# The Hashemite Kingdom of Jordan Telecommunications Regulatory Commission

# Green Paper of 'Internet of Things'

---

*Comments by Axon Partners Group*

*27 June 2017*

AXON

# 1. Introduction

On 16 May 2017, the Telecommunications Regulatory Commission ('TRC') published, for public consultation, a Green Paper on the Internet of Things ('IoT') and Machine-to-Machine (M2M) communications. The present document provides the response of Axon Partners Group Consulting S.L.U. (hereinafter, 'Axon Consulting') to the questions posed by the TRC in the Green Paper.

Many of these TRC questions are expressly addressed to parties that offer, or intend to offer, IoT services in the Jordanian market. Axon Consulting is not a provider of IoT or other electronic communications services, but an international consulting firm with a strong focus on the telecommunications, Internet and media industries. Accordingly, Axon Consulting will answer questions addressed to IoT service providers only insofar as its response can be a meaningful contribution to the public consultation instigated by the TRC.

Since its establishment in 2006, Axon Consulting has completed more than 100 regulatory assignments in the electronic communications sector, and has helped regulators design and implement regulatory policies that are crafted to the specific needs of their domestic market, while drawing maximum benefits from international best practice.

Axon Consulting has been particularly active in the Middle East in recent years, supporting several major public and private sector clients in Jordan, the UAE, Saudi Arabia, Oman and Bahrain.

Based on our international and regional experience, our sector expertise and the insights we have gained on IoT and M2M-related regulatory, strategic, market and technical issues, we wish to respectfully use this opportunity to provide our views on the TRC's Green Paper, from the perspective of international consultants specialised in the field. We hope that our comments that follow will contribute to a more complete and representative survey of views on the present and future of IoT/M2M in Jordan, and the role the TRC can play in this context.

Please note that the views set out in this document are those of Axon Consulting only and do not necessarily represent those of any of its clients.

# 2. Responses to the public consultation

## 2.1. Introduction

***Q1: Is the definition of IoT mentioned previously complying with your vision and the services you provide. If not, please elaborate.***

The definition of IoT proposed in the Green Paper is taken from Recommendation ITU-T Y.2060, paragraph 3.2.2. Like most ITU definitions, it has the advantage of a certain international consensus and credibility, which market players cannot easily contest. Nevertheless, the merits of this or any other definition depend on the context in which it is used. For example, a definition of IoT in a legal or regulatory document may need to be more precise, avoid commonly used but only vaguely defined technical concepts, and be linked to the specific legal definitions and terminology used in the relevant set of rules of the jurisdiction in question.

There are other examples of international definitions of IoT that can provide inspiration for an alternative definition. For example, the IoT European Research Cluster (IERC) has proposed the following, more detailed and precise, definition for IoT: "*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.*"[1]

Other international attempts to define IoT have only highlighted the difficulties of achieving an optimal definition. The IEEE (Institute of Electrical and Electronics Engineers) has dedicated an 86 page document to this subject alone ("*Towards a definition of the Internet of Things (IoT)*")[2] and has finally come up with two alternative definitions: a relatively short one for a "small environment scenario" and a very long one for a "large environment scenario".

To conclude, a reference to the ITU definition seems sufficient for the purposes of the present public consultation and general public debate. However, once the TRC

[1] See http://www.internet-of-things-research.eu/about_iot.htm
[2] Available on http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

decides on the specific regulatory action, if any, it needs to take with regard to IoT (and M2M), it should consider adopting a definition that is more specifically adapted to the nature and needs of that regulatory action and consistent with the terminology defined elsewhere in Jordan's telecoms legislation.

## 2.2. **Implementing IoT and M2M Services**

***2.1: Do you offer any IoT services in the Jordanian market? If Yes, answer the following:***
***2.1.2: Kindly, list and briefly explain those services.***
***If your answer is no, please answer the below question:***
***2.2: Do you have future plans to offer new IoT services in Jordan? What services? And timeframe? Please elaborate.***

As an international consultancy, we are not in a position to answer these questions (other than on behalf of our clients, which is not the purpose of our independent contribution to this public consultation).

## 2.3. **IoT Implementation Challenges**

***3.1: What are your expectations to the IoT traffic capacity in Jordan for the next 5 years?***
***3.2: In which fields of implementation it's expected to have the highest "data interaction" traffic and which is expected to be the lowest?***
***3.3: Please arrange the above mentioned challenges in terms of limiting the IoT wide implementation, from the most affecting factor to the least. Please justify and elaborate.***
***3.4: Are the data rates offered in Jordan sufficient to handle the IoT traffic especially for time - sensitive services?***
***3.5: Please suggest at least three categories that classify the services that reflects reliability levels that can be needed.***
***3.6 Please classify the services in term of latency acceptance ranges.***
***3.7 Please list any further challenges that might affect the implementation.***

Our replies under this heading are limited to **questions 3.5 to 3.7**.

IoT services can make use of a variety of platforms, from fixed telecommunications lines to a wide range of wireless technologies, such as RFID, NFC, Wi-Fi, Bluetooth, XBee, ZigBee, Z-Wave and Wireless M-Bus. Reliance on the existing cellular networks and technologies, e.g., through LTE-NB or even EC-GSM has the advantage of using

a widely deployed infrastructure, and it can be implemented relatively easily by the existing public telecommunications service providers, through software upgrades, even if the underlying infrastructure and standards were not originally designed for IoT and M2M, but for human-driven services.

These different available or emerging technologies offer different reliability levels and latency acceptance ranges and do not provide regulators with a clear and stable set of standards. Therefore, even if reliance on a mix of such technologies for IoT is likely to remain common in Jordan and elsewhere for a while, we believe that a more forward looking regulatory approach regarding reliability and latency standards for IoT services should be aligned with those applicable under the emerging standards for 5G.

One reason for this is that, even though 5G standards are still being finalized, they are being designed with (also) IoT in mind, right from the start. Further, there is at least an agreement on the three main usage scenarios that 5G must support, namely:

- enhanced mobile broadband (eMBB) for Internet access with high data rates to enable, for example, rich media applications (e.g., virtual reality (VR), augmented reality (AR), and high-resolution video streaming) or cloud storage and applications;
- ultra-reliable low latency communications (URLLC), for various remote control applications (e.g., robotics, surgery, infrastructure protection, smart grids, etc.), intelligent transportation systems etc. with very strict requirements, especially as regards latency and reliability; and
- massive machine type communications (mMTC), the scenario most clearly envisaging enablers of IoT, with dense sensor networks and billions of connected low-cost devices, combined with high requirements on scalability and increased battery lifetime. That said, certain types of IoT and M2M services for mission-critical applications, which do not require a very high number of small devices, but uninterrupted and robust exchange of data, will be better served by the URLLC scenario.

In broad terms, we believe there is a degree of consensus in the industry on the type of services and applications that are best served under each of the above scenarios (some of which are mentioned as examples above), and this can probably provide an answer to your question 3.5.

However, we would respectfully advise against any attempt to impose a "top down" regulation of minimum reliability, latency or other, similar, standards by type or service or application. IoT and M2M services are evolving very rapidly, and specific applications within the same industry or type of application may require very different

specifications. Furthermore, it is extremely difficult for most national regulatory authorities to pursue a "go it alone" standardisation process in this regard. Voluntary reliance on international standards and, in particular, those currently developed for 5G, may be the best way forward.

As regards your **question 3.7**, IoT faces a number of significant implementation challenges, with varying degrees of possible influence by national regulators or telecommunications and other electronic communications services. The table below provides an indicative list of regulatory challenges, as we see them, and their relative importance, as far as we can judge from international experience, even though we appreciate that this is just a preliminary view (1 = not very important, 2 = important, but not critical, 3 = critical).

| CHALLENGE | IMPORTANCE |
|---|---|
| **CONNECTIVITY** | |
| Insufficient or costly spectrum | 3 |
| Insufficient network coverage | 3 |
| Limitations/uncertainty on identifiers (numbers or IP addresses), especially if the service is using a public network | 3 |
| Standardisation and interoperability, need for open standards | 2 |
| International connectivity | 2 |
| **SECURITY** | |
| Data protection/privacy issues, anonymization of users' data in a distributed and mobile environment | 2 |
| Information security, network safety and liability issues | 3 |
| Uncertainty on intellectual property rights | 1 |
| **OTHER REGULATORY** | |
| Uncertainty on licensing requirements (if any) and applicable rules | 3 |
| Preventing distortions of competition on the market | 3 |
| Consumer protection rules | 1 |

**Table 2.1 Indicative list of regulatory challenges [Source: Axon Consulting]**

In addition to these challenges, which are wholly or partly related to the applicable regulatory and legal network, the deployment of IoT/M2M faces a range of commercial or technical challenges that fall outside the scope of a regulator's sphere of influence. Examples of such other challenges are shown in the table below.

| CHALLENGE | IMPORTANCE |
|---|---|
| Creating or matching consumer demand for IoT through commercially attractive applications | 3 |
| Appropriate technical assessment of information security risks and measures required to mitigate it; vulnerability of IoT devices to cyberattacks | 3 |
| Dealing with increased overall energy demands (even if consumption by single sensors or devices is very low) and battery life | 3 |
| Need to store and process huge volumes of data | 3 |

**Table 2.2 Indicative list of other challenges [Source: Axon Consulting]**

## 2.4. IoT and M2M regulatory, legal, consumer rights issues

***4.1: Do you think that at the current stage of time there should be a specific regulation for IoT and M2M?***

***4.1.1: If yes, what are the suggested topics that should be covered in the IoT regulation? If No,***

***4.1.2: From your point of view:***

***- What is the possible solution for handling the IoT issues at the current stage?***

***- Do you think that TRC should deal with the impacts of IoT services on security, privacy, numbering, spectrum and competition and be ready if companies chose to provide them at large? Or not doing anything until these issues become mature and regulated globally?***

***4.2: How can you solve the above mentioned challenges that face the consumers?***

***4.3: What indicators and when do you think is the right time to regulate IoT?***

***4.4 Do you think at the current stage of time an intervention by TRC should be taken to regulate Licensing and spectrum management to enable/allow providing IoT service in the kingdom through allocating spectrum for IoT Services?***

***If Yes, how this can be achieved? Please elaborate. If no,***
***4.5 When the review should take place to specify the need of taking an action?***
***4.6 If you are offering or planning to offer IoT services in the Jordanian market, please list what type of connectivity methods and technologies you are using (or will use)?***
***4.7 Do you think that the spectrum and backhaul capacity you have will meet the demand of the IoT needs?***
***4.8 Regarding the millimetre wave bands, do you think they will be useful and meet the requirements of IoT?***

Our replies under this heading are limited to **questions 4.1 – 4.1.2**:

Legal uncertainty on the status of IoT/M2M under currently applicable rules is one among several factors that may work against the growth of such services in Jordan. However, IoT/M2M services are new and rapidly evolving, with very few (or no) examples of ad hoc regulation worldwide.

We believe that, without helpful international precedents and given the early stage of development of IoT/M2M in Jordan today, the introduction of specific national regulation of IoT/M2M may risk being considered premature and heavy-handed. That said, this preliminary view may need to be reassessed in light of any comments the TRC will receive from market players.

Even if these comments confirm that ad hoc regulation of IoT/M2M is premature or unnecessary in any event, there is substantial regulatory guidance that TRC may consider providing already, e.g., in the form of guides, booklets, Q&A etc. wish to support the implementation of IoT/M2M in Jordan. Such guidance may concern, for example:

- Clarification of the licensing status of IoT under the current rules by, e.g., drawing the necessary distinctions between public/private telecommunications networks (both of which can be used for IoT/M2M services); connectivity service providers/IoT service providers/IoT users and end-users; licensable/free spectrum; approval of equipment; and their implications, i.e., the specific rules that apply to each scenario under the current telecommunications laws and regulations (pending the adoption, in the future, of any *ad hoc* regulation).
- Information on the international standards in place or in preparation with regard to IoT/M2M, with links to the relevant public and private international organisations for more information.
- General information to foster consumer awareness of the pros and cons of IoT/M2M.

- A reference to the rules applicable today in Jordan regarding security, privacy, numbering, spectrum, competition and consumer protection, even where these are just general, incomplete and not IoT-specific.

***4.8 When do you think that regulating market competition issue of IoT in Jordan will be a critical issue?***
***4.9 Are the competition regulations in Jordan sufficient to handle the above IoT issue?***
***Or a modification on the current regulations is needed? Or a new separate regulation for the competition in IoT issues should be adopted? Please elaborate on more details.***
***4.10 Is there a need for issuing market structures and pricing schemes that defines IoT services pricing and describing how IoT can drive competitive advantage through better information and more localized decision making? Please elaborate***

Internationally, the discussion of possible competition issues in IoT has focused on certain potential problem areas but has failed, so far, to point at specific instances of abuses or other infringements of competition rules.

Such (so far mostly potential) threats to competition associated with IoT include:

- the control, by a handful of major service providers, of "Big Data" collected through IoT devices and hence the possible risk of abusive use of this new type of asset;
- bottlenecks or abusive conditions for access to numbering or spectrum for IoT that may favour incumbents over innovative new market entrants;
- various forms of exclusive dealings and discrimination by dominant companies;
- bundling of certain devices or technologies with analytics services and/or an obligation to share data with the supplier.

The prevailing international view is that such competition issues, if and when they arise, can generally be dealt with on an *ex post* basis, relying on general competition law provisions. As far as we are aware, there seems to be no call for any IoT-specific competition law regulation. Similarly, competition law inspired *ex ante* regulation of electronic communications has not yet led to IoT-specific product markets susceptible to ex ante regulation or *ex ante* remedies or pricing regulations for IoT services in particular. Having said that, there are more generically defined electronic communications services, such as broadband services, which are today subject to *ex ante* regulation in some countries. This may, of course also affect the conditions for the provision of IoT, among other data services, in the countries concerned.

The competitive situation for IoT/M2M services may well change in the future, as the market's may gradually consolidate around a few major players. Any related feedback from Jordanian market players may also help refine the above views, as distortions of competition and the need for regulatory interference are not always easy to identify without first hand, non-public, evidence from the companies concerned.

***4.11 Do you have a policy for visibility and secure management of "Things" on your network today?***
***4.12 Are you collecting management or visibility information from the "Things" on your network?***
***4.13 How are you collecting security and operations data about "Things" on your network?***
***4.14 How would you rate your ability to provide security to the "IoT" services?***
***4.15 What controls do you plan on deploying in the next 5 years to protect against security risks?***
***4.16 What do you think the greatest security threat to the IoT will be over the next 5 years?***
***Regardless if you do or not providing IoT services, please answer the following:***
***4.17 Who should take responsibility for managing the risk imposed by new "Things" connecting to the Internet and the local network? And when is the best time that to issue a regulation to protect security?***
***4.18 Do you think that there is a need for security protection regulation to be issued in the current time?***
***If No, when is the best time that a regulation to protect security should be issued?***
***4.19 Do you think that securing IoT will demand to restructure your current organization's security policies and directives? If yes please explain how. If No, how you are planning to handle IoT services and devices security?***
***4.20 Are you dedicating Gateways, IPS, and Network monitoring systems to your connected "Things"? Or you are utilizing your current Network infrastructure and systems?***
***4.21 What kind of encryption algorithms your organization uses for your network communications?***

Most of the above questions are clearly addressed to the providers of IoT only. As regards **question 4.16**, we believe that security poses a major threat to the development of IoT. The implications can be particularly alarming for sectors such as fleet management, security and surveillance applications, medical devices, inventory applications, smart grids and industrial process management.

The greatest security threat for IoT stems from the relatively open, unsecure-by-design, nature of IoT devices, which are generally cheap, with limited computing power and protection against network-borne threats. This makes them particularly susceptible to, for example, "worm"/ransomware attacks, similar to "WannaCry", which recently affected more than 150 countries. Such attacks may be an "attractive next frontier" for hackers worldwide, especially for IoT devices that are connected to smartphones or corporate networks.

Security issues stemming from design flaws are difficult to tackle at a national level through regulation, particularly if the market concerned is relatively small, as is the case in Jordan. As in other areas of digital security, detailed top-down regulation may be inappropriate, because security threats and the required countermeasures are evolving far too rapidly for legislation to catch up. A possible immediate role for TRC in this regard can be:

- the provision of information to the public on the emerging international certifications for IoT security and,
- the provision of non-binding guidelines and recommendations on certifications that may be required for particularly sensitive types of IoT applications, in specified sectors.

**Questions 4.17 and 4.18**: Security tasks and any domestic rules the risk imposed by new "Things" connecting to the Internet and the local network cannot be dealt with separately from a country's overall cybersecurity policy, rules and authorities entrusted with their implementation. Accordingly, addressing IoT-related security risks requires a holistic approach and coordination with Jordan's National Information Assurance and Cyber Security Strategy (NIACSS), as well as the relevant services and resources of the National Information Technology Center (NITC) and the Ministry of Information and Communications Technology (MoICT).

However, general cybersecurity measures and rules may be insufficient to deal with some of the more practical security issues associated with IoT/M2M. In this regard, we believe that TRC has a key role to play as the authority most closely regulating scarce resources (spectrum and numbering), QoS and consumer protection issues in the telecommunications sector. It is also the authority supervising the obligation of market players' obligations with their individual or class licenses. Insofar as IoT services are provided by such licensees, the TRC has, again, a key role to play as a regulator and enforcer. It may be also in a better position to impose *preventive* measures against IoT security breaches, as opposed to *suppressive* measures, which are better suited to the powers of criminal enforcement and other State authorities.

IoT security issues are already emerging as a priority across the world, and countries have no time to lose in clarifying their domestic regulatory powers and tasks in this regard. For the reasons discussed above, we believe the TRC should play a key role against security risks associated with IoT, notwithstanding the need for coordination with other authorities. In immediate terms, it may be difficult for the TRC (and not necessarily required by the market) to adopt any IoT-specific security rules. However, it may be possible to incorporate such rules in more broadly scoped regulatory measures (e.g., those dealing with consumer protection, any future revisions of the texts of current licenses etc.).

***4.19 Do you have a policy for data privacy and protection of "IoT" services today? If yes, how do you apply this policy? And do your consumers aware of such policies?***
***4.20 How would you rate your ability to protect privacy of the "IoT" data?***
***4.21 What controls do you plan on deploying in the next 5 years to protect data privacy?***
***4.22 Do you think that there is a need for data privacy protection regulation specific for IoT services to be issued?***
***4.23 From your point of view, do you think customers and end users should have any assurance of privacy when subscribing to IoT services? If yes, please mention how should this be achieved? If No, please elaborate.***
***4.23 If you are providing IoT services, what do you are using to differentiate the numbers used for IoT services-Is there any specific numbers or ranges for IoT services- please List it if any?***
***4.24 Do you think that there is a need for specifying a numbering range (in the National Numbering Plan) for IoT services in the current time?***
***If yes, please suggest a numbering range for IoT services.***
***4.25 Do you think that the late migration to IPv6 will limit the IoT expansion?***
***4.26 Do you agree to use a specific code (MCC) in IMSIs permanently for M2M services abroad?***
***4.27 In case MVNO, what are your arrangements to enable them to use your Network to provide the IoT services to their customer inside the Kingdom And outside?***
***4.28 What is the percentage of Internet addresses using version six that are used to provide IoT services to those using version four in your network?***
***4.29 List and Clarify the percentage of the IoT services interim their identifiers that used by your network (IP address, MAC address ...) to provide IoT services?***
***4.30 Any recommendation about the Addressing and Numbering for IoT services provided by non-telecommunication licensed companies?***

On **questions 4.22-4.23**: Data protection is a key issue in the context of IoT and can be addressed in two different ways: through general ("horizontal") rules or through IoT-specific measures.

To the best of our knowledge, Jordan does not yet have a general data protection regime in place. International experience suggests that the adoption and effective implementation of a data protection regime is a long and controversial legislative process, which requires years of practical implementation experience for the regime to become really effective. It is also a process whose legislative components are largely outside the scope of the telecoms regulator's powers.

This leaves IoT-specific data protection rules as the only other alternative, at least in the form of a simple set of provisions that should guarantee some basic data protection rights for the users of IoT services, without going into the lengthy and detailed extremes of modern "horizontal" data protection laws.

Such a targeted regulatory intervention may be possible in the framework of any revisions to the more general telecoms rules (e.g., those relating to consumer protection or the conditions of individual or class licenses) or model clauses to be proposed by the TRC. As mentioned earlier, the adoption of comprehensive stand-alone regulations (including data protection rules but also other issues) dealing exclusively with IoT/M2M services strikes us as, at best, premature at this stage.

On **questions 4.24, 4.26 and 4.30**: Service providers in Jordan are best placed to provide practical insights on their individual numbering needs for IoT/M2M services. In the event that these views do not lead to substantial consensus, however, it may be useful to draw some benefits from the parallel international debate on these issues.

As an example of this discussion, we would refer to the conclusions reached in BEREC's[3] February 2016 Report on "Enabling the Internet of Things".[4] Briefly, the report concluded that:

- The identifiers used for IoT services in public networks are E.164 and E.212 (IMSI) numbers as well as IPv4 and IPv6 addresses.
- In the short and medium term, classical telecommunications numbers (E.164 and E.212) will continue to be one solution to identify IoT devices. IPv4 can provide a

[3] Body of European Regulators for Electronic Communications.
[4] Available here: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

complementary addressing resource, but its address format supports a relatively limited number of globally addressable devices, even though many connected devices may be located behind one IPv4 address using Network Address Translation (NAT).

- At least in the longer term, the use of IPv6 addresses is likely to become the preferred solution, because IPv6 has a significantly larger address space and can support a considerably higher number of devices.
- The possible scarcity of E.164 should be analysed and solved by national regulatory authorities at national level, e.g. by introducing a new numbering range for IoT services or increasing the mobile number resources.
- CEPT suggests the relaxation of the criteria for the assignment of MNCs, as this may facilitate change of connectivity provider – besides over-the-air provisioning of SIM – without having to physically swap the SIM. However, broadening the circle of assignees might lead to a scarcity of E.212 MNC resources since in many countries only 100 MNCs are available.

***

We thank the TRC for this opportunity to provide comments and we'll be happy to respond to any questions or invitations for further input that you may have.