

Regulating the IoT: 2020s and beyond

The Internet of Things (IoT) is the interconnection of physical devices — including ones taking input from humans — through a mobile or satellite network, or over the Internet. Although it has been around for nearly two decades, the Internet of Things (IoT) is still one of the trendiest acronyms in the world of tech and has unsurprisingly attracted the attention of regulators worldwide in recent years. The widespread deployment of IoT devices revealed the need for a more specific regulatory framework to address associated concerns; specifically, which regulations apply to the IoT value chain, the availability of scarce resources (frequencies and numbers), privacy and security.

This paper aims to dissect IoT by addressing the ensuing regulatory challenges.

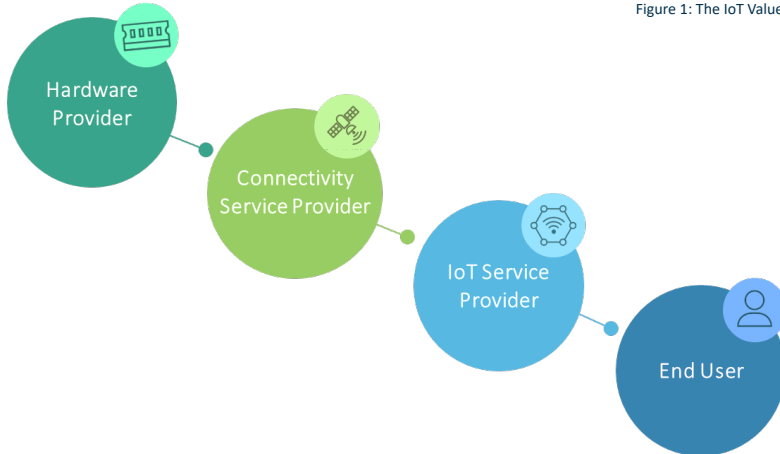
Regulating the IoT Ecosystem

The IoT ecosystem differs from the traditional telecommunications ecosystem, in that it involves a number of incumbent players, including the connectivity service provider (typically a mobile or satellite operator), device manufacturers, platform providers and IoT service providers. Given the complex IoT value chain, which of the respective services can be described as a telecommunications service and should be regulated under the telecommunication's regulatory framework?

The first issue to consider is whether the same telecommunications regulatory framework can apply to some IoT applications, where communication can be restricted to machine-to-machine (M2M), with limited or no interaction with end-users at all. Most telecommunications regulatory frameworks clarify this ambiguity and define

telecommunications services as the act of communication between “things and things”.¹ Ultimately, if the use of an IoT sensor includes the transmission of signals or data, even without the involvement of a human, it is most likely to be considered a telecommunications service.

Figure 1: The IoT Value Chain



Referring to the question of what IoT services in the value chain fall under the scope of telecommunications services and those that should be regulated; services in the IoT value chain depend, ultimately, on the connectivity provider – offering the wireless connectivity underlying the IoT network – that is responsible for the conveyance of signals to the end-users. In most cases, the connectivity provider will be considered a telecommunications provider, subject to a series of obligations. However, the connectivity itself accounts for a relatively low proportion of the overall revenue in the value chain and a closer look may produce a different conclusion: in the IoT ecosystem, the main service provided is not the connectivity, but the applications and related devices and sensors.

The applicability of the telecommunications framework beyond connectivity service providers is much less definitive. IoT providers, such as connected-car manufacturers or integrators of IoT smart farming applications, are – in principle – not responsible for the conveyance of connectivity and barely fall under the definition of telecommunications service providers. Instead, they create a distinct and integrated IoT service for their customers and are ultimately responsible for the quality of the IoT service provided. This fact has led several regulatory authorities to regulate IoT service providers as resellers of telecommunications services, or to simply apply specific telecommunications rules to them (e.g. in UAE a registration procedure is applicable rather than a telecommunication

¹ For instance see definition of “electronic communications service” in Article 2(4)c of the Directive (EU) 2018/1972 establishing the European Electronic Communications Code.

license).

Stakeholders within the IoT value chain must be aware of the applicable regulatory framework — if their role is considered a telecommunications service provider, they will be subject to obligations including licensing requirements, regulatory fees or consumer protection obligations, and risk facing penalties for non-compliance.

The IoT Enablers: Connectivity and Identifiers

Spectrum and Connectivity

Spectrum is one of the key enablers of the IoT and as the connections between (virtual and physical) things are mostly wireless; the amount of available spectrum will have to be increased to accommodate the resulting traffic between connected devices.

IoT is not limited to any specific technology and is likely to use frequency allocations across the entire spectrum, using either terrestrial or satellite connectivity. There is no single solution for spectrum access that fits all possible use cases since their technical requirements differ dramatically, for example regarding data rate, reliability, range and output power of the IoT devices. Currently, the majority of IoT services are being delivered within the existing frequency allocation regulatory framework. However, in some cases, enabling IoT connectivity may require changes to the framework.

The purpose of this paper is not to present the frequencies allocated to IoT connectivity or those that should be, but rather to highlight certain challenges that IoT connectivity providers may face when considering entering the market. Access to spectrum for IoT applications can also be done under the “General Authorization Regime” that permits the operation of radio devices and stations that are compliant with specific technical characteristics to avoid harmful interference, without a frequency license. This concerns mostly lowpower devices that can tolerate signal latency and do not require protection against interference. Typically, devices operating under the general authorization regime, will not require a frequency license, but will still need to be type approved. In some jurisdictions, a network (blanket) license, covering the use of several devices or stations, may still be applicable.

If no licensing exemption applies, the IoT connectivity provider will need to obtain a frequency license. In this case, the connectivity provider should consider the licensing and fees regulatory framework since the difficulty of market access depends on whether a blanket license or an individual license is applicable. This is particularly relevant for satellite IoT applications, where frequency use fees may depend on the number of earth stations deployed and are not based on the overall bandwidth used. This spectrum

fee structure has been established in many regulatory frameworks, having in mind the deployment of larger earth stations or gateways, and can be problematic when it comes to the deployment of over 100 small IoT devices within a specific jurisdiction. A less stringent framework may apply to VSAT stations, although at present in most jurisdictions, there is no similar approach applied to small IoT modules communicating with the satellite, resulting in a legal lacuna of applicable regulatory fees. IoT connectivity providers should engage with the regulator to ascertain the applicability of blanket licensing frameworks where a frequency license is required for the operation of IoT devices.

Identifiers and Numbering

Although only some IoT devices require telephone numbers or IP addresses as identifiers, many countries hesitate to assign identifiers to IoT devices as they are treated as a scarce resource. Since the growth of IoT devices is expected to increase, there are concerns regarding adequacy of numbering resources and IP addresses. However, we do not foresee this becoming an issue any time soon, by which point, regulators may have found a solution through a dedicated IoT/M2M numbering/address range, or by increasing resources dedicated to existing ranges. This paper focuses instead on the extraterritorial use of numbering resources, the use of eSIMs and the restriction of permanent roaming. All these issues relate to the mobility of the IoT devices and the necessity to support the circulation and portability of connected devices from one country to another and from one network to another.

The extraterritorial use of E.164 and E.212 of national numbering ranges for M2M services is not globally harmonised and some jurisdictions restrict the extraterritorial use of numbers. Additionally, roaming regulations may limit the extraterritorial use of numbers. Cellular connectivity is reliant on IoT services which use permanent roaming for IoT devices outside their country of production, while the SIM originates from the production country. For example, e-cars use SIMs stemming from their country of production, although the e-cars are used worldwide. However, there is no uniform approach to permanent roaming. This is problematic as restrictions on permanent roaming in one country can inhibit the use of data internationally and present challenges to global device deployment. Concerns about competition are behind the regulatory inconsistencies as roaming operators can leverage permanent roaming to gain a competitive advantage over national operators. The Body of European Regulators, BEREC, believes that permanent roaming for IoT connectivity should not be discarded. Brazil, on the other hand, observes that permanent roaming could lead to unbalanced competition as the roaming operator would provide full-scale telecommunications services in the country without a license and without paying local taxes.

Additionally, IoT devices are widely deployed, making it impractical to change SIM cards when switching mobile operators. The SIM card has evolved, however, into the embedded SIM (“eSIM”), offering the ability to change service providers over-the-air (OTA) without physically changing the card. More commercial uses for eSIM services will increase in 2020 – along with its regulation. Turkey has already introduced a limited legal framework where operators and device manufacturers can market eSIMs. The UAE also permits the use of eSIMs with prior approval from the telecommunications regulator.

Securing the IoT Ecosystem: Security and Privacy Considerations

Security

The security of the IoT network depends on its availability, authenticity, integrity, confidentiality, the services provided through the network, and the data stored or transmitted by it. IoT network security is at the forefront of regulatory concerns as cyberattacks on IoT devices have grown at an unprecedented rate in the last year. IoT is a global network infrastructure, connecting physical and virtual objects, with a high degree of autonomy and interoperability. As its ecosystem is only as safe as the weakest link in the system, the risks to infrastructure – such as electrical grids – are a major cybersecurity concern.

The first issue is to identify who is responsible for securing IoT devices/networks and subsequently liable if there is a security breach. Current self-regulatory regimes are gradually being replaced by governments imposing security implementation requirements on device manufacturers, with some due diligence responsibilities falling on IoT providers.

Security of IoT communications equipment may also be related to the type-approval of equipment. For instance, the Emirati regulator, the TRA, has included security by design as a key requirement for type approval of IoT communication equipment and the Dutch Spectrum Regulator is proposing a set minimum digital security requirements for IoT products by potentially reviewing the Radio Equipment Directive (RED).

Current legislative actions tend to focus on consumer IoT devices, but recent legislative initiatives also concern government IoT, smart cities and critical infrastructures. In the EU eHealth sector, connected medical devices manufacturers will need to comply with EU Medical Device Regulations effective in May 2020,² while in the US, the connected medical devices framework is still voluntary under the FDA’s guidelines. However, the US may soon follow the EU approach considering the trade implications of US-produced

² Implementation deadline will be however pushed forward due to COVID-19.

medical equipment to be imported to the EU.

Critical infrastructure security has been at the centre of regulatory focus in recent years and the use of IoT by critical infrastructure providers (e.g. electricity providers, transportation, or health providers) may represent many benefits but pose significant risks for the security of the related networks. Therefore, while specific cybersecurity requirements fall only on operators of critical infrastructure, they should ensure the IoT providers and devices used are compliant with the cybersecurity rules. In practice, and to ensure compliance with the EU Networks and Information Security (NIS) regulatory framework, critical infrastructure operators generally engage in due diligence when using IoT applications and use specific security compliance clauses in their contracts with the IoT providers.

Lastly, telecommunications service providers in the IoT value chain providing services in the EU should also consider the cybersecurity requirements under the telecommunication regulatory framework. More specifically, they will need to ensure an adequate level of privacy and confidentiality while processing personal data based on the ePrivacy Directive. Furthermore, they must ensure compliance with the recently adopted European Electronic Communications Code,³ which established a security baseline to communications service providers intended to prevent and minimize the impact of security incidents. For more information on EU Cybersecurity rules, see the Impact of Cybersecurity Regulations on ICT Companies in the European Union.

Privacy

Privacy protection challenges arise with regards to IoT due to the potential of the technology to generate and collect an extensive amount of data, especially when the data is considered personally identifiable information (personal data). Currently, there are no specific data protection rules applicable to IoT applications, although the US Federal Trade Commission (FTC) has identified the risks of lack of IoT privacy standards, and the General Data Protection Regulation (GDPR) specifies that stringent rules should apply for IoT device privacy. The EU's Article 29 Working Party (WP29) issued an opinion on IoT – long before the implementation of the GDPR, recognising the vulnerability of the IoT devices. IoT specific privacy standards, data protection codes of conduct and certification schemes will likely be adopted shortly and focus on the accessibility, privacy by default of the IoT devices, and effective consent mechanisms. It should be noted that the data protection requirements extend to all players of the value chain involved with the processing of personal data. Special consideration should be given by the manufacturers of IoT devices that must comply with the principle of "Privacy by Design", meaning that they must assess a product's potential privacy risks during the product development and

³ Article 40 of the Directive 2018/1972.

manufacturing phase.

IoT providers should also be aware of data localisation rules when deciding to expand their services across jurisdictions. Data localisation rules require data concerning citizens or residents to be stored, collected, and processed within the jurisdiction of the data subject or where data are collected. This requirement relates to privacy and data security concerns but also law enforcement access to data concerns. Data localisation restrictions are important for IoT devices since their function depends on the data they collect, the possibility to transfer the data and storage in cloud applications in data centres across the world.

In the EU, while the free flow of data without obstacles within the Union is supported by removing unjustified restrictions to the location of data, restrictions on cross-border data transfers exist through data protection rules. Recent EU initiatives aimed at ensuring data sovereignty may, however, impede the free flow of IoT data across the European continent. Although data sovereignty could be solved by data centres in Europe, there is a significant dependency on non-European cloud infrastructure, and data is also handled by non-European service providers.

Outside of the EU, data localisation requirements have been imposed, for instance, by the UAE and the KSA concerning IoT devices. In the UAE, some sensitive data collected by IoT devices should be stored in the country. In the KSA, a new framework has been proposed to require all servers, network components and devices used to provide IoT services, as well as all data, to be kept within the KSA.

IoT Investment Needs Regulatory Reform


IoT entails important regulatory and legal issues – open questions and regulatory gaps still exist after more than a decade since IoT devices and applications have come to market. Recently, IoT has been deployed and used for more innovative applications, across a variety of sectors and has attracted regulatory attention. While there are restrictions to IoT, many countries want to encourage IoT innovation and reform their regulatory framework to ensure they do not inhibit its growth. However, regulations are implemented at a much slower pace than the deployment of the IoT technology, provoking uncertainty among providers of these services. This can also foster mistrust from end-users with regards to the security and privacy aspects of IoT devices and use. Updated regulations are necessary for the optimal deployment of IoT technology as investors will be less reluctant to support new IoT applications. Additionally, a harmonisation of rules across the globe is crucial, considering mobility is the main characteristic of IoT devices. IoT players should follow the development of regulations surrounding the Cloud, Big Data, and 5G, given their strong correlation with IoT development.



We lead countries to fair tech

Access Partnership is the world's leading public policy firm that provides market access for technology. Our team uniquely mixes policy and technical expertise to optimise outcomes for companies operating at the intersection of technology, data and connectivity.

9th Floor, Southside
105 Victoria Street
London SW1E 6QT
United Kingdom
Tel: +44 (0) 20 3143 4900
Fax: +44 (0) 20 8748 8572
Email: compliance@accesspartnership.com

 AccessAlerts
 AccessPartnership

www.accesspartnership.com