Zain's Response to TRC

Green Paper of "Internet of Things"

9th August 2017

Zain welcomes the opportunity that the Telecommunication Regulatory Commission (TRC) has offered to provide comments and share thoughts to its green paper entitled: "Internet of Things (IoT)" (The Paper).

I. INTRODUCTION AND SUMMARY

Internet of things (IoT) and Machine-to-Machine (M2M) represent a huge opportunity and can bring substantial socio-economic benefits to Jordanian users, businesses and government. IoT offers unrivalled opportunities for economic productivity and innovation; it can even create entirely new markets.

The IoT is fast becoming the new driving force behind the global economy. Analysts estimate that by 2020, there will be over 15 billion connected devices, with 3.4 billion in North America alone[1]. Of these, 1.2 billion will represent cellular M2M connections, an important part of the competitive connectivity landscape.

[1] Machina Research (2016).

In summary, Zain believes that IoT in Jordan is still at an early stage in terms of regulation; regulators and policymakers should avoid strict IoT-specific regulation and instead; allow the IoT market to mature under generically applicable frameworks. Unnecessary or technology-biased regulation will strangle innovation, raise costs, discourage investment, and harm consumers.

II. ANSWERS TO THE GREEN PAPER QUESTIONS:

Zain would like to share its thoughts and answers to the specific questions that were raised by TRC in its Paper.

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

Multiple definitions do exist for IoT. However, efforts to define IoT are premature. It is not necessary to determine in detail which [IoT] definition is the most appropriate, but the inclusion of the spectrum in the definition is essential. we support the following definition:

"The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data, and that might require a dedicated spectrum".

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.

Zain offers some IoT services, and is working hard to provide more and more IoT services to its customers, the current services are:

- Zain Track: Tracking Service that utilizes GPS to locate and track vehicles. The service works through installing a tracking device inside the vehicle, and the location of the vehicle will be sent to the customer via Zain network.

- Zain Camera: Video Surveillance Service by using the Internet to allow the customer to monitor his/her premises/belonging etc., through his/her smartphone, tablet, or personal computer.

- Zain Home Security: a service where alerts are sent to the customer in event of any unauthorised intrusion or strange movement in their home.

- Zain Tanki: a service in which a device reads fluid level (diesel, water etc.) inside the tank, the customer can then read the liquid level through an application. He/she will also be able to receive alert messages for certain quantity percentages.

3.1: What are your expectations to the IoT traffic capacity in Jordan for the next 5 years?

We generally see that there are no clear and specific expectations of the IoT traffic capacity for the next 5 years, due to fast changing customer behaviour and demand for IoT services that will be available within the coming 5 years; the growth of the IoT and the number of connected devices are mainly driven by emerging applications and business models, and supported by

standardization and falling device costs, also supported by the development of governments and municipalities.

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?

With IoT catching up, smart meters and smart homes (Building & home automation) are the most awaited feature, with brands already getting into the competition with smart appliances. Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted that smart homes will become as common as smartphones.

Connected healthcare and agriculture yet remain the potential giant of the IoT applications. The concept of connected healthcare system and smart medical devices and smart farming bears enormous potential not just for companies, but also for the well-being of people in general.

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.

As the Internet of Things (IoT) continues to gain attention, it is important to understand the potential challenges the technologies present.
here are some challenges that might be faced when implementing IoT from the most affecting factor to the least:

1. Spectrum and bandwidth flexibility
2. Mobility/coverage
3. Network and device energy efficiency

4. The economic factor
5. Latency
6. Reliability
7. Interoperability and standardization
8. Massive number of devices
9. Traffic capacity
10. Achievable end user data rate

3.4: Are the data rates offered in Jordan sufficient to handle the IoT traffic especially for time - sensitive services?

The volume of the IoT services provided in Jordan is still small and is considered at its early stages, therefore the data rates currently offered by operators would not give proper indication in that regard. However, for time-sensitive services other factors could be of higher importance such as latency and bandwidth, and so necessitate the emerging of new technologies like 5G, and here the role of the regulator/TRC becomes crucial in facilitating the introduction of these technologies, including the availing of new spectrum with reasonable prices.

3.5 : Please suggest at least three categories that classify the services that reflects reliability levels that can be needed.

1. Connected cars
2. Managed streets and traffic lights
3. Health care
4. Home security and appliances
5. Transportation

3.6 Please classify the services in term of latency acceptance ranges.

The IoT will increase the range of services, each requiring varying levels of bandwidth, mobility and latency. For example, services that are related to public safety or personal safety will generally require low latency. On the other hand, services that provide metering information for example, which is a normal monitoring activity might have latency acceptance ranges.

3.7 Please list any further challenges that might affect the implementation.

Security is a key consideration for businesses adopting IoT/M2M technology, which means that for many businesses M2M is not a simple 'plug and play' technology. In relation to privacy and security, clearly there are real concerns if due consideration is not given.

The security of data in transit does not ensure the 'end to end' security of M2M data, particularly for any data stored within the 'endpoints' of the service (the user device and service platform, which typically lie outside of the communication network). It is the responsibility of the entity providing a cellular M2M service to ensure adequate security measures applied 'end-to-end' within their services and that the data within the endpoints of their service is adequately protected.

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?

Regulators and policymakers should avoid strict, IoT-specific regulation and instead allow the IoT market to mature under generically applicable frameworks. A flexible and gradual approach by regulators is essential as different IoT services may have different requirements. The government should support self-regulation by IoT stakeholders, risk management-based approaches, and privacy management programs that empower stakeholders to achieve important policy goals without regulation.

We believe that the regulator intervention should be limited to: Spectrum dedication management (operators are not at risk of interference and can control usage levels as they have exclusive access to their spectrum bands), and Numbering allocation and devices type approvals.

Currently there is no harmonised dedicated spectrum allocation for M2M and it is fitted in where it can be. To remedy this situation, operators are using spare capacity on 2G, 3G and 4G systems for M2M services within existing spectrum

allocations, therefore, Regulatory bodies should work with mobile and M2M stakeholders, including mobile network operators and equipment vendors, to examine which bands should be harmonized, and what band plan considerations should be prioritized. Harmonized spectrum bands need to be able to support the full range of potential M2M deployment scenarios. This includes high data-rate applications which could require substantially more spectrum than existing forecasts. It should also prevent the operators from being under risk of interference.

In addition, regulation should avoid technology restrictions, while relying on competition. Excessive or technology biased regulation can hinder innovation, raise costs, limit investment and harm consumer welfare. Therefore, we encourage TRC to support a policy framework that is based on equal services and technological neutrality.

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 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 millimeter wave bands, do you think they will be useful and meet the requirements of IoT?

Regarding regulating Licensing and Spectrum management, we kindly refer to our answer to Q 4.1 - 4.3 above.

The Millimetre waves are not the right waves to carry IoT, IoT requires long waves and lower spectrum to provide the adequate coverage levels and to guarantee longer battery life time.

4.6 When do you think such development of mobile networks as mentioned (in section ii switching and roaming) will be needed in Jordan?

4.7 Is there any need for a regulatory framework by the TRC to regulate the IoT roaming issues?

4.8 Do you think that the current signed roaming agreements are appropriate to encourage IoT services in Jordan? Or do those agreements need update?

4.9 Is your company welling to dedicate SIMs for M2M Communications? if Yes, will the cost rates vary from normal roaming services?

4.10 Is there any need to draw a distinction between person-to-person communications and IoT connected devices in terms of roaming?

4.11 Is there any need for the TRC to intervene in switching process, mechanisms, switching mechanisms, and cost for the purpose of achieving a competitive market for IoT services? If not, more explanation is needed.

Roaming generally is implemented through bilateral agreements between operators. Roaming has traditionally been designed as a service to enable foreign visitors to continue to use their mobile service while travelling abroad—i.e., as a temporary service for an individual, facilitated by a host provider. For IoT, the roaming end user may be companies offering IoT services in foreign markets, also facilitated by a host provider, so the connectivity is provided

through commercially negotiated roaming agreements between mobile operators, therefore, there is no need for any intervention from regulator since this would not be appropriate, as restrictive roaming regulations could deter the proliferation and efficacy of IoT.

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

At this relatively early stage of IoT market development, it is not clear whether there will be a need to modify the current competition regulations. The major issues that shall be taken into consideration is selling below the cost (price war), barrier to entry and create new products and services.

these concerns are generally similar in nature to the competition issues in other than IoT arena, which again doesn't require specific actions at least at this early stage of IoT implementation.

If you provide an IoT services,

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?

Zain believes the security is vital to building and maintaining consumer confidence in mobile services to date, and will be as critical to the success of IoT connected services that have the potential to support and deliver increasingly sophisticated and security sensitive services. We do have a very high degree of security, access control, and enforcement various privacy policies.

The IoT platform owner has the full responsibility to make sure of their devices security. The government could impose minimum security standards on IoT manufacturers, leading them to make their devices secure even though their customers don't care.

If you provide an IoT services,

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.

Zain already has well-established data protection and privacy policies, which is utilized in any current and future arrangements with IoT platform and other services vendors.

However, IoT services typically involve more parties than simply mobile operators, such as device manufacturers, companies developing systems, and online platforms providers. It is important that privacy and data protection procedures/protocols apply consistently across all IoT platform providers and device manufacturers.

It is very important for the customers to be confident that the companies are using their connected device data securely and in ways that protect their privacy.

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?

Zain suggests to have dedicated number range (s) for IoT services taking into consideration the number of MSISDN digits to meet the future growth and need. In light of the huge number of connected within the mid to long term, the scalability is a consideration for addressing, so the current version of the Internet Protocol (IPv4) is extremely limited, the new version (IPv6) being rolled out by ISPs around the world has enough addresses for almost any conceivable number of devices. The transition from IPv4 to IPv6 has taken longer than expected, and policy makers may need to continue with programmes to encourage the transition in the medium term.

In conclusion and based on the common best practices, Zain believes that the regulator should support self-regulation by IoT stakeholders since imposing any specific regulations at this early stage will limit the innovation, raise costs, discourage investment, and harm consumers.

We welcome any further discussion with the TRC at their convenience of all views and thoughts communicated in this response.