IoT: Seven areas for regulators and policy makers to consider

October 2016

Tom Rebbeck

The potential for IoT to have a positive economic, societal, and environmental impact worldwide is substantial, but its development also raises new questions to be addressed by regulators and policy makers. The need to protect consumers, and to help them understand how their data is being used, must be balanced against the need to ensure that the potential of the IoT market is not stifled.

Governments are not neutral actors in IoT

Governments are active participants, as well as rule makers, for IoT, with government policy driving some of the largest IoT projects worldwide. For example, the European Union is aiming for 80% of electricity meters to be smart meters by 2020, and in the USA, Recovery Act funding supported smart grid initiatives. Governments are also supporting the deployment of vehicle accident alert systems (such as the European Commission's initiative, eCall), and providing funding for smart cities and more general IoT innovation.[1]

Governments need to be wary of the potentially negative consequences of their involvement. For example, one operator suspended its plan to build a large-scale LPWA network after the national government suggested that it would instead fund a similar system to support smart city services. However, after 18 months with no development of the promised government network, the country in question still has no LPWA connectivity

Seven key areas of interest for regulators

We have identified seven key areas of interest for regulators reviewing IoT (see ***Figure 1***).

Figure 1: Key issues in IoT regulation [Source: Analysys Mason, 2016]

Issue	Regulatory and policy considerations
Device and service security	• New rules may impact multiple regulators (for example, healthcare devices may require involvement from telecoms and healthcare regulators). • Few countries will have the clout to mandate security standards alone.
Data privacy and ownership	• Issues around data ownership could involve device manufacturers, application providers, and network operators, and affect multiple regulatory bodies.
Network security and resilience	• New services (such as healthcare and energy) may require increased levels of security and resilience. • Multiple government bodies beyond communications regulators may be involved in regulation.
Data sovereignty and residence	• Governments considering restrictions on the transfer of IoT data will need to balance the benefits against potential consequences. IoT organisations may choose not to launch a service if rules appear too restrictive, or require substantial local investment.

[1] For example, the UK government has committed GBP40 million to projects such as IoTUK, a national programme that supports the development and adoption of IoT in the UK.

© Analysys Mason Limited 2015

Issue	Regulatory and policy considerations
Allocation of scarce resources (including spectrum and numbering).	• Most IoT applications will be low bandwidth and will not require additional network capacity.[2] • Some applications (for instance, healthcare) may benefit from dedicated spectrum, such as that proposed for 2 x 3Mhz in the 700MHz band, to support higher quality-of-service levels. • Regulators may also need to clarify rules about existing spectrum usage.[3] • A number of countries, including the Netherlands, Norway and Spain, have released new number ranges for M2M services. • When addressing the allocation of resources, governments can encourage the use of IPv6 by encouraging its use by the public sector, as Belgium has done.
Roaming and network switching	• Many (if not most) IoT companies would prefer flexibility when it comes to which option to use for connected services worldwide (for example, a choice between using a local physical SIM, a global roaming SIM or an eSIM). • Rules surrounding eSIMs and permanent roaming are often unclear, creating avoidable uncertainty.
IoT standards	• The absence of globally accepted IoT standards is a barrier that may be delaying IoT deployment. • Regulators and governments should consider how they can support the development of standards.[4]

Policy makers need to consider existing rules when exploring IoT regulation

We believe that four broad factors should be considered when reviewing regulation and policy for IoT:

- Although IoT development raises some new concerns, many issues will already be covered by existing regulation, making new rules unnecessary. For example, privacy concerns have been raised about drones that can take videos or photographs, with some attempts to ban drone photography.[5] Most countries already have legislation on photography, which means that additional rules are not needed.
- Current and planned regulation may be too stringent for IoT, and could threaten innovation. The need to relax existing rules has been recognised in both Japan and Korea.
- IoT requires regulatory certainty due to the long-term nature of investments. A 15-year lifetime for an IoT device will not be uncommon. For such commitments, the firms involved will want to have confidence in the regulation. For example, the rules governing permanent roaming[6] are unclear in many countries and this may dissuade IoT companies from using it.

2 Analysys Mason forecasts that IoT devices will represent 3% of total global cellular traffic in 2020. See Analysys Mason's *Wireless network data traffic: worldwide trends and forecasts 2015–2020*. Available at: www.analysysmason.com/Research/Content/Reports/Wireless-Network-Traffic-Jan2016-RDTN0.

3 For example, in March 2016, Ofcom clarified that certain VHF bands could be used for IoT applications. See article: Ofcom (London, UK, 23 March 2016), *VHF radio spectrum for the Internet of Things*. Available at: http://stakeholders.ofcom.org.uk/binaries/consultations/radio-spectrum-internet-of-things/statement/vhf-iot-statement.pdf.

4 RAND Europe recently published its report *Accelerating the Internet of Things in the UK*, which explores some of these topics. Available at: https://www.rand.org/randeurope/research/projects/accelerating-internet-of-things-uk.html.

5 In 2013, US state of New Hampshire's government unsuccessfully attempted to introduce a bill to ban "images of a person's residence to be taken from the air." Available at: http://www.modelaircraft.org/gov/statebills/NHHB619.pdf

6 Permanent roaming is where a SIM from one country is installed permanently in a device that originates in another country. For example, in Ireland, the lottery terminals use SIM cards from Telefónica Spain.

© Analysys Mason Limited 2016

- Finally, IoT is a global business, which limits the impact that any single national government can have over many aspects, including IoT standards. While it may not be desirable or possible for governments to decide upon standards, they do have influence.[7]

Analysys Mason has over 30 years of experience supporting telecoms regulators and policy makers, and in recent years has supported several organisations on the topics discussed above. If you would like to hear more about how we can assist you, please contact Tom Rebbeck, Research Director, Enterprise and IoT tom.rebbeck@analysysmason.com or James Allen, Partner and senior regulatory expert, james.allen@analysysmason.com.

7 In the UK, the government is providing support, including funding, for the development of the Hypercat standard.

© Analysys Mason Limited 2016