What’s Got Hot in the Internet of Things?

Krishna Jhala - Senior Counsel - Digital & Data
k.jhala@tamimi.com - Abu Dhabi

Introduction

As Professor Klaus Schwab (Founder and Executive Chairman of the World Economic Forum) said we are at the beginning of *The Fourth Industrial Revolution,* a revolution which is fundamentally changing the way we live, work and relate to one another. This revolution, through a fusion of technologies (including Artificial Intelligence, Blockchain, and Internet of Things (‘IoT’)), is blurring the lines between physical, digital and biological spheres. While it may seem disruptive in nature, it brings with it new unforeseen challenges. Globally, various authorities are grappling with these issues and this has resulted in a spurt of policy and guidance documents, notably in the realm of cyber security, data protection, cloud computing regulatory framework and IoT.

Simply put, IoT is a system of physical things embedded with sensors, software, electronics and connectivity that creates a network in which physical objects can exchange data internally or with other connected machines. Thus, any physical object can be transformed into an IoT device if it can be connected to the internet and controlled accordingly. In the UAE, the IoT market is (on a conservative basis) expected to double over the next five years.[1]

To regulate and foster this growth, the UAE government issued its IoT Policy on 22 March 2018 (‘IoT Policy’). However, the Telecom Regulatory Authority (‘TRA’) is yet to issue the regulations/procedures necessary to operationalise the implementation of the IoT Policy.

Objectives of the IoT Policy

The IoT Policy aims to regulate IoT within the UAE and has been issued by the TRA with the intention of making the UAE a leading country in developing IoT services.

TRA developed the IoT Policy based on certain specific considerations which include:

1. to provide a secure IoT Service;
2. to meet all reasonable demands for IoT Service;
3. to support ongoing innovation;
4. to manage scarce resources efficiently;
5. to protect the rights and interests of the user of IoT; and
6. to provide clarity for IoT market development.

The TRA may also issue further regulations, directives, and/or guidelines to provide incentives and support in developing the IoT environment in the UAE. If it is required, ministries and regulators for particular industries may develop their own additional IoT-specific guidelines through coordination and consultation with the IoT Advisory Committee (which was established for IoT related matters within the UAE and has representatives from various identified ministries, regulators, public sector entities and experts and is chaired by the TRA).

Key Definitions under the IoT Policy

As with most technology related matters, there is a bit of jargon. To understand the IoT Policy, you need to understand the key definitions:

IoT is defined as "*global infrastructure for information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*";

IoT Service is defined as "*set of functions and facilities offered to a user by IoT Service Provider and it does not encompass IoT specific connectivity*"; (like connected home appliances, connected cars, Bluetooth enabled pagers in restaurants, driverless vehicles);

IoT Service Provider means "*any person that provides an IoT Service to users including individuals, businesses, and the government that will comprise the provision of IoT related service/solutions*". (like car manufacturers, telecom service providers);

IoT-specific Connectivity means "*connectivity that is transmitting, broadcasting, switching or receiving IoT related data by means of a Telecommunications Network covering a wide area*";

Mission Critical IoT Service means "*an IoT Service which upon failure may result in adverse effects on the health of individual(s), public convenience or safety, and/ or national security*." (like driverless cars, drones, medical devices).

The IoT Policy is applicable to all those concerned with IoT within the UAE including but not limited to licensees (like Etisalat and Du), IoT Service Providers and IoT Service users (i.e. individuals, businesses, and the government).

Relevant Provisions under the IoT Policy:

1. An IoT Service Provider has to register with the TRA and obtain an IoT Service Provider Registration Certificate in order to provide IoT Services. Providers of Mission Critical IoT Services have additional requirements which include maintaining subscriber information such as the subscriber's name, address

and ID, the device's model and registration number, and any other information that the TRA may stipulate from time to time.

2. It is a pre-requisite for an IoT Service Provider to have a local presence (on either the mainland or a free zone). In the absence of a local presence, an official representative who is locally present may be appointed. The official representative shall be responsible for all communications with the TRA and UAE law enforcement agencies.
3. The IoT Policy sets out the additional requirements for Radio and Telecommunications Terminal Equipment ('RTTE') that provide IoT Services. In addition to the existing type approval requirements for RTTE, in case the RTTE has the potential to collect data/information and/or provide the IoT Service, it will have to: (i) indicate the features and functions of the device that collects data, sensory inputs such as cameras, location identifiers, and microphones; (ii) indicate the impact on the device's features or use in case of unavailability of connection; (iii) the device shall be capable of being reset to its original settings; and (iv) that 'Security by Design' be an incorporated feature to combat unauthorised usage.
4. Any person who wishes to provide IoT specific Connectivity should directly approach the TRA and the TRA will conduct a case-by-case assessment on whether a licence for deployment and operation of an IoT specific Connectivity network within the UAE is necessary. There are currently no set procedures for providing IoT specific connectivity.
5. A subscriber identification module (SIM) is an integrated circuit that securely stores the international mobile subscriber's identity. The IoT Policy specifically permits the use of physical SIMs and eSIMs, however, soft SIMs (essentially a virtual SIM where there is no SIM hardware and the SIM functionality is delivered onto the device virtually, or over the air ('OTA'), once the user switches it on) shall require TRA's prior approval, which indicates a separate licence requirement for soft SIMs.
6. As per the IoT Policy, IoT Service Providers have to follow specific principles of data storage:

- Purpose limitation: Data must be collected for specified, explicit and legitimate purposes only and shall not be further processed in a manner that is incompatible with those purposes;
- Data minimisation: Data must be adequate, relevant and limited to what is necessary for the purposes for which it is processed; and
- Storage limitation**:** Data must be kept in a format that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.

7. Data is classified into four categories based on the potential adverse impact caused in the case of a breach of confidentiality or unauthorised disclosure of the data. Such categories include:

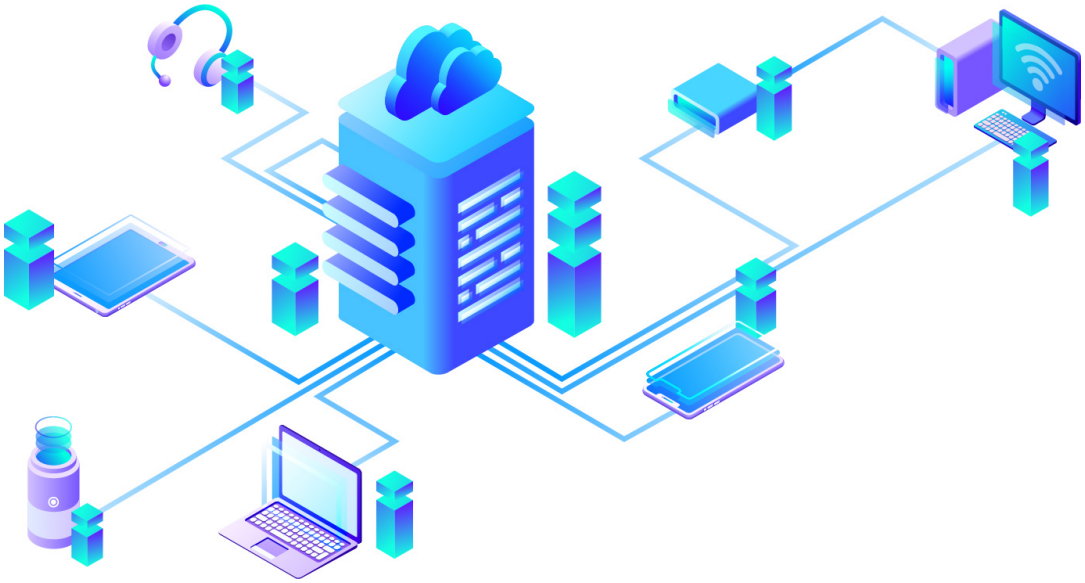
- "Open", i.e., can be used freely or subject to a minimum limit;
- "Confidential", i.e., may cause limited damage;
- "Sensitive", i.e., may cause significant damage; and
- "Secret", i.e., may cause significant damage to supreme interests of the country and very serious damage to individual, businesses and the government.

There are data localisation requirements which state that Secret, Sensitive and Confidential data for individuals and businesses are to be stored primarily in the UAE. However, such data may be stored outside of the UAE if the destination country has data security and user protection polices which are at least of the same level as those followed in the UAE. Further, Secret, Sensitive and Confidential data of the government must remain in the UAE under all circumstances. Open data for data for individuals, businesses and the government may be stored within the UAE and/or outside the UAE. With regards to the IoT Policy, the TRA deems Personal Data (which refers to information relating to identifiable Natural Person as defined under GDPR) to be Secret data for individuals. (This may be problematic in practice as not all personal data such as your name, email address needs to be a 'secret' in every circumstance).

8. The IoT Service Providers must use an encryption standard that fulfils the requirements of the competent UAE authorities. Where a higher encryption standard is required by the IoT Service Provider, TRA approval shall be sought, and will be reviewed on a case-by-case basis.
9. The TRA has implemented a numbering plan for M2M (machine to machine technology) services. For Mission Critical IoT Services, the Licensees should be able to differentiate between assigned numbers.

Where a clear distinction between numbers cannot be made, then Licensees may be supported by the TRA with assignment of numbering block(s) within the M2M numbering range.

10. The TRA exercises forbearance on roaming of IoT devices (i.e. devices using SIMs of foreign networks/roaming on Etisalat and Du's network appears permitted).
11. Through the IoT Policy, the TRA aims to encourage the use of the wider adoption of the OTA/remote provisioning of devices for IoT Services and has the power to stipulate mandatory OTA/remote provisioning requirements for specific Mission Critical IoT Service. OTA refers to the ability to remotely change the SIM profile without physically accessing the SIM. Further, transition to IPv6 is encouraged by the TRA.



Items to be Detailed in the IoT Regulatory Procedures:

As mentioned above, TRA has to issue the IoT Regulatory Procedures which will contain detailed procedures on the following:

1. IoT Service Provider's registration procedure;
2. detailed procedures for the use of eSIMS;
3. data security and user protection polices/regulations to be followed in the UAE;
4. regulatory and legal requirements for the monitoring and interception of data by UAE law enforcement agencies; and
5. encryption standards to be used by IoT Service Providers that meet UAE authority requirements.

Breach of IoT Policy

As per the IoT Policy penalties (penal and fiscal) of non-compliance with the IoT Policy and/or the UAE's Telecommunications regulations are defined within the UAE Telecommunications Law, which may include temporary or permanent service suspension. Some examples of breaches include: providing services without a licence; not having up-to date information of subscribers in regard to Mission Critical IoT Services; non-adherence to defined consent requirements for Data Processing; non-adherence to data storage requirements; provision or activation of Soft SIMS without TRA approval; and non-provision of OTA/remote provisioning services where mandatory. The violations/breach of the IoT Policy will be applicable only when once the it is operational.

Effectiveness

While it was intended that the IoT Policy will be implemented within one year of its issue i.e., by 22 March 2019, there is no further indication from the TRA regarding the issuance of IoT regulations/procedures and actual operationalisation of this policy. It is not clear whether the IoT Policy, once enforced, will provide a transition period for the existing IoT Services to be registered with the TRA.

Conclusion

In light of the present IoT Policy and until such time as it comes into force, it may be prudent for IoT Service Providers to review their current operating procedures and protocols, in order to determine whether they comply with the IoT Policy, for example focusing on identifying the categories of data (*open, confidential, sensitive, secret*); identifying the specific storage limitations of data; and considering stipulations for the storage of the different categories of data (within and outside of the UAE).

The UAE is not the only GCC country addressing the IoT. KSA's IoT regulations have been discussed in *An Overview of Telecom Licensing in Saudi Arabia* published in the March 2019 edition of Law Update and Oman recently conducted a public consultation on IoT and M2M.

Al Tamimi & Company's TMT team regularly advises on telecom, media and technology matters. For further information please contact Krishna Jhala (K.Jhala@tamimi.com).

[1] https://www.techsciresearch.com/report/uae-internet-of-things-iot-market/1396.html