Representing:

Organisation

Organisation (if applicable):

TELIT COMMUNICATIONS SPA

What additional details do you want to keep confidential?:

No

If you want part of your response kept confidential, which parts?:

Ofcom may publish a response summary:

Yes

I confirm that I have read the declaration:

Yes

1. IoT definition, applications and demand:

The "Internet of things" (IoT) is a phrase that serves as a broad label for the idea of an increasingly connected future where regular, everyday items will be fitted with sensors and the ability to connect to networks and transmit data. Machine to machine (M2M) communications, however, is a networking term that describes the technology that enables devices to communicate with each other. Today's more advanced M2M systems involve not just machine to machine communications but man to machine and vice versa. M2M is the key to the IoT because it encompasses the technologies that are necessary to enable a successful IoT environment. In the new M2M-driven world, there will be a continuous exchange of information between sensors attached to connected, everyday items or infrastructure, computers, and the networks. For the future, as envisioned, to work the system must be designed to handle the transmission, receipt, and processing of exponential amounts of data.
The penetration of Internet adoption, faster mobile connections, and the availability of advanced computing capability in the form of cheaper, smaller devices with significant processing power has facilitated the growth of the Internet of things. The key element driving this market is the ability to install inexpensive sensors in machines and devices. These sensors collect real-time data and transmit it via the Internet or wireless networks to computers, other machines, or to people. At the receiving end, application software converts data to useful information.
In 2012, an estimated 8.7 billion things were connected worldwide and projections show that with the new technological capabilities this could grow to 50 billion by the year 2020.

All of these factors present significant possibilities for the IoT to be successful and be an important emerging market that has implications across a host of service sectors. As Ofcom notes, IoT will have a transformative impact in sectors such as healthcare, transportation, and energy; TIA believes that the IoT also holds great potential for other important sectors, such as manufacturing, defense, and emergency services, among others.

To facilitate the technology development in this area, TIA has continued to update it's TR-50 M2M protocol standard series. The updated standards, TR-50 TIA 4940.020 and TR-50 TIA 4940.000, will enable manufacturers, even those with limited telecommunications experience, to equip their offerings with secure and affordable connectivity. This smart devices framework can operate over different underlying transport networks.

2. Spectrum requirements :

Efficient use of scarce spectrum resources is a subject of increasing interest to policymakers, the information and communications technology (ICT) industry, other industry sectors, and the scientific research community. This has been necessitated in part by the parallel increase in demand for spectrum uses beyond commercial communications – including for satellite or aeronautical applications, radiolocation, or other civilian or military capabilities. Against this backdrop, spectrum sharing may hold promise as a means to increase the efficient use of spectrum – whether by accommodating multiple user groups or types of uses – and to help alleviate challenges in spectrum scarcity.

More efforts are needed to facilitate the deployment of Authorized Shared Access (ASA)/Licensed Shared Access (LSA) approaches. ASA is a ″third way″ spectrum management system that combines elements of traditional ″command and control″ spectrum management with geolocation technology, e.g., by providing users with a ″token″ to use spectrum at certain times/places. ASA/LSA approaches show great promise as a means to enable sharing among disparate uses. They provide a means to ensure ongoing viability of incumbent uses by creating a policy environment that enables compatible operations with new uses. Meanwhile, these approaches also provide secondary users a means to gain access to spectrum that is already licensed to one or more primary users, but may be under-utilized or capable of supporting multiple uses. However, to achieve these benefits, spectrum released on a shared basis should be globally harmonized to ensure the economies of scale that will facilitate the large-scale deployments necessary to fully utilize the promise of these technologies. Harmonization will thus facilitate further private-sector development of standards that incorporate spectrum sharing into the toolbox of techniques used for network management and operational support.

3. Network-related issues:

o Approaches to delivering IOT services

M2M is the fastest–growing segment of the U.S. telecommunications industry, increasing 61.6 percent in 2013 following a 62.2 percent rise in 2012. Low–cost sensors allow virtually any device to become M2M–capable and new applications are being developed that are driving demand. Government regulations are also supporting M2M growth. Safety and security requirements for automobiles have resulted in much of the automotive hardware having M2M capability. In general, hardware now has sensors, RFID and communication capabilities. Remote servicing of equipment and remote diagnostics are among the market applications. Satellite M2M is also growing. Vehicles have been the leading M2M market but healthcare, utilities, consumer electronics, energy and manufacturing are growing rapidly.

o Degree of openness

In its discussion of how IoT services could be deployed, TIA notes its concern with Ofcom's reference to ″open versus proprietary″ standards. Recently, there have been some attempts to re-define ″open standards″ that may disrupt the development of standards and the related balance of interests. For some, the concept of ″open″ is being equated with patented technology that is ″free″ (without payment) or ″free to use freely″ (without payment and without any restrictions). These proposed re-definitions are being used to advocate policy changes that would undermine the rights of those who have invested in the development of the standardized technology.

While the notion of patents being ″free to use freely″ is superficially attractive, like most ″free″ things, it comes at a cost. Technological capabilities and innovations most often result from substantial investments in R&D. Such investments typically drive the growth of the investor's patent portfolio. If patent holders in standards-setting activities are expected to give away or waive their patent rights, there are likely to be significant adverse results including:

– Technology leaders will reduce or cease participation in (or technical contributions to) voluntary standards-related activities; or

– Individuals and organizations will not invest (or will invest less) in the development of innovative and next-generation technology in the technical areas subject to standardization, thereby creating innovation ″dead zones″ in those areas.

These types of adverse results would cause (a) the standardization system; (b) its open, voluntary and consensus-based process; and (c) ultimately the resulting Open Standards, to be less effective or successful than they are today. Moreover, TIA believes that these results would have a negative impact on global respect for intellectual property that helps stimulate innovation and develops local economies around the world.

In fact, true ″open standards″ are market-driven, and promote competition and innovation. Such standards are developed or ratified through a voluntary, open and consensus-based process. This process is defined by flexible policies that balance incentives to participate in and contribute to the formulation of standards. This process benefits users and consumers by the broad implementation of the resulting standards.

One element of a voluntary, open and consensus-based process addresses the inclusion of patented technologies. The patent policies of standards organizations typically find a balance among differing interests. For example, implementers need to access and use

patented technology included in the standard. Patent holders need to preserve their rights in a way that encourages them to contribute their innovative solutions to the standardization effort. Fair, reasonable, and non−discriminatory (FRAND) patent policies seek to provide this type of balance by helping to make that patented technology available to all on "reasonable and non-discriminatory" (i.e., FRAND) terms and conditions. This widely accepted definition of an "open standard" is reflected in the following:
− Global Standards Collaboration (GSC) − Resolution GSC-12/05: (Opening Session) Open Standards - www.gsc.etsi.org;
− ITU-T −http://www.itu.int/en/ITU−T/ipr/Pages/open.aspx; and
− American National Standards Institute (ANSI) − http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/Critical%20Issues%20Papers/Open−Stds.pdf.
For example, TIA supports the GSC Resolution that outlines the following elements of an "open standard":
− The standard is developed and/or approved, and maintained by a collaborative consensus-based process;
− Such process is transparent;
− Materially affected and interested parties are not excluded from such process;
− The standard is subject to RAND/FRAND Intellectual Property Right (IPR) policies which do not mandate, but may permit, at the option of the IPR holder, licensing essential intellectual property without compensation; and
− The standard is published and made available to the general public under reasonable terms (including for reasonable fee or for free).
Consistent with this voluntary, open and consensus-based process, globally recognized standards bodies like TIA, the International Organization for Standardization (ISO); the International Electrotechnical Commission (IEC); the International Telecommunication Union (ITU); the European Telecommunications Standards Institute (ETSI); and the Institute of Electrical and Electronics Engineers (IEEE); etc. all produce open standards that address many important ICT challenges in the marketplace while preserving incentives for further innovation and improvements over time.
Open standards enable interoperability, interworking and connectivity. There are varying types of open standards, ranging from those that specify network protocols and service interoperability to electrical connectivity to software and system interfaces. TIA's standards committees, for example, develop protocols and interface standards relating to fiber optics, public and private interworking, telco cable infrastructure, wireless and mobile communications, multimedia and voice over IP (VoIP) access, as well as healthcare ICT applications and vehicular telematics.

4. Security and resilience:

We appreciate that Ofcom must strike a delicate balance of numerous interests in addressing issues of network security in the IoT space. We urge that any regulatory efforts in this area be guided by the following principles: (1) that successful efforts to improve cybersecurity will leverage public−private partnerships to effectively collaborate on addressing current and emerging threats; (2) that greater cyber threat information sharing between the public and private sector should be enabled; (3) that policymakers and regulators should ensure that they address economic barriers for owners and operators of critical infrastructure in efforts to secure cyberspace; (4) that research funding for ICT and specifically cybersecurity research and development should be prioritized; (5) that the global nature of the ICT industry necessarily requires a global approach to addressing cybersecurity concerns.

TIA believes that market forces can create innovative security solutions. In order to address network security concerns, IoT devices can be made to work together to produce comprehensive, actionable security intelligence in near real-time. With this approach, an organization's overall security position can be increased with little or no human intervention required and it can also increase the intelligent independence of endpoints. Additionally, the IoT can be secured through industry-driven adoption of global best practices and standards. Country-specific standards should be avoided so that the technology is not inhibited in its development and global reach. Existing successful public-private partnerships can facilitate this approach and enable information sharing across companies and sectors.

In order to successfully address and support high levels of security for an IoT ecosystem, the nature of threats must be properly understood.

- Vast majority of cyber-attacks are caused by error, and addressed more slowly
- ~80% of all cyber breaches are due to poor cyber hygiene and are preventable
- Incidents of successful cyber-attacks in which the root cause is ultimately traceable to ICT equipment security vulnerabilities are extremely rare or non-existent

Also, approaches should distinguish between communications network security and end-user security because the risk profile varies greatly in these areas. The majority of cyber breaches that result in a data breach are targeted at individual or institutional end-users, not at communications networks themselves while communications network breaches are extremely rare and are addressed rapidly. Further, communications networks present a different risk profile than other types of infrastructure as successful cyber-attacks are quite unlikely to disrupt communications networks to the degree that public safety, health, widespread economic disruption, etc. would. Communications network failures caused by cyber-attacks can also be more easily mitigated against those failures than other types of infrastructure.

The ICT industry is global in nature with companies conducting different functions (manufacturing, R&D, services) across facilities in multiple countries. ICT products are often designed and built in different locations using globally-sourced components. Therefore, a global approach is required to address IoT security concerns.

5. Data privacy:

Ensuring strong privacy protections for consumers and industry is certainly one of the greater challenges for IoT technologies since the approach is one where data sharing is a necessity. We believe IoT can effectively address data privacy concerns by ensuring that the networks and communications protocols used are secure and resilient. Additionally, industry believes that any IoT services must be transparent about what data will be collected, how it will be used, and who will have access in order to allow the user to make an informed choice. We urge regulators not to adopt privacy regulations that would make it impossible for IoT systems to flourish. Instead, industry should be allowed to adopt best practices that allow individual users to manage their level of data sharing.

6. Numbering and addressing:

7. Devices:

Advances in sensor technology have dramatically reduced the cost of sensors. The increased availability of low-cost sensors will expand the potential market for M2M, as cost issues in installing sensors in devices are not expected to be significant. A major driver will be the development of standards that will pave the way for devices to connect to the network. Standards reduce costs because manufacturers and software developers can produce for multiple applications and multiple end uses allowing the benefits of economics of scale. The commoditization of standards-based M2M devices will increase market adoption. Meanwhile, expansion of LTE networks will reduce the cost of transmitting data, which should ultimately have a positive impact, as service costs should come down. Average monthly spending began to decrease in 2013 as advanced wireless networks reduced the cost of data transmission. We expect that trend to accelerate and project average monthly spending per device to drop from $7.90 in 2013 to $6.70 in 2017, a 4.0 percent decline compounded annually.

8. Digital literacy:

The ICT industry recognizes that the emerging IoT marketplace is a great opportunity for growth. This cannot be achieved without consumer buy-in and adoption of these new services. However, TIA does not believe there are glaring deficiencies in the approach currently being used by device manufacturers. By and large, the ICT manufacturer community is already conducting much of this outreach today to inform increasingly shorter product cycles as they compete in the global ICT market. In addition, since the penetration rate for mobile, wireless devices has grown, consumers are increasingly more aware of the enormous benefits and possible risks. To ensure awareness, application developers should continue to conduct outreach to consumers and use transparent policies that enable informed use. This is an area where government can also play a role by conducting marketing campaigns and providing tips to the public through consumer agencies.

9. Data analysis and exploitation:

The principal driver of the U.S. market is the soaring demand for data. Big data applications are propelling the data center and cloud computing markets. M2M facilitates the generation of data. LTE rollouts, the expansion of the fixed broadband infrastructure and ongoing deployment of fiber enable more data to be transmitted. Wireless penetration in the United States passed the 100 percent mark in 2012 and reached 105.2 percent in 2013.

Additionally, as we previously noted, consumers have readily embraced these new technologies and have been willing to share their data in order to get the lower cost, more efficient, and personalized service offerings. Mobile phones have become a major generator of data and mobile phone penetration is now greater than 100 percent. Big data enables the combination of disparate sources of information into a single database that allows LTE rollouts, the expansion of the fixed broadband infrastructure and ongoing deployment of fiber enable more data to be transmitted.

The key implications of the growth of ″big data″ systems that could inhibit growth have been identified by Ofcom in other sections of this request for input. The biggest factors will be network security, data privacy, and standardization.

10. International developments:

TIA expects the development of IoT to be driven by a global – not regional – approach that is based on the development of open, voluntary, and consensus-driven standards. Numerous standardization efforts already exist that will contribute to the development of an interoperable IoT resulting from healthy competition amongst these standardization efforts. TIA broadly supports the ″multiple path″ approach to the development of international standards. While some express the view that only certain standards bodies can produce ″international standards″ because they largely adhere to a national framework, TIA believes that any standard that is developed through an open, transparent process and is widely implemented on a global basis should be considered to be an international standard (1).

For example, the following organizations have existing efforts that will build towards the IoT:

- TIA
- Alliance for Telecommunications Industry Solutions (ATIS)
- oneM2M
- 3GPP
- IEEE
- Twenty Critical Security Controls
- Software Assurance Forum for Excellence in Code (SAFECode)
- Open Group Trusted Technology Forum (OTTF)
- IEC 62591 (WirelessHART)
- EPCglobal
- Global RFID Interoperability Forum for Standards (GRIFS)
- 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks)
- ROLL

(1) Based on lengthy experience in developing standards and knowledge of standards and patent policies globally, TIA has concluded that successful international standardization

policies are marked by certain general characteristics. While this is not an exhaustive list, these patent policies: (1) apply to those directly participating in the technical standardization, (2) balance the interests of all stakeholders, (3) permit patent holders to obtain a reasonable and non-discriminatory ("RAND") return on their innovation, (4) encourage bilateral negotiation of licensing terms between licensor and licensee outside of the standardization process; and, (5) provides for reciprocity when a license is offered to a licensee.

11. Ofcom's role :

We value the consideration Ofcom is giving to the newly emerging marketplace for IoT services and capabilities. The potential benefits IoT presents for to consumers, government, and industry in the form of greater efficiency, safety, and accuracy are infinite. The technology development for IoT, however, is still in the early phases and thus, innovation must be allowed to shape the direction of technology not rigid rules. Therefore, regulatory policies should focus on enhancing innovation and encouraging investment as this will be vital for this technology to develop and become widely available.

12. Additional comments:

Telit as a TIA member supports TIA inputs.