germany[17].

Challenge

In regulation that has been developed at the European level, it was initially not clear whether licensed mobile networks would be allowed to connect drones[18]. It is also not clear in a number of Member States whether licensed spectrum can be used to connect drones, which are seen to be airborne, as opposed to terrestrial devices.

Network slicing for drone communications

Opportunity

As part of the Airbus test referred to above, 5G network slicing for drone communications was also tested. A robust slice for drone control and an independent slice for drone payload (a camera for inspection tasks such as rail maintenance) operated at the 5G connected mobility testbed at the A9 autobahn in Germany.

Challenge

The current regulatory framework is currently far from clear as to whether such prioritisation is allowed, for example, whether it is consistent with the concept of 'necessity' set out in the Net Neutrality Regulation.

AGRICULTURE

Non-personal IoT data sharing

Opportunity

Digital farming represents an unprecedented opportunity to create value and business opportunities by applying data-driven solutions. This includes improving resource efficiency, productivity, environmental processes, animal health and welfare, and providing tools to mitigate climate change. It can also decrease administrative and bureaucratic costs and enable science-based policies connectivity in rural areas.

12 See Manifesto: European Automotive and Telecoms Alliance at https://eata.be/wp-content/uploads/2019/03/05082-EATA-manifesto-March-2019.pdf
13 https://www.vodafone.com/content/dam/vodafone-images/public-policy/reports/pdf/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf
14 www.CarDataFacts.eu
15 https://www.government.nl/latest/news/2019/06/03/eu-countries-and-car-manufacturers-to-share-information-to-improve-road-safety
16 http://ec.europa.eu/growth/sectors/aeronautics/rpas_en
17 https://www.vodafone.com/content/index/media/vodafone-group-releases/2018/mobile-tracking-and-control-technology-for-long-distance-drone-flights.html
18 The draft of the European Commission's proposal for the regulation of Open Category drones specified the use of two unlicensed spectrum bands (2.4GHz and 5GHz) to connect drones. This was, however, modified in a subsequent iteration.

Challenge

Copa-Cogeca and a number of other partners have taken great steps to promote sharing of non-personal data across the agricultural supply chain[19]. However, such sharing is not yet widespread.

HEALTH

Opportunity

The EU spends around €700 billion each year on combatting chronic diseases. Emerging digital technologies can help the EU move towards prevention-focused and outcome-driven healthcare, reducing the cost of healthcare delivery while improving healthcare outcomes.

Challenges

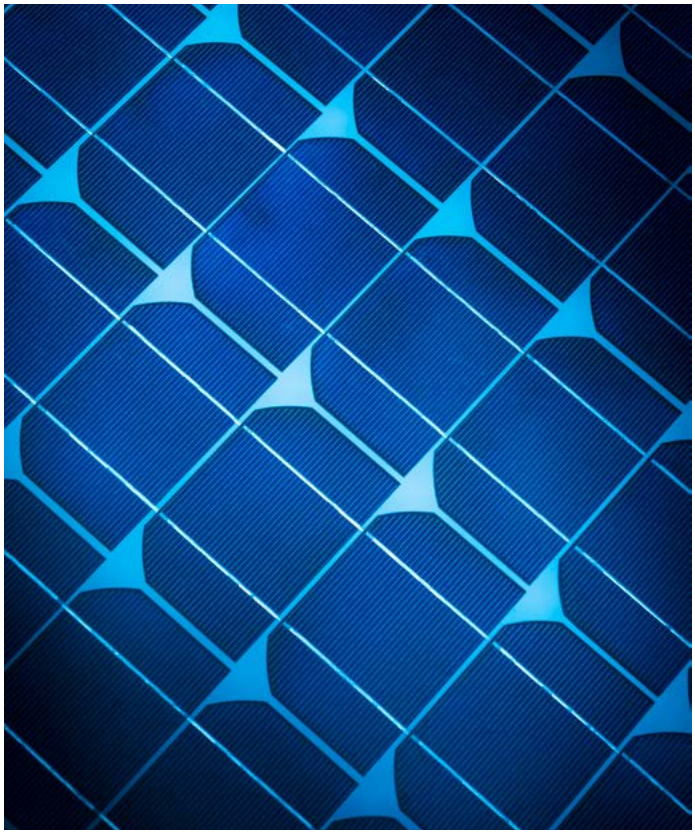
The current regulatory framework does not incentivise the reimbursement of digital therapies (i.e. remote patient monitoring), which in turn inhibits the adoption of IoT in healthcare from a user perspective.

Many med-tech customers operating across the EU would benefit from the harmonisation of patient records and data interoperability of digital patient records.

ENERGY

Opportunity

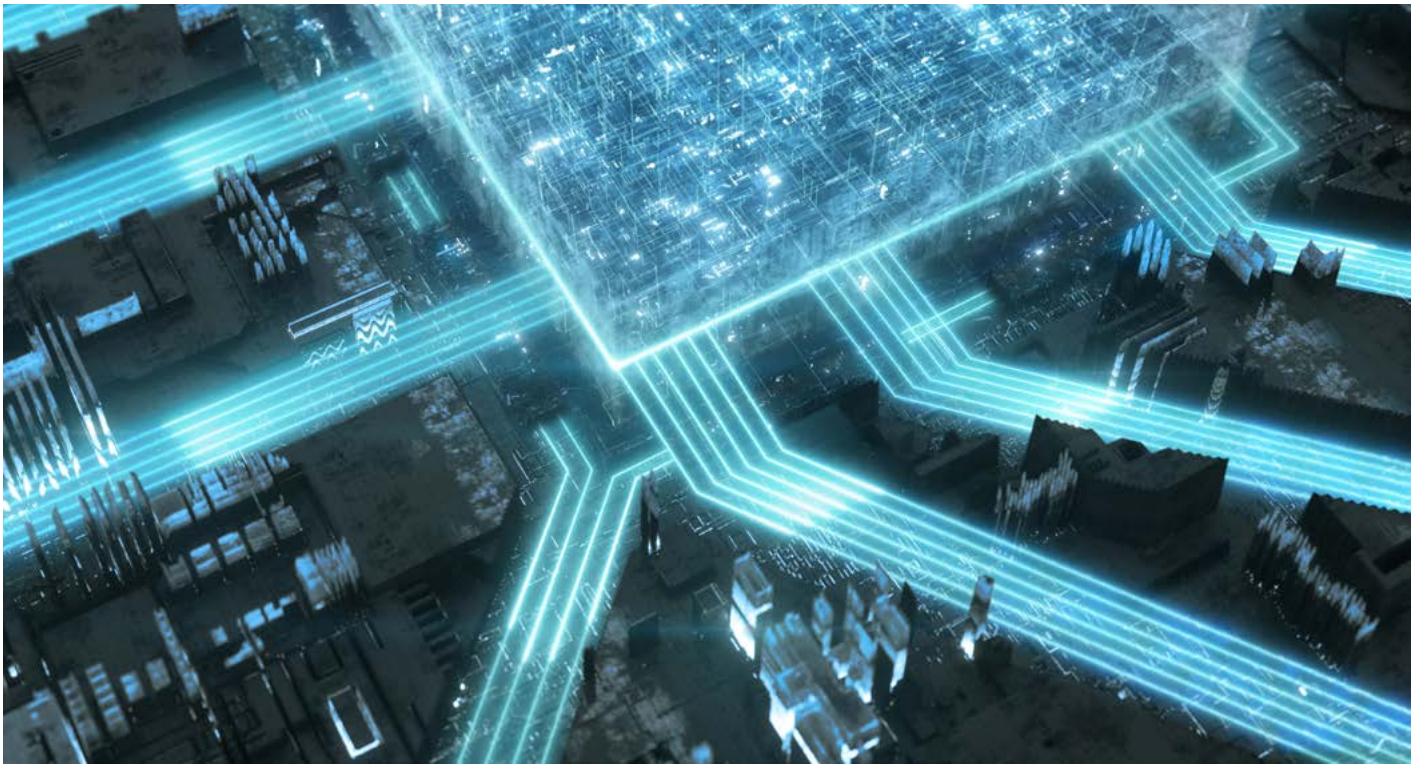
The digitisation of the energy sector is expected to grow rapidly as the 'electrification of energy' in production and consumption increases. The journey of energy from centralised fossil-based heat and electricity production to distributed renewable electricity plays a key role in reducing carbon emissions. This transformation process of energy production is ongoing, and we expect it to only accelerate based on most recent Intergovernmental Panel on Climate Change climate reports stating that more and faster action is needed than was earlier believed. Europe has committed to lead this development globally by substantially cutting its emissions.



Challenge

ESMIG (the European Smart Energy Solution Providers) has called for a new European regulatory framework for IoT, stating that the lack of a truly harmonised approach to IoT poses a critical risk for the deployment of borderless IoT applications and the European industry as a whole. This is because it: (a) increases fragmentation and costs, (b) prevents potential technology providers from taking advantage of the economies of scale that a harmonised environment brings, (c) hampers innovation and (d) decreases the willingness for private sector investment. Furthermore, it can severely impact the future competitiveness of markets that rely on data generated on various digital applications and services[20].

19 https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf
20 https://esmig.eu/news/europe-needs-strategic-and-future-proof



ELECTRONIC COMMUNICATIONS

Opportunity

From now until 2022, the GSMA has forecast that mobile operators could generate €720 billion of economic value in the EU (4.1% of GDP) as the region experiences growth in productivity brought about by continued adoption of IoT technology and the increased digitisation of industry and services across a range of different industry sectors, leveraging industry-wide standards and specifications. Success in the 5G era will rest on the ability of governments to implement regulatory frameworks that encourage sustainable investment and drive innovation[21].

Challenge

The GSMA, the Alliance for Internet of Things Innovation (AIOTI) and Cable Europe have previously highlighted concerns that the sector-specific regulation of telecommunications is fragmented, with the level of service regulation varying considerably across Member States. This is seen as a particular issue for IoT, where products and services are supposed to be provided and consumed across borders. These associations have also highlighted that it is important to ensure that any IoT service, which includes interpersonal communication only as an ancillary feature, should be clearly exempted from the rules related to interpersonal communication services. In the context of the IoT, this may include a service with a communications element which is of very limited functionality and thus not a substitutable communications service[22].

21 https://www.gsmaintelligence.com/research/?file=884c77f3bc0a405b2d5fd356689be340&download
22 https://aioti.eu/wp-content/uploads/2017/05/Joint-Industry-Statement -on-IoT-and-Innovation.pdf

2. Obstacles to the successful development of IoT in the EU

In Section 1, we set out the European market context for IoT development, along with policy insights from the European Commission, BEREC and the OECD. We also described difficulties reported by specific industries which they believe result from the regulatory framework and act as an obstacle to the development and adoption of IoT technologies in their sectors.

In this section we discuss the significant obstacles we have identified to the successful development of IoT in Europe. We provide early evidence that the EU is already falling behind its competitors and relate this to the adverse regulatory environment faced by EU IoT innovators and investors relative to the conditions faced by IoT players in the USA and China.

We consider that this is not the result of an active and rational choice by regulators to ensure better protection of the citizen interest in Europe, contrasted with a more laissez-faire approach in other regions.

It is, rather, the result of a regulatory regime that is ill-designed for the needs of the IoT sector; the burdens we have identified are not those that yield enhanced protection, but those that exist through:

- uncertainty in the application of rules designed for interpersonal communications to M2M interactions;
- additional difficulties resulting from a failure to harmonise the application of rules across the single market; and
- a lack of technological neutrality, so (a) rules differ between cellular and non-cellular applications, even where they operate in the same market and encompass risks that are identical across the two; and (b) industry-specific standards are developing across a number of sectors that 'pick' particular IoT technologies, without consideration of the broader IoT context and the harm that this silo approach entails for the development of IoT across the EU economy.

We have also observed that IoT development is falling behind due to limited adoption of IoT best practices, including the voluntary sharing of non-personal machine-generated data and IoT security measures.

2.1 Studies indicate that the EU is falling behind

Since 2012, Vodafone has been undertaking a global review of the IoT market in conjunction with a market research agency and consultancy in order to better understand how companies in different regions are adopting this technology.

In the 2019 Barometer[23], the core sample consisted of 1,430 qualified respondents involved in shaping their company's IoT strategy, suppliers and technology requirements.

In a supplemental review commissioned by Vodafone in April 2019[24], it was found that the current rate of IoT adoption is lowest in Europe (also reflecting the findings of the 2018 study[25]), observing that IoT had been adopted by 43% of businesses in the Americas and 40% of businesses in APAC, compared to only 23% in Europe. Furthermore, the review also found that Europe is lagging behind the other regions in terms of the sophistication index, which demonstrates the correlation between the scale of implementation and depth of strategy and IoT return on investment.

The review highlighted that removing uncertainty around standards and legislation, and providing clear guidance, is key to encouraging IoT adoption in the EU.

2.2 Legal analysis shows that the EU regulatory regime is too complex compared with other global regions

Vodafone commissioned the global law firm Hogan Lovells to create a benchmarking table to compare the electronic communications regulatory requirements related to IoT across the EU, China and the USA[26].

The study showed that of the 31 categories of ex-ante telecommunications regulatory requirements found in the EU, only 18 are found in China and 12 in the USA. This leads to higher compliance costs and lower legal certainty for IoT players in the EU compared to other major regions.

23 Vodafone IoT Barometer 2019, accessible at https://www.vodafone.com/business/news-and-insights/white-paper/vodafone-iot-barometer-2019

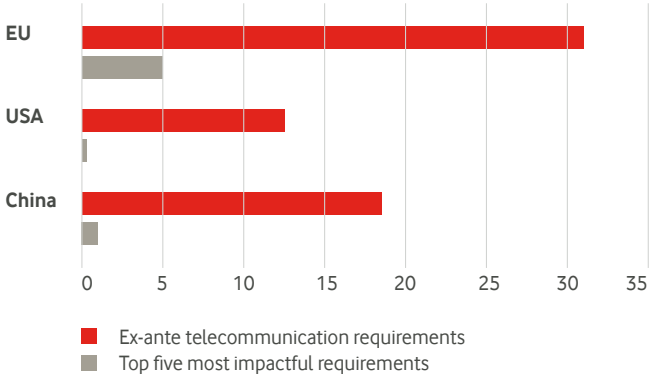
24 'Vodafone IoT Barometer follow-up: the European story' 2019

25 IoT Barometer 2017/18, accessible at https://www.vodafone.com/business/news-and-insights/white-paper/the-iot-barometer-2017-18

26 https://www.hlmediacomms.com/files/2019/03/Hogan-Lovells-A-comparison-of-IoT-regulatory-uncertainty-in-the-EU-China-and-the-United-States-March-2019.pdf

If the most 'impactful'[27] regulatory requirements to the IoT business are selected (absence of single authorisation, numbering, net neutrality, over-the-air (OTA) switching of provider and ePrivacy rules) and compared against the USA and China, then the difference in regulatory uncertainty becomes even more significant.

Figure 3: Comparison of telecom rules relevant to IoT in the EU, China and the USA



Source: Hogan Lovells, March 2019[28]

For example, there is still insufficient certainty that an IoT device that uses non-national numbering resources can be deployed on a harmonised basis across the EU, contrasting with the situation in the USA and China.

2.3 There are considerable regulatory challenges in the EU relevant to IoT

Many regulatory obligations applicable to providers of ECS are designed with interpersonal communications in mind, and their application to M2M services creates needless costs and barriers to pan-European deployment of IoT solutions.

The obligations associated with general authorisations for the provision of ECS (including those related to the use of numbers) as listed in Annex I of the EECC are not obligatory. Member States may impose them, but they are not required to.

The EECC is clear that a service should not be considered as an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing ECS. However, such an approach causes inherent uncertainty in relation to IoT, in particular when a human user is involved.

Being transnational in nature, many IoT services are hit particularly hard by remaining obstacles to the internal market. The market for electronic communications remains less harmonised than a number of other European industries (such as automotive, gas and aviation). As IoT is an essential input for European industry, these sectors are adversely affected in the event of a lack of a harmonised EU approach.

Interpretations on regulation relevant to IoT can vary between Member States, hindering the development of the internal market for IoT services and preventing the emergence of pan-European IoT service offerings and innovation[29].

Obligations relating to the types of regulatory requirements that may be applied to IoT are not harmonised either between different IoT use-cases or different Member States, leading to fragmented regulatory requirements hampering the roll out of pan-European IoT services. For example:

Telephone numbering
National rules on telephone numbers vary across Member States, including limitations on extraterritorial use and limitations or prohibitions on the use of supranational numbers. These rules create barriers to pan-European deployment of IoT, yet serve no purpose in the context of M2M communications.

Number portability
Requirements likewise provide no utility for M2M communications in principle, because the telephone number has no intrinsic value to the user. Yet the non-flexible application of ECS regulation in certain Member States requires IoT connectivity providers to include number portability in the IoT platform, even if it will serve no purpose.

Calling line identification (CLI)
CLI and CLI blocking are also of no relevance for M2M communications, yet a non-flexible application of ECS regulation at a national level may require that IoT solutions incorporate CLI and CLI blocking.

27 The weighted impact of these regulatory requirements on the business is based on Vodafone data and internal analysis only. It takes into account some factors involved in the design and deployment of internal processes that can ensure compliance with the respective regulation(s) (e.g. cost of infrastructure and deployment, hardware and software investments, supply chain and distribution time and costs, time to market and consultancy fees).

28 Comparison of IoT regulatory uncertainty in the EU, China, and the United States. Hogan Lovells, March 2019 available at https://www.hlmediacomms.com/files/2019/03/Hogan-Lovells-A-comparison-of-IoT-regulatory-uncertainty-in-the-EU-China-and-the-United-States-March-2019.pdf

29 See, for example, the initial consultation issued by the Irish Regulator (COMREG) on a new numbering range proposed for M2M/IoT (https://www.comreg.ie/publication/review-mobile-numbering-resources/), which defined M2M in such a way as it was limited to M2M on mobile and fixed networks only.

Law enforcement

Some national laws on data retention have already been criticised by the Court of Justice of the European Union as being disproportionate in the context of interpersonal communications[30]. Their application to M2M communications, for example, to messages sent by a parking meter or a connected waste bin to its central server, appears even more disproportionate without a clear law enforcement justification. This would also be the case for ECS rules relating to the legal interception of communications.

Roaming

The Roaming Regulation is designed to protect EU citizens from excessive pricing and bill shock when they use their communication device while travelling. Most M2M services do not need protection under the Roaming Regulation, either because the connected object does not travel ('permanent roaming'), there is no usage-based charging or because data is transmitted in predictable amounts, such as in the case of engine telematics.

Routing emergency calls

National regulations often impose on providers of ECS the obligation to route emergency calls to the nearest public-safety answering point. While highly desirable for number-based interpersonal communications or in IoT applications designed to enhance human safety (e.g. eCall systems for automobiles), emergency call routing should not be imposed across the board on all IoT applications, particularly M2M services or consumer IoT devices with limited or no human interaction. This is consistent with the EECC's requirement that emergency call routing be imposed only for number-based interpersonal communications.

Notification requirements

The EECC permits, but does not require, Member States to impose notification requirements for the provision of ECS[31]. Under the EECC, "the least onerous authorisation system possible should be used"[32]. Yet declaration requirements for the provision of ECS remain in all Member States, including annual reporting obligations in some cases. In addition to excessive notification requirements, regulatory authorities in different Member States adopt different approaches to which players, if any, in the IoT ecosystem must be declared as ECS providers. IoT services are generally designed to operate on a pan-European level. The obligation to file declarations in 28 Member States, combined with inconsistent national approaches to which each IoT actor must file, create unnecessary regulatory burdens and barriers to the cross-border supply of IoT services.

Switching between providers

In addition to number portability, other mechanisms to facilitate switching may be imposed by Member States on IoT providers, such as the over-the-air (OTA) provisioning of SIM cards. OTA provisioning should be applied on a technology-neutral basis, as recommended in the EECC[33]. Different technologies use different types of identifiers and may have more or less switching capability, and imposing switching mechanisms on only one type of technology would distort competition and innovation on the merits.

Cybersecurity

IoT ecosystems are only as safe as the weakest link in the system. Currently, there is a great heterogeneity in security practices and requirements between different parts of the ecosystem, as well as between different Member States. Different connectivity technologies also have vastly different security characteristics. IoT security should be approached as a coherent whole, with consistent levels of security for each part of the ecosystem based on a risk analysis. Imposing high security requirements on one player in the ecosystem will serve no purpose if other players have low or non-existent security practices, given the security vulnerability that will result from the interconnected nature of the IoT supply chain. The EU's Cybersecurity Act is an opportunity to create coherent cybersecurity certification based on common standards and requirements for IoT applications, devices and connectivity, but greater efforts are required to drive the implementation of such best practices[34] across the IoT supply chain.

30 CJEU, Case no C 203/15, Tele2 Sverige and Watson, 21 December 2016

31 Article 12(3)-(4) EECC

32 Recital 41, EECC: "The least onerous authorisation system possible should be used to allow the provision of electronic communications networks and services in order to stimulate the development of new communications services and pan-European communications networks and services and to allow service providers and consumers to benefit from the economies of scale of the internal market".

33 Recital 249, EECC

34 For example, the GSMA Internet of Things Security Guidelines (https://www.gsma.com/iot/iot-security/iot-security-guidelines/) and the Internet of Things Security Foundation (IoTSF) Best Practice Guidelines (https://www.iotsecurityfoundation.org/best-practice-guidelines/).

3. Areas where urgent change is required

In Section 2, we described the significant regulatory obstacles we have observed that stand in the way of successful development and deployment of IoT in Europe.

Our identification of these obstacles, and our description of the areas where the regulatory framework needs improvement, were derived from an extensive analytical and engagement exercise leading to the completion of this IoT White Paper. This included:

- gathering of qualitative data from vertical industry sectors;
- direct experience deploying IoT in the EU;
- IoT regulatory analysis and benchmarking carried out by global law firm Hogan Lovells;
- Vodafone IoT Barometer findings, including a specific follow-up on the European story;
- Brussels' event bringing together over 100 stakeholders to discuss the challenges facing Europe's future policy approach to IoT;
- analysis on realising the economic potential of machine-generated, non-personal data in the EU35; and
- the mapping analysis of how the ex-ante regulatory regime relating to electronic communications networks and services applies to IoT, looking in particular at where rules are either unclear or inappropriately applied.

In Sections 3.1 and 3.2, we explain how the mapping exercise was developed and the main learnings we identified. We then look more broadly at the parts of the regulatory framework that need to be improved if we are to catch up with the IoT development and adoption we observe in other global regions, most notably in the USA and China.

3.1 Our regulatory mapping exercise has allowed us to identify in detail where existing regulations are being inappropriately applied to IoT applications

Vodafone's mapping exercise was designed to explore in detail how current ECS regulations apply across existing IoT applications. We identified the rules which we believe are reasonable and proportionate and should apply, given the specific risk implied by each IoT (as opposed to interpersonal) communications service. This enabled us to identify where the application of regulations to IoT could be imposing a barrier to development and adoption in the EU and how to address it, either by proposing disapplication or change/adaption to meet the M2M ecosystem needs. In particular, for each IoT use-case, across each industry vertical and mapped onto each EU rule, we were able to identify cases where:

- the application of rules applicable to IoT is ambiguous or unclear, increasing the risk that different Member States will apply them differently in each of their jurisdictions;
- the application of rules applicable to IoT is excessive, leading to burdens that are not explained by the risk posed by the IoT service in question;
- the application of rules applicable to IoT is insufficient, leading to unaddressed risks that could cause harm and could threaten IoT development (if that harm leads to a loss of confidence in IoT); and
- the application of rules applicable to IoT is causing market distortions through uneven application to cellular vs non-cellular technologies[36]:
  - in some cases, there is a need for the rules to be in place to secure a policy outcome, but the rule applies only to cellular applications, thus leaving a gap where the IoT service is provided via non-cellular connectivity; and
  - in other cases, there is not a need for the rules that are in place (or they are not proportionate), so their presence is causing an unnecessary burden on those using cellular IoT technologies, but not on those that make use of non-cellular connectivity.

These market burdens and distortions create significant obstacles to the success of IoT in the EU. As we have set out in Section 2.2, those seeking to develop and deploy IoT in the USA and China typically are not facing these obstacles. Without correcting these identified issues, we are placing the EU at a significant disadvantage relative to our global competitors.

35 Available at https://www.vodafone.com/content/dam/vodafone-images/public-policy/reports/pdf/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf

36 By non-cellular here we refer to Low Power Wide Area private networks deployed in unlicensed spectrum.

Vodafone's study comprised a multi-sector analysis of the deployment of IoT across 12 broad sectors[37] of the economy. These were:

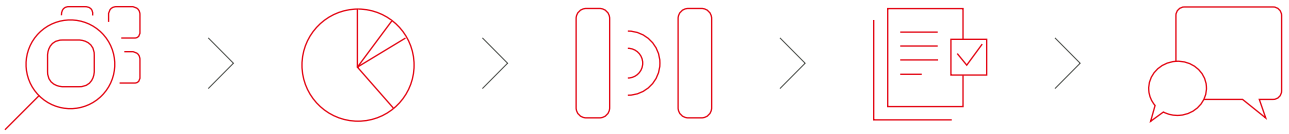
- agriculture and environment;
- automotive;
- construction;
- consumer electronics;
- emergency services and national security;
- healthcare;
- intelligent buildings;
- manufacturing and supply chain;
- retail and leisure;
- smart cities and transport;
- smart enterprise management; and
- utilities.

We carried out separate analysis of 192 specific use-cases of IoT across these sectors (e.g. for the automotive sector, there were 20 different IoT use-cases, and for the consumer electronics sector, there were 35 different IoT use-cases).

We then mapped each of these IoT use-cases against 24 electronic communications regulatory requirements (i.e. those applying to regulated ECS[38]).

Finally, we identified the IoT connectivity enabling technologies used for each use-case, i.e. when the connectivity service for the IoT application is offered via cellular IoT only, via non-cellular IoT only or where the IoT application is deployed using either forms of connectivity. This analysis was used to identify (i) where a particular application was being supplied in competition via both cellular and non-cellular technologies; and, if so, (ii) how regulation applies to each of the technologies.

Figure 4: Analysis underpinning the multi-sector mapping study



We reviewed 12 industry sectors, 192 IoT use-cases.

We mapped 24 regulatory requirements currently in place across those use-cases.

We identified the competing connectivity technologies across all industry sectors.

We case-by-case reviewed how many regulatory requirements are suitable for each of the IoT applications.

We put forward recommendations for a 'designed-for' IoT framework that would address the obstacles that have been identified.

37 The inspiration for this review was the study 'M2M application characteristics and their implications for spectrum' conducted by the consultancies Aegis and Machina Research for the UK regulatory body Ofcom. This study assessed the potential implications for radio spectrum of growing demand for M2M applications and covered 149 distinct M2M applications across 12 market sectors. The sectoral review was further complemented and updated with IoT use-cases from both cellular and non-cellular IoT providers.

38 We have identified and listed regulatory requirements deriving from the EECC (consolidating the Access Directive, Authorisation Directive, Framework Directive and Universal Service Directive), net neutrality, Roaming Regulation and some of the horizontal regulations (ePrivacy Regulation, Cybersecurity Act).

Figure 5 illustrates how the application of rules needs to be adjusted – in each separate use-case and for each particular rule being applied – so that the application of rules matches the risk of harm and prevents unnecessary burdens, continuing risk of harm and loss of confidence in IoT, and distortion through rules being arbitrarily applied to some connectivity technologies and not others.

In summary, Vodafone's approach has been to set out objective criteria that specify rules which are actually needed to protect consumers from harm, or meet some other specified public policy goal, but ensure that rules are not incorrectly applied to IoT use-cases where they are not needed. It does so in a technology-neutral way that applies protection according to risk and does not arbitrarily allow risks to go unaddressed due purely to whether connectivity happens to be provided through cellular or non-cellular means.

3.2 Analysis on the aggregate extent of rules misapplied to IoT

As well as providing specific recommendations for the rules to be applied to the IoT use-cases analysed, our mapping exercise shows the extent to which regulations have been misapplied to IoT.

It should be noted that the percentages and values generated by this analysis are primarily for illustrative purposes, for the following reasons:

- the results are based on our analysis of what the optimal/reasonable application of rules should be for each IoT use-case across the 12 sectors analysed. This approach is open to further discussion; and
- our analysis allows us to analyse 192 IoT use-cases in 12 sectors of the economy, mapping against a total of 24 telecoms regulatory requirements. It should be noted that the list of electronic communication requirements is not exhaustive and not all IoT use-cases are of equal economic or social importance. This means that not all incorrectly applied rules will have the same adverse impact on the development of the particular IoT use. We have not attempted to apply weights to any of these elements when looking at aggregate effect.

While our aggregate observations do not provide a precise measure of the extent to which the application of rules requires change (and which type of change is needed), they nevertheless illustrate that this issue has a significant impact and that different types of changes are needed.

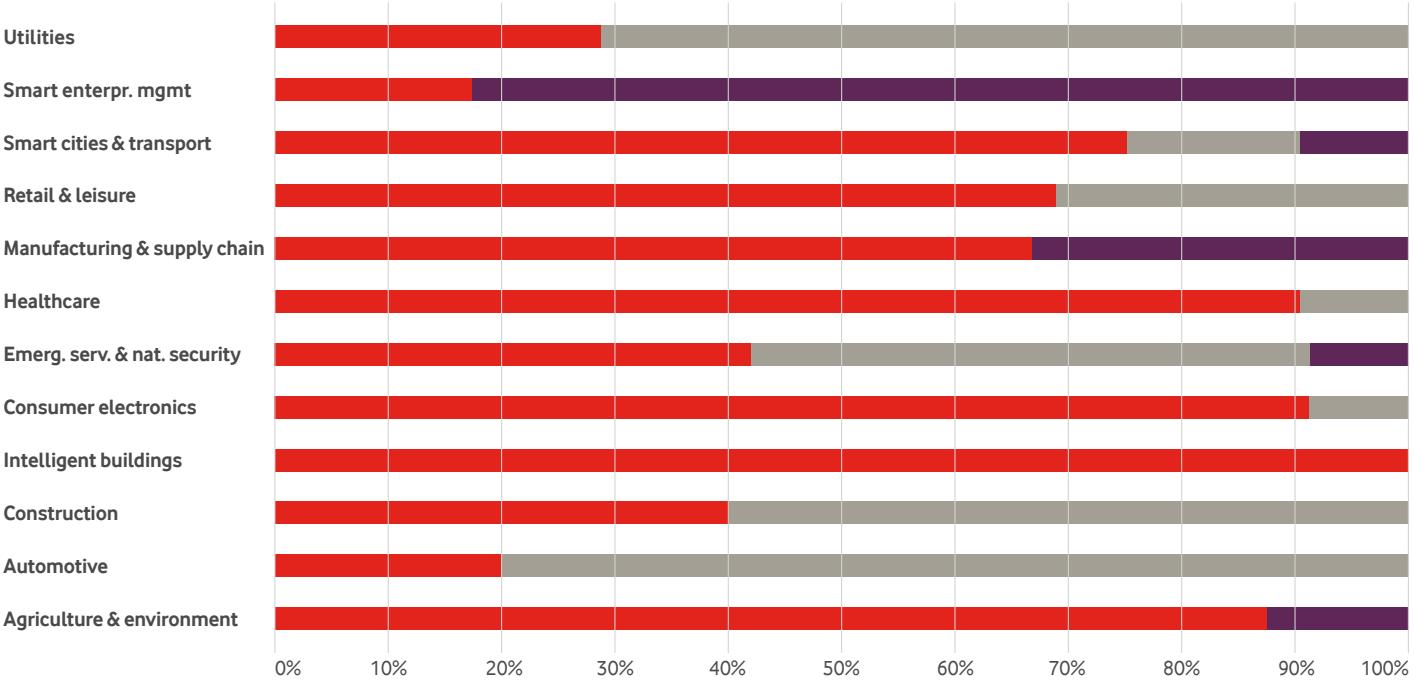
Figure 5: Categorisation of how the application of rules needs to be adjusted to ensure appropriate oversight of IoT use

	Currently no rules in place	Current rules apply only to cellular	Current rules apply to both cellular and non-cellular
Analysis of risk suggests rules are needed	New rules needed	**Need to 'level up'**	No change required
Analysis of risk suggests rules are **not** needed	New change required	**Need to 'level down'**	Need to disapply

Analysis of IoT connectivity technologies

In Figure 6, we show, for each of the 12 sectors analysed, the percentage of IoT use-cases provided via cellular technology, via non-cellular technology[39] or via both forms of technology. The analysis shows that in the majority of sectors, most IoT use-cases can be supplied in parallel using a range of connectivity technologies.

Figure 6: Percentage of IoT use-cases in each sector that are provided through cellular and/or non-cellular technology



Source: Vodafone internal analysis

39 Our analysis indicated that IoT applications in very remote areas (e.g. deep water fishing in the 'agriculture and environment' sector), marked as 'non-cellular only' were connected through satellite connectivity only, which is one of the non-cellular types of connectivity.

However, despite the existence of competing connectivity technologies for IoT, our illustrative analysis suggests that approximately 30% of the requirements analysed apply only to the providers that connect IoT applications via cellular networks using SIM cards and public numbers.

This is an important result. It shows that a non-technology-neutral policy approach for IoT will impact most IoT use-cases and cover the majority of sectors to a greater or lesser degree.

Analysis of IoT regulatory requirements

We then considered the way in which each of the 24 regulatory requirements analysed might currently be applied to each IoT use-case across the 12 sectors analysed. For each use-case in each sector, we considered whether the current application of the rules needs to be modified (and if so, how) to ensure it is fit for purpose. Where we made a judgement that a change in the application of the rules was needed, we categorised the change needed as belonging to one of the following types:

- **rule needs to be disapplied**: There is a rule that seeks to address a risk that is not relevant to the IoT use-case (e.g. device registration for an IoT device with limited voice functionality);
- **rule needs to change**: The way in which a general rule is applied or risks being applied to the IoT use-case needs to change in certain circumstances (e.g. no application of Roaming Regulation to a B2BC IoT use-case where there is no usage-based charge to the end user);
- **rule needs to 'level up'**: There is a rule in place that is needed but is being applied to use-cases that are connected via cellular IoT only. The rule needs to be 'levelled up' to cover all connectivity solutions (e.g. security-related requirements for consumer-facing IoT devices);
- **rule needs to 'level down'**: There is a rule in place that is not needed and is currently being applied to use-cases that are connected via cellular IoT only. The rule needs to be 'levelled down' (e.g. data retention obligation for an agricultural IoT use-case); and
- **rule needs to be applied based on an assessment of IoT functionality**: There is a rule in place. However, its application needs to be modified so that it applies based on the risk of harm relevant to the functionality of the IoT device (e.g. no requirement for data retention in an agricultural IoT device, as opposed to a consumer-facing IoT device).

As is set out on the following pages in further detail, the number of rules whose application needs to be changed (in any of the above forms) is significant, and spans the different types of changes identified.

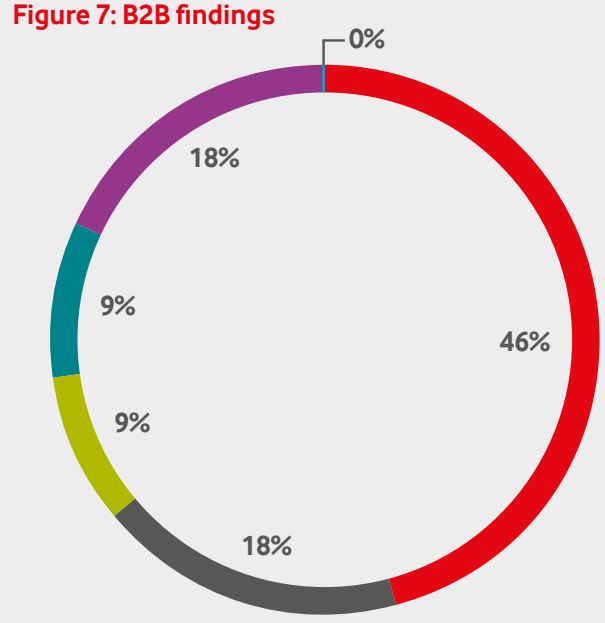
Analysis of whether the IoT use-case is business, consumer or involves both

We then divided the 12 sectors in to two broad groups, depending whether the contractual relationship established between actors involved in the value chain was business-to-business (B2B) only, or involved a consumer (business to consumer (B2C) or business to business to consumer (B2B2C)). This helped us to map the applicable rules to each sector and assess their relevance. For the purpose of this exercise, we considered that if any of the IoT use-cases within a certain sector involved a B2C or B2B2C relationship, then the whole sector would fall under this category. This had the following results:

- **B2B sectors**: Agriculture and environment, construction, manufacturing and supply, smart enterprise management. In the case of B2B IoT applications, 11 regulatory requirements were relevant to the analysis; and
- **B2C and B2B2C sectors**: Automotive, consumer electronics, emergency services and national security, healthcare, intelligent buildings, retail and leisure, smart cities and transport, utilities. For B2C and B2B2C IoT applications, all 24 regulatory requirements were relevant to the analysis.

In the B2B sector, we observed that all the requirements analysed needed to change in some form, as shown in Figure 7 below.

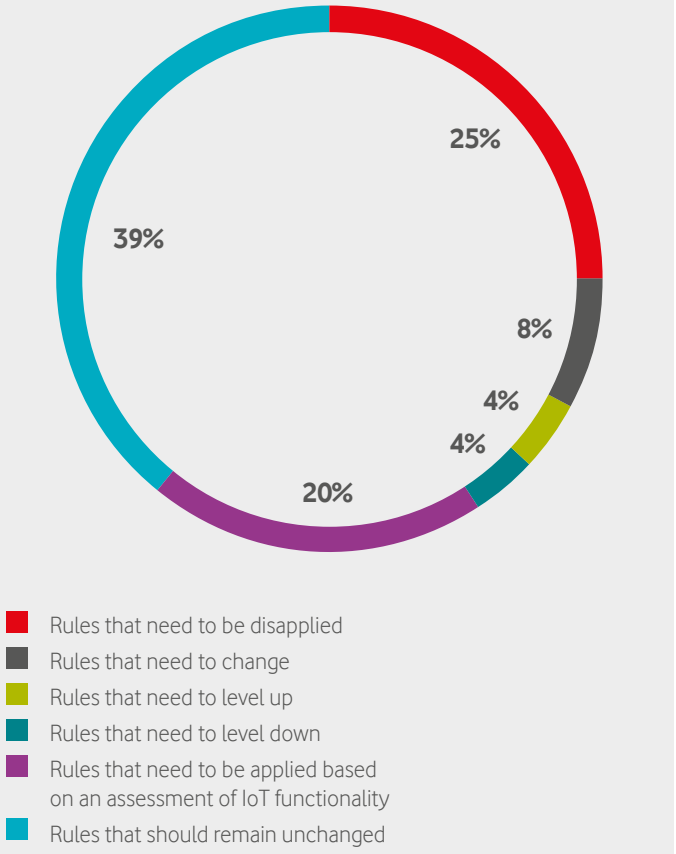
Figure 7: B2B findings



Source: Vodafone internal analysis

For B2C and B2B2C IoT applications, we found that only 39% of the rules should remain unchanged, as shown in Figure 8 below.

Figure 8: B2C and B2B2C findings



Source: Vodafone internal analysis

IoT use-case impact analysis relevant to each of the sectors reviewed

It should be noted the impact of misapplied rules varies considerably across the sectors analysed. For example, we identified 18 different IoT use-cases within the intelligent buildings sector compared to five IoT use-cases in the construction sector. This means that IoT connectivity providers deploying use-cases in the intelligent buildings sector may face higher costs (compared to deployment in the construction sector) where there is an incremental cost associated with compliance with additional rules for each use-case.

Figure 9 provides an illustrative overview of the impact of the abovementioned findings when applied to the totality of IoT use-cases analysed.

Figure 9: IoT use-case impact analysis

	Rules that need to be disapplied	Rules that need to change	Rules that need to level up	Rules that need to level down	Rules that need to be applied based on an assessment of IoT functionality	Rules that need to remain unchanged
Agriculture and environment (8 use-cases)	40	16	8	8	16	0
Automotive (20 use-cases)	120	40	20	20	100	180
Construction (5 use-cases)	25	10	5	5	10	0
Consumer electronics (35 use-cases)	210	70	35	35	175	315
Emergency services and national security (12 use-cases)	72	24	12	12	60	108
Healthcare (20 use-cases)	120	40	20	20	100	180
Intelligent buildings (18 use-cases)	108	36	18	18	90	162
Manufacturing and supply chain (12 use-cases)	60	24	12	12	24	0
Retail and leisure (29 use-cases)	174	58	29	29	145	261
Smart cities and transport (20 use-cases)	120	40	20	20	100	180
Smart enterprise management (6 use-cases)	30	12	6	6	12	0
Utilities (7 use-cases)	42	14	7	7	35	63

Source: Vodafone internal analysis

3.3 We have categorised into four broad areas the basis for a new cross-cutting IoT regulatory framework

Drawing both from the mapping study and the broader analytical and engagement exercise carried out in preparation of this White Paper, we have been able to categorise into four broad areas the changes that are needed to address outstanding issues and promote IoT in the EU. These are detailed in Figure 10, along with evidence of the extent of the problem, where available, and specific case studies of how IoT development could be accelerated were the identified issue to be addressed.

Figure 10: Categorisation of key areas where change to the regulatory framework is required

	Area where change is required	Illustrative evidence of extent	Case study examples of issue
1	Uncertainty over how rules apply to IoT, meaning that rules designed for interpersonal communications are being applied to IoT/M2M applications, thus raising the cost of doing business and introducing delays.	53% of requirements applicable in sectors with consumer-facing IoT applications (e.g. retail and leisure) should either be dissaplied, changed or applied based on an assessment of IoT functionality. Only 39% of applicable requirements for consumer-facing IoT applications make sense and should continue to apply in the future.	Product revision and launch delay: IoT providers face difficulties in launching consumer IoT products which feature limited voice and SMS (e.g. enabling communication between pre-defined closed users or family members) as it is caught by inappropriate ECS requirements. This has caused delay of launch and product features being reduced, including removal of SMS/voice features (e.g. SOS bands, in-home alarms).
2	Fragmented application of rules across Member States, thus hindering the ability to operate seamlessly across the single market.	Vodafone estimates that a requirement to configure national numbering and platform elements would involve a build time of 9–12 months per country.	Providers have encountered delays in rolling out connected devices across the EU (e.g. eight-month delay in Italy for connected cars). Lack of clarity where an IoT-enabled industrial machine will end up when the SIM is installed in the production process means that a fragmented EU approach results in significant business uncertainty. Some machines are also sold via dealers, or installed as an intermediary product in a manufacturing process.
3a	For historic reasons, rather than as a result of an objective analysis of the risk of harm, different rules applied to IoT applications according to whether they are connected via cellular or non-cellular technology, thus distorting investment choices and hindering Europe's ability to keep up with its competitors on IoT innovation and adoption.	Approximately 90% of IoT applications in the consumer electronics sector can be provided by either cellular or non-cellular connectivity; in the intelligent buildings sector, all connectivity technologies compete for all applications, while in the agriculture sector, 90% of applications can be provided from all technologies. Nevertheless, in every industry sector, 30% of the observed regulatory requirements apply only to cellular IoT.	Consumer tracking applications (e.g. for bikes, pets, bags, fitness) and white goods (e.g. smart washers and dryers) can be connected via cellular or non-cellular technology; however, regulatory requirements, such as portability, roaming, OTA switching, CLI, SIM registration, lawful interception and roaming, apply only to cellular IoT.

	Area where change is required	Illustrative evidence of extent	Case study examples of issue
3b	EU industry-specific policies explicitly favouring non-cellular technologies, thus also distorting investment choices and hindering Europe's ability to keep up with its competitors on IoT innovation and adoption.	The 2035 net benefits from 'vehicle to everything' adoption are reduced by €23 billion if car manufacturers are constrained to using non-cellular standards – demonstrating the consequences of mandating connectivity standards that exclude cellular rather than supporting technology-neutral developments[40].	In addition to automotive and Cooperative Intelligent Transport Systems (C-ITS), policy discussions are currently underway at the European level in the agricultural, intelligent buildings and aviation sectors which are likely to have a significant impact on how IoT is to be deployed in each of these sectors.
4	Limited adoption of best practices in relation to IoT, including the voluntary sharing of non-personal machine-generated data, IoT security certification and contractual measures addressing IoT liability.	Sharing non-personal IoT data would realise €1.4 trillion in economic benefits by 2027[41]. Recent research from Consumers International and the Internet Society reveals that 28% of people who do not own a smart device will not buy one due to security concerns[42]. The European Commission Staff Working Document (SWD(2018) 137) on liability for emerging digital technologies highlights a number of issues related to IoT.	Sharing does not yet happen in a material way, although there are examples of sector-specific best practice (e.g. agricultural, automotive)[43]. IoT security measures are still not commonplace across the IoT supply chain, although best practices exist[44]. Potential liability issues in relation to emerging use-cases such as drones or autonomous cars.

40 https://www.analysysmason.com/About-Us/News/Press-releases/socio-economic-benefits-of-c-v2x-study-Dec2017/
41 Cross-reference to Deloitte report referenced at footnote 13.
42 https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/
43 Cross refer to best practices in section 1 – footnote 11 (ACEA) and footnote 19 (Copa-Cogeca).
44 https://www.consumersinternational.org/news-resources/news/releases/consumers-international-launches-trust-by-design-guidelines-for-consumer-iot/

4. Proposal for a new cross-cutting IoT regulatory framework

In Section 3, we set out the results of our detailed analysis into how rules have been applied across a list of existing IoT industry use-cases. This formed part of a broader exercise designed to identify, and categorise, which parts of the regulatory framework need to be modified or clarified to remove barriers to EU IoT development and adoption.

We find significant difficulty in the way rules have been applied across applications, with rules not correctly and proportionately applied according to the risk of harm, with variation by technology not accounted for by differences in risk and with a lack of harmonisation across Member States. This is further exacerbated by technology-specific standards being set in particular industries in a way that frustrates the development of joined-up approaches to the EU's IoT development. We also find that there are IoT best practices not being adopted as broadly as they should.

In this section, we conclude with our vision for a new IoT regulatory framework that will address the regulatory challenges currently faced by those wishing to make a success of IoT in Europe and address the other issues that have been identified. We believe that a Recommendation would provide the clarity needed. If taken forward, we feel optimistic that the European industry would then be in a position to lead the way in the development and adoption of transformational, new IoT technologies.

4.1 Legal basis for introducing a cross-cutting regulatory framework for IoT

In order to consider how the regulatory framework should be modified, we have first examined the legal basis on which any modification would be founded.

Article 173(1) of the Treaty on the Functioning of the EU (TFEU) requires that the Union and the Member States ensure that the conditions necessary for the competitiveness of the Union's industry exist, which include:

- speeding up the adjustment of industry to structural changes;
- encouraging an environment favourable to initiative and to the development of undertakings throughout the Union, particularly small and medium-sized undertakings;
- encouraging an environment favourable to cooperation between undertakings; and
- fostering better exploitation of the industrial potential of policies of innovation, research and technological development.

The innovation principle[45], flexibility and future-proofing[46], and technology neutrality[47] have emerged as key principles to foster innovation, research and technological development in the Union, in furtherance of Article 173(1) TFEU, low compliance costs, regulatory certainty and clarity, and harmonisation contribute to increased research and innovation[48], and increased competitiveness[49], in the Union.

Applying consistent interpretations to EU legislation in a manner that reduces legal uncertainty, compliance costs and barriers to the internal market for IoT will also benefit small and medium-sized enterprises, which are major drivers for IoT innovation in the Union.

Where the Commission finds that divergences in the implementation by the national regulatory or other competent authorities of the regulatory tasks specified in the EECC could create a barrier to the internal market, Article 38(1) of the EECC calls on the Commission to adopt, as necessary, having taken utmost account of the opinion of BEREC, recommendations in relation to the harmonised application of the provisions of the regulatory framework.

The introduction of a Recommendation for IoT will provide regulatory certainty for Member State national regulatory authorities responsible for the development and enforcement of electronic communications regulation, as well as policymakers in industry-specific markets who are developing regulation which may impact the digitisation of that industry sector.

45 Conclusions of the Competitiveness Council of 26 May 2016 (point 2), http://www.consilium.europa.eu/register/en/content/out/?&typ=ENTRY&i=ADV&DOC_ID=ST-9580-2016-INIT; Towards an Innovation Principle Endorsed by Better Regulation, EPSC Strategic Note, Issue 14, 30 June 2016

46 Future Proof Legislation, EESC Opinion, 2016

47 Article 3(4)(c), EECC

48 European Commission Better Regulation Toolbox, Tool #21, Research & Innovation, pp149-150

49 European Commission Better Regulation Toolbox, Tool #20, Sectoral Competitiveness, p138

4.2 Proposed new IoT Recommendation

A new, designed-for IoT framework, would be consistent with the following principles **(the 'IoT Principles')**, consistent with the EU Treaty and applied in the manner also set out below.

1 TO ADDRESS UNCERTAINTY OVER HOW RULES APPLY TO IoT

Proportionality

Regulatory burdens on IoT players should be reduced or eliminated in situations where those burdens are not strictly necessary to achieve the underlying policy objective that the regulatory measure was originally designed to address; where there is a choice among several appropriate measures, the least onerous measure must be used.

- To ensure a proportionate approach, in applying the IoT Principles, given the provisions of the EECC related to 'ancillary features', Member States will take full account of the need to ensure that any regulatory requirements apply based on the service functionalities of the IoT application in question. Annex 1 sets out a practical guidance for such an approach, based on an analysis of whether the IoT application is one that involves 'Closed Data' and/or 'Open Data' and/or 'Closed Voice' and/or 'Open Voice'. Where this forms the basis of any part of a new Recommendation, it could provide a checklist for national regulatory authorities when seeking to understand how to apply the EECC consistently to IoT services.
- Regulatory bodies should allow efficient network management for IoT services and encourage the development of innovative services with specific quality needs. An operator should be allowed to dynamically share resources across network slices in the most efficient way, to ensure the best possible quality for end users.
- Connectivity providers should be allowed to process communications metadata to the extent necessary to provide the agreed service. This includes processing for billing and customer relationship management, ensuring the security of the service, the prevention and investigation of fraud, and service development, as well as for creating aggregated, statistical information derived from communications metadata.

  Consent should not be the only means to allow further processing of communications data. In the case of natural persons, consent is an acceptable approach, while for legal persons, contractual agreements should be used.

2 TO ADDRESS FRAGMENTED APPLICATION OF RULES ACROSS MEMBER STATES

- **Harmonisation**

  The interpretation and application of EU legislation to IoT services should be consistent with the approach applied by other Member States in order to avoid fragmentation of the internal market and high compliance costs for IoT providers and users.
- **Cross-border supply**

  The interpretation and application of EU legislation should encourage cross-border supply of IoT services and the emergence of pan-European IoT solutions, and any limitations on the right to cross-border supply must be objectively justified and proportionate and should not exceed those necessary to achieve the relevant objectives.
- To facilitate harmonisation and cross-border supply, BEREC should create a single authorisation regime for IoT using supranational numbers assigned by the International Telecommunication Union. This authorisation should enable service provision consistent with **Annex 1**. Where a provider is authorised to provide IoT in one Member State using such a supranational numbering range, it can deploy across the EU.

3 TO ADDRESS CONCERNS ABOUT LACK OF TECHNOLOGICAL NEUTRALITY

- **Undistorted competition**
  Regulation should foster a level playing field between national IoT actors and those located in other Member States, as well as between IoT actors using different technological solutions. The requirements in **Annex 1** should be applied in a consistent way across different IoT technologies.
- **Technology neutrality**
  Regulatory obligations should apply equally, without regard to the underlying technology used, and avoid favouring or penalising one particular technology solution or technique.
- To ensure undistorted competition and a technology-neutral approach, sector-specific regulatory bodies should develop regulation in that sector that impacts digital services in a technology-neutral manner.
- Such sector-specific policy and regulatory initiatives affecting IoT connectivity should first be communicated by Member States to BEREC for its view on their compatibility with technology neutrality and the innovation principle.
- **Appropriate security**
  Appropriate security obligations relevant to the risk should be applicable EU-wide and across the entire IoT value chain, taking into account the state of the art and the level of risk throughout the product lifecycle.

4 TO ADDRESS CONCERNS ABOUT THE LIMITED ADOPTION OF BEST PRACTICES IN RELATION TO IoT AND PROMOTE EUROPEAN COMPETITIVENESS AND END-USER TRUST

- To promote end-user trust, participants in the IoT value chain should adhere to recognised IoT security best practices and contractually require their trading partners to do the same.
- **Innovation and future-proofing**
  The interpretation and application of EU legislation to IoT services should facilitate EU-based innovation, including through the use of regulatory flexibility, and experimentation.
- To promote innovation, participants in the IoT value chain should reasonably endeavour to share non-personal, machine-generated data on a fair, reasonable and non-discriminatory (FRND) basis, taking full account of any related security, privacy, competition law or confidentiality consideration.
- To address potential issues around liability, participants in the IoT value chain should ensure contractual arrangements between them are clear in relation to which party is responsible in the event that an IoT-enabled product causes damage.

Annex 1: Analysis of IoT functionality and corresponding regulatory requirements

	Source regulation	Rationale for requirement	Specific rule	Analysis of IoT functionality and corresponding regulatory requirements								
				Data			Voice			Messaging		
				Closed data	Walled garden	Open internet access	Closed User Group (1 to 1)	Closed User Group (1 to 2-5)	Open User Group (1 to any)	Closed User Group (1 to 1)	Closed User Group (1 to 2-5)	Open User Group (1 to any)
1	EECC	Identifiers	CLI			✓			✓			✓
2		Change of provider	Number portability						✓			✓
3			OTA switching			✓*			✓*			✓*
4		Emergency call/disaster response	Emergency communications					✓	✓			
5			Availability of service					✓	✓			
6		Consumer information remedies	Contract requirements			✓		✓	✓			✓
7			Transparency and publication of information			✓		✓	✓			✓
8			Quality of service			✓		✓	✓			✓
9			Operator assistance, directory enquiry services (DQ)					✓	✓			
10		Consumer protection	Out-of-court dispute resolution			✓		✓	✓			✓
11			Special measures for end-users with disabilities			✓		✓	✓			
12			Selective barring for outgoing calls or premium SMS or MMS									✓
13		Consumer charging	Cost control			✓		✓	✓			✓
14			Billing accuracy			✓		✓	✓			✓
15			Non-payment of bills			✓		✓	✓			✓
16			Itemised billing					✓	✓			✓
17		Consumer access to numbers and services							✓			
18	Law enforcement	Security	Data retention		✓	✓		✓	✓		✓	✓
19			Lawful interception			✓			✓			
20			Device registration									
21	Other regulation relevant to ECS/ECN	Roaming	Price caps, transparency	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*
22		Net neutrality	Prioritisation									
23			Sub-internet offers									
24		ePrivacy		✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*

✓ Rules should apply ✓* Rules should apply with certain IoT-specific conditions

Elaboration on conditions to be applied

OTA switching

The customer (enterprise and/or hardware manufacturer) should be able to choose the preferred functionality (between non-OTA or OTA) – where requested, it should be provided.

Roaming regulation

Roaming regulation should apply to all IoT applications which connect through public networks and meet the following criteria: (a) IoT application offers access to open internet, (b) where the device is moving between Member States and (c) there is a risk of usage-based charge to the end user.

ePrivacy

Tailored rules should apply for the different roles that different parties play in the IoT value chain (e.g. connectivity provider, hardware provider, service provider) and the various relationships in which IoT devices and services are sold (e.g. B2C, B2B, B2B2C, B2B2E (employee)).

Connectivity providers should be allowed to process communications metadata to the extent necessary to provide the agreed service. This includes processing for billing and customer relationship management, ensuring the security of the service, the prevention and investigation of fraud, service development, as well as for performing required analytics to create aggregated, statistical information derived from communications data.

To the extent IoT communications data would be used by the Connectivity provider to provide Value Added Services based on further processing of the said data, this must be agreed with the recipient of the connectivity service.

Consent should not be the only means to allow further processing of communications data. In the case of a natural person, consent is an acceptable approach, while for legal persons, contractual agreements should be used.

Definitions relevant to IoT functionality

Closed data – IP end-points are technically restricted as part of the service.

Walled garden – the user is given access to specific content or functionality in an online environment. Although not a technical restriction, in effect, this does not include the open internet.

Open Internet Access – there are no restrictions, technical or otherwise, on the service.

Closed User Group – a Closed User Group communication is a communication which is restricted to a single user or a pre-defined group of users (consistent with ETSI standard ETS 300 136). In our approach, we propose a ceiling to the number of pre-defined users that can form part of the Closed User Group (five users). Beyond this ceiling, the service would not qualify as a Closed User Group. This approach is open to further discussion.

Open User Group – the user is able to communicate with any third party of their choosing.

Registered Office:
Vodafone House
The Connection
Newbury
Berkshire
RG14 2FN

Registered in England No. 1833679
Telephone: +44 (0)1635 33251