DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration
Docket No. 160331306-6306-01

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Comments of Ericsson

Kelley A. Shields
Director, Government Affairs and Public Policy

Jared M. Carlson
Vice President, Government Affairs and Public Policy, North America

Ericsson
1776 I St., N.W.
Suite 240
Washington, DC 20006
Telephone: (202) 824-0103

June 2, 2016

Executive Summary

In Ericsson's view, 5G is the technology that will unleash the true potential of the Internet of Things. To support the IoT's development, the government should unleash the resources that will ensure U.S. leadership in 5G by releasing more spectrum for commercial use.

Through network slicing, 5G technology will allow a single infrastructure to meet the very different needs of Massive and Critical IoT devices – it will enable networks to handle the incredible increase in data from the billions of low energy, low data devices, while also providing very high reliability, availability and security for critical uses.

We also encourage the government to support global standards and best practices and to allow industry to continue to innovate and coalesce around the most favorable IoT solutions. Industry is already tackling the difficult questions of interoperability, security and global standards that will be necessary for an internationally interconnected ecosystem.

Security can best be addressed by standardization bodies and through voluntary, collaborative industry efforts. Regulation may lock in outdated technology, pick technology winners and losers, and hinder innovation and efforts to globally harmonize. 5G security will safeguard confidentiality, incorporate integrity protection and ensure availability.

Intellectual property rights will play an important role in the success of the IoT. Ericsson has underlined its dedication to contribute to a successful and strong ecosystem by recently launching an IoT joint licensing platform. Our goal is to streamline licensing of standard essential patents to ensure innovative IoT companies continue to be rewarded fairly, while inspiring new IoT solutions and facilitating their market entry to the benefit of consumers and the IoT marketplace as a whole.

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration
Docket No. 160331306-6306-01

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Comments of Ericsson

Introduction

The Internet of Things will revolutionize the way mobile networks must function as billions of devices send and receive data, many of them wirelessly across 5G networks. By 2021, Ericsson forecasts there will be around 28 billion connected devices, 16 billion of which will be related to the IoT.[1] This will represent an enormous economic impact: potentially $1.9 trillion in global economic value-add through sales in 2020[2] and up to $11.1 trillion a year in global economic impact – equivalent to about 11 percent of the world economy – by 2025.[3]

We already see the IoT beginning to emerge on today's technology and existing infrastructure. For example, in Estonia, Ericsson already has deployed more than 630,000 remotely readable smart meters and integrated a central automatic meter reading system for data gathering for a major electricity distribution company. However, 5G is the technology that will unleash the true potential of IoT.

---

1 *See Ericsson Mobility Report*, June 2016 at 10, http://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

2 Press Release, Gartner, Gartner Says the Internet of Things Installed Base will Grow to 26 Billion Units by 2020 (Dec. 12, 2015), http://www.gartner.com/newsroom/id/2636073.

3 Jam Manyika et al., The Internet of Things: Mapping the Value Beyond the Hype, June 2015 at 2, *available at* http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

To support the IoT, networks will need to provide different functionalities for different IoT uses and 5G is how the mobile industry will meet this challenge. 5G networks will enable the carriage of data coming from billions of low-energy and low-data-usage connected devices, while also providing very high reliability and availability for critical IoT uses that will provide great value to society. Through network slicing, 5G will support different requirements for different industries, while allowing different sectors to maximize scale by using a common infrastructure. Industry is already tackling the difficult questions of interoperability, security and global standards that will be necessary for an internationally interconnected ecosystem.

In Ericsson's view, the most vital role for the government to play in supporting the IoT's development is to make spectrum available for 5G. We also encourage the government to support global best practices and to allow industry to continue to innovate and coalesce around the most favorable IoT solutions without the government preemptively picking technology or standards winners and losers.

I. The Mobile Network is the Foundation for the IoT.

A. IoT with Existing Infrastructure.

While it is the development and rollout of 5G that will allow for the true realization of the IoT, we are seeing the IoT emerge today on existing technology. Indeed, we have already built the world's largest IoT network: the mobile network, which provides global reach, reliability, quality of service and security, as well as flexibility and scalability.[4] Mobile networks have unmatched global coverage. Today, mobile networks already provide the foundation for a very wide range of IoT applications and M2M services. They cover 90% of the world's population

4 *See Accelerating IoT*, http://www.ericsson.com/ourportfolio/telecom-operators/accelerating-iot?nav=marketcategory002.

with over 230 million cellular M2M subscriptions,[5] which users trust to carry their private personal information and conduct business transactions.

Existing 3G and 4G cellular technology offers advanced functionality when it comes to quality of service and security, which will be increasingly important as more IoT devices connect to the network. LTE already has mechanisms to assign priority access to certain classes of devices to make sure that data gets through even in emergency situations where there may be network congestion. Security also is an integral part of 3GPP cellular standards and includes mutual authentication, signaling integrity and user data encryption of traffic for existing generations. As we discuss below in section IV, security is similarly being built into 5G standards.

B. 5G is the Future of IoT.

Looking into the near future, 5G will be the connectivity platform that fully enables the Internet of Things. The overall aim of 5G is to provide ubiquitous connectivity for any kind of device and any kind of application that may benefit from being connected. 5G networks will not be based on one specific radio-access technology. Rather, 5G is a portfolio of access and connectivity solutions addressing the demands and requirements of mobile communication beyond 2020.[6]

This is the ideal foundation for the IoT, as different IoT uses will require different functionalities from the network. The IoT will include both "Massive IoT" and "Critical IoT." For Massive IoT, networks must cost-effectively support an enormous number of IoT devices over a broad area, as these devices will be ubiquitous in every sphere of life. Most of these will

---

[5] *Id*.

[6] 5G can be considered an ecosystem of multiple different access technologies – cellular Wi-Fi, Bluetooth, proprietary radios, unlicensed and licensed spectrum, and more. These will carry a variety of data into the transport networks depending on the applications.

be sensors and actuators that consume low to moderate amounts of energy in order to sustain long battery life and that will not require low latency. We already have started exploring the possibilities with, for example, connected water (where sensors monitor water quality) and connected vineyards (where sensors measure many environmental factors to help vineyards improve their businesses).

By contrast, Critical IoT uses will require incredibly high network reliability and strong security, as well as ultra-low latency. These uses will provide profound value to society. For example, we will reduce traffic injuries and deaths and improve traffic flow with autonomously driving vehicles. We will enable doctors to perform surgery on patients in remote areas thousands of miles away. And we will see large machinery, such as mining vehicles, being sent hundreds of feet below ground and operated remotely by a person sitting safely above ground.

5G will provide a common infrastructure for these uses. This will stimulate new business models because different sectors will not need separate infrastructure investment, and it also will protect spectrum from fragmentation.[7] At the same time, 5G networks will be multi-purpose and will support different virtual networks with different characteristics through network slicing. Each network "slice" can support a different configuration of requirements and parameters, including security specifications, enabling a single infrastructure to support use cases with significantly varying requirements.

One good example of how network slicing could work in the IoT is the connected car. A self-driving vehicle will need to have a very reliable and secure connection, so one network slice could provide very low latency and high availability so it can make decisions in milliseconds. The same car can, at the same time, have a high-speed mobile broadband connection for its on-

---

7 Ericsson, *5G Radio Access* at 5 (April 2016) https://www.ericsson.com/res/docs/whitepapers/wp-5g.pdf at 5 ("Ericsson 5G White Paper")

board entertainment system run through a different network slice, to enable HD Video and music streaming services. Another slice of the network could be collecting other measurements from different devices inside the car that do not require constant supervision, such as servicing parameters that need to be transmitted back to the service center by the car's service date, perhaps once a year.[8]

II. The Government Can Best Support IoT Infrastructure by Facilitating Reallocation and Sharing of Underused Federal Spectrum and by Working to Identify new Spectrum for IMT at WRC-19.

NTIA can support IoT infrastructure by facilitating reallocation of underused federal spectrum for both exclusive commercial use and for sharing between government and commercial users. NTIA can also play a valuable role by advocating for globally harmonized spectrum for IMT at WRC-19. The broader federal government can continue to make spectrum available for commercial use for 5G deployment.

In order to support increased traffic capacity and to enable the transmission bandwidths needed to support very high data rates, 5G will extend the range of frequencies now used for mobile communication. This includes new spectrum below 6 GHz, as well as spectrum in higher frequency bands. [9] Spectrum allocations at lower bands will remain vital as the backbone for mobile-communication networks in the 5G era. High frequencies, especially those above 10 GHz, can serve as a complement to lower frequency bands and will provide additional system capacity and very wide transmission bandwidths for extreme data rates in dense deployments.[10]

---

8 Andres Torres, *Network Slices: The Best Thing since Sliced Bread* (Sep. 11, 2015), http://www.ericsson.com/spotlight/cloud/blog/2015/09/11/network-slices-best-thing-since-sliced-bread/.

9 Ericsson 5G White Paper at 6.

10 *Id*.

The ITU-R has identified candidate bands between 24-86 GHz to be considered for IMT at WRC-19.[11] The U.S. Government can play a crucial role in the IoT's emergence and growth by participating in the studies proposed by the WRC-15 on these bands[12] and by advocating to and working with other governments for WRC-19 to identify at least 10-12 MHz of spectrum for IMT from these bands, preferably harmonized globally.

The mobile industry is working to gain access to spectrum in the 6 GHz to 20 GHz range as well, but so far, regulators seem to be focused on higher frequency bands. Looking specifically at the U.S., the FCC's Spectrum Frontiers rulemaking is a positive step in providing for 5G spectrum needs that Ericsson strongly supports. It is, however, focused on those higher bands – 27.5-28.35 GHz, 38.6-40 GHz, 37-38.6 GHz, and 64-71 GHz. We do, however, expect the FCC to seek further comment in the near future on bands below 24 GHz that might be used for 5G services, and we likewise strongly support that effort.

The mobile industry will continue to need exclusively licensed spectrum but, sharing is becoming a necessity as we seek solutions to support increasing demands for services and traffic. Two examples of sharing arrangements include LSA planned in Europe for the 2.3 GHz band

---

11 *See* Resolution 238 (WRC-15), *Studies on frequency-related matters for International Mobile Telecommunications identification including possible additional allocations to the mobile services on a primary basis in portion(s) of the frequency range between 24.25 and 86 GHz for the future development of International Mobile Telecommunications for 2020 and beyond*, https://www.itu.int/dms_pub/itu-r/oth/0a/06/R0A0600006C0001PDFE.pdf. These bands include These bands include 24.25-27.5 GHz, 37-40.5 GHz, 42.5-43.5 GHz, 45.5-47 GHz, 47.2-50.2 GHz, 50.4-52.6 GHz, 66-76 GHz and 81-86 GHz, which have allocations to the mobile service on a primary basis; and 31.8-33.4 GHz, 40.5-42.5 GHz and 47-47.2 GHz, which may require additional allocations to the mobile service on a primary basis.

12 The ITU has formed a Task Group 5/1 to conduct the sharing and compatibility studies and report its findings to WRC-19. The first meeting of this Group was held 23-24 May 2016 in Geneva and a formal structure was established to implement the tasks accorded to it.

and the Citizens Band Radio Service for 3.5 GHz in the U.S.[13] Ericsson is very interested to see how the LSA/SAS models will work in practice and to what extent they can meet the needs for spectrum. We do not advocate for further adoption of these models without seeing them proven in practice however. It is exclusive, licensed spectrum that has helped to drive the mobile broadband revolution.

III. The Government should Support the Market Driven Process for developing IoT Technology Best Practices

IoT is a rapidly evolving area, with technology best practices for IoT being established simultaneously by standards bodies, industry alliances, and open source activities. We encourage NTIA not to endorse the views of any particular organization or alliance at this time, and we ask the government to support the market driven process. We do ask the U.S. Government to support policies that promote internationalization of IoT solutions and standards, as this is necessary for a globally-connected, interoperable IoT marketplace to emerge.

IoT standardization efforts are focusing on a set of main areas, including devices, service enablement, connectivity, data models and semantics, among others. 3GPP technologies, for example, are rapidly evolving with new functionality tailored towards the IoT, on both the network and device side. 3GPP has addressed reducing the cost of LTE devices by reducing peak rate, memory requirement and device complexity. 3GPP extended discontinuous reception (eDRX) functionality enables achieving more than 10-year battery life by allowing the device to remain in sleep mode when communication with the network is not needed. Now, 3GPP is defining narrowband IOT for low power LTE and other radio and core network technologies for M2M communications. Through 3GPP core network enhancements, a single LTE cell site can support millions of IoT devices.

---

[13] Ericsson 5G White Paper at 6.

The Internet Engineering Task Force (IETF) has already has spent a decade working on key IoT standards and guidance. The IETF has specified how the core protocol for IoT, the Internet Protocol version 6 (IPv6), can be used with many wireless and wired IoT communication technologies. Its ongoing work continues to cover even more technologies. More recently, a significant amount of IETF's IoT work has focused on security and how to make strong security mechanisms feasible on variety of constrained devices. IETF is also responsible for many key IoT application layer protocols, e.g., HTTP, HTTP/2, and the Constrained Application Protocol (CoAP).

Many other bodies are addressing factors that will enable the IoT. For instance, IEEE has incorporated IoT into a large number of standards, including in the 802 Standards Committee, which is tying IoT back to Ethernet[14] and Wi-Fi[15] and also dealing with networks for different deployments such as ZigBee and Wide Area Smart Grid Networks.[16] The Industrial Internet Consortium (IIC) is establishing solutions for how to build industrial IoT solutions by defining reference architecture. The Open Connectivity Foundation (OCF) is providing specification and has an open source project ensuring interoperability among consumers, business and industry. The Broadband Forum is driving residential and business broadband access, architecture, technology and requirements. The Open Mobile Alliance is establishing lightweight M2M specifications and ensuring interoperability at the application layers for provisioning, device management and software updates. The MEF is defining carrier Ethernet including service orchestration. Bluetooth SIG is defining Bluetooth Low Energy and Bluetooth Mesh and IP. The

---

[14] See IEEE Standard for Ethernet, IEEE 802.3.

[15] *See* IEEE Standard for Wireless Local Area Networks, IEEE 802.11.

[16] *See* IEEE Standard for Low-Rate Wireless Personal Area Networks, IEEE 802.15.4.

ITU-T Study Group 20 is working to define IoT technology deployment for smart cities, and security is a major item in their considerations.

The U.S. Government's most important role in this area is to support the industry-driven standardization and best practices process and, where it is involved in such bodies, work to prevent other governments from taking over the process. In such fora, the government can also work to support internationalization of IoT solutions and standards.

IV. Security can be Best Addressed by Standardization Bodies and through Voluntary, Collaborative Industry Efforts.

"The pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking."[17] While security is a very important consideration for the Internet of Things, regulation may lock in outdated technology, pick technology winners and losers, and hinder innovation and efforts to globally harmonize.

Security can best be addressed by standardization bodies and through voluntary, collaborative industry efforts. Ericsson encourages the federal government to continue to support voluntary and collaborative cyber risk management practices.[18] There are numerous efforts underway to address IoT security within multiple standards organizations, and government action at this time would likely interfere with this ongoing work.

To safeguard *confidentiality* in 5G networks, Ericsson strongly supports the use of standardized, publicly evaluated cryptographic data protection algorithms, wherever in the

---

[17] Tom Wheeler, Chairman, Federal Communication Commissions, Remarks at the American Enterprise Institute (June 12, 2014).

[18] *See, e.g.*, Admiral David Simpson, Chief, Federal Communication Commission Public Safety and Homeland Security Bureau, Remarks at the WTA – Advocates for Rural Broadband Spring Meeting Cybersecurity Panel (May 5, 2015), http://transition.fcc.gov/pshs/docs/speeches/DGS_WTA_051515.pdf (FCC has taken a "collaborative approach to cybersecurity, working in partnership with private-sector stakeholders" and the Commission "is using voluntary mechanisms to implement cyber risk management practices based on the 2014 NIST Cybersecurity Framework[.]").

network encryption is employed. Because we are seeing an increasing use of transport layer security, such as over Hypertext Transfer Protocol ("HTTP") within a connection encrypted by Transport Layer Security ("TLS") for Internet data traffic, some question if there needs to be any encryption of the data plane for 5G radio access. Ericsson believes that 5G standardization can provide a generic baseline of data protection (encryption and integrity) for the data plane, thereby adding security for 5G networks by not relying solely on the potential use of higher layer protection. This is already being considered in IoT enhancements for 2.5G standards. Standardization can also provide for encryption of the signaling plane, which carries sensitive data such as user identifiers.

As did earlier 3G and 4G standards, 5G standards will continue to incorporate *integrity* protection of the signaling control plane. Without integrity protection, denial-of-service and downgrade attacks would be relatively simple.

Ensuring *availability* of 5G networks will be one of the most important aspects for using 5G as the foundation for critical IoT and companies will need the flexibility to address this in as many ways as possible.

The main challenge as we embark upon the IoT is that networks can no longer assume all end-user devices are trustworthy, and therefore changes in the radio protocol design may be a key consideration to address this. Companies may provide 5G radio access using a device gateway architecture, in which connections of many devices would be aggregated at a gateway device. We anticipate this will be a common choice because very low cost devices will probably support other radio technologies, such as Bluetooth or ZigBee. In such cases, security functionality may be proxied by the gateway. Companies could also utilize network slicing to confine attacks to limited portions of the network.

Ericsson believes that the security design principles of previous cellular standards, such as the ability to provide mutual authentication and an encrypted connectivity service, will still apply for 5G. The migration from 3G to 4G and the concomitant placing of more data plane functionality at the network edge has also led to valuable insights that can be reused in 5G standards, such as requirements on secure environments in access points and backhaul security. Similarly, the wealth of experience protecting IP-based networks against attacks will likely be reused as design principles for 5G.

User privacy will be high on the agenda in 5G. We foresee that 5G standards will define more sophisticated privacy protections mechanisms in the radio access networks. In addition, access to services and data provided by connected IoT devices such cameras and various vehicle/public transport sensors require advanced access control and authorization mechanisms.

As noted above, we present this information to add to the government's holistic understanding of security that will impact the IoT, but we reiterate that the government should defer from regulation at this time.

V. Intellectual Property Rights will Play an Important Role in the IoT's Success.

Intellectual property rights will be an important factor in the development and success of the IoT market. A successful IoT ecosystem is dependent on adoption of standardized technology that can reach global scale. In order to allow for standardized solutions with broad industry support, and given the sophisticated technologies involved, intellectual property rights play an important role to fairly reward those companies investing proprietary technology and time in standards development while at the same time allowing fair, reasonable and non-discriminatory access to manufactures of IoT products.

Ericsson has underlined its dedication to contribute to a successful and strong ecosystem by recently launching an IoT joint licensing platform.[19] Our goal is to streamline licensing of standard essential patents to ensure that innovative IoT companies continue to be rewarded fairly, while inspiring new IoT solutions and facilitating their market entry to the benefit of consumers and the IoT marketplace as a whole. The IoT joint licensing platform will offer efficient aggregate access to multiple patent holders' standard essential patent portfolio by providing one predicable and simple licensing offer to IoT product companies. This will decrease transaction costs for both patent holders and IoT product companies using standardized technology.

Ericsson further believes that such IoT joint licensing platform can be an efficient market place for vertical IoT businesses' technology licensing needs, with flat per unit licensing fees for the various verticals that reflect how much of the connectivity technology a device uses. IoT product companies can incorporate years of R&D investment and innovation in their business models by getting access to and leveraging global networking technologies. This will enable them to reduce time to market and reach scale faster. Consumers, in turn, will benefit from a robustly competitive IoT product market.

Conclusion

Ericsson thanks the Department of Commerce for seeking input into how the government can best foster the advancement of the IoT. Ericsson encourages the federal government to support the IoT's development by releasing more spectrum for commercial use and by

[19] *See* Press Release, Ericsson, Ericsson establishes industry patent Licensing Platform for IoT, (Feb. 3, 2016), http://www.ericsson.com/thecompany/press/releases/2016/02/1983359; *see also* Rethink Wireless, *Ericsson sets up Patent Licensing Marketplace for Industrial IoT* (Feb. 8, 2016) http://rethink-wireless.com/2016/02/08/ericsson-sets-up-patent-licensing-marketplace-for-industrial-iot/.

advocating for more spectrum for IMT at WRC-19. We also encourage the government to support global standards and best practices and to allow industry to continue to innovate and coalesce around the most favorable IoT solutions, including for security. Finally, we remind the government that protecting intellectual property rights will be an important factor in the development and success of the IoT market.

Respectfully submitted,

ERICSSON

By: /s/ Kelley A. Shields
Kelley A. Shields
Director, Government Affairs and Public Policy

Jared M. Carlson
Vice President, Government Affairs and Public Policy, North America

Ericsson
1776 I St., N.W.
Suite 240
Washington, DC 20006
Telephone: (202) 824-0103

June 2, 2016