OECD publishing

OECD DIGITAL ECONOMY PAPERS
No. 252

THE INTERNET OF THINGS

SEIZING THE BENEFITS AND ADDRESSING THE CHALLENGES

2016 MINISTERIAL MEETING ON THE DIGITAL ECONOMY

BACKGROUND REPORT



2016 MINISTERIAL MEETING
THE DIGITAL ECONOMY:
INNOVATION, GROWTH
AND SOCIAL PROSPERITY

OECD
BETTER POLICIES FOR BETTER LIVES

FOREWORD

This report was prepared as part of the documentation for Panel 2.2 of the OECD Ministerial Meeting on the Digital Economy, "Tomorrow's Internet of Things". It provides information and discussion on the opportunities and challenges around this emerging set of technologies.

Preparation of the document was undertaken by Gaël Hernández, OECD, with the support of an expert group from Canada, the European Commission, Germany, Korea and the United States. We would like to thank, in particular, Julia Marquier, Nae-Chan Lee, Young-gyun Jeon, Achilleas Kemos and Rudolf van der Berg for their contributions together with delegates from the Working Party on Communication Infrastructure and Services Policy and the Working Party on Security and Privacy on the Digital Economy.

This report was approved and declassified by the Committee on Digital Economy Policy on 13 May 2016 and prepared for publication by the OECD Secretariat.

Note to Delegations:
This document is also available on OLIS under reference code:
DSTI/ICCP/CISP(2015)3/FINAL.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

© OECD (2016)

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for commercial use and translation rights should be submitted to rights@oecd.org.

TABLE OF CONTENTS

FOREWORD 2
EXECUTIVE SUMMARY 4
INTRODUCTION 7
SECTION I: THE INTERNET OF THINGS, AN EMERGING PLATFORM FOR INNOVATION 8
SECTION II: SEIZING THE BENEFITS OF THE IOT 11
Benefits of the IoT 11
Facilitating private sector innovation with the IoT 11
Facilitating innovative public sector delivery with the IoT 13
Challenges relating to the deployment of the IoT 17
Digital security and privacy risks 17
Interoperability of technologies and policy frameworks 24
Investment 25
Jobs and skills 25
SECTION III: AREAS FOR STAKEHOLDER ACTION 27
Evaluate and assess existing policies 27
Promote the use of global technical standards 28
Evaluate spectrum resources to satisfy IoT needs 30
Adapt research and innovation policies 33
Encourage private sector innovation 35
Promote skills needed to maximise opportunities in the labour market 36
Build trust in the IoT 36
Further develop open data frameworks 38
Consider adapting numbering policies to foster competition and innovation 40
IPv6 as a fundamental enabler for the IoT 40
Telephone numbers for the IoT 41
Solutions to facilitate provider switching and avoid lock-in 42
Extra-territorial use of numbers 43
NOTES 45
REFERENCES 51

EXECUTIVE SUMMARY

The Internet of Things (IoT) could soon be as commonplace as electricity in the everyday lives of people in OECD countries. As such, it will play a fundamental role in economic and social development in ways that would have been challenging to predict as recently as two or three decades ago. IoT refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. Important IoT application domains span almost all major economic sectors: health, education, agriculture, transportation, manufacturing, electric grids, and many more. Proponents of IoT techniques see a world in which a bridge's structural weaknesses are detected before it collapses, in which intelligent transportation and resilient electrical grids offer pleasant and efficient cities for people to live and work in, and in which IoT-supported e-applications transform medicine, education, and business.

The combination of network connectivity, widespread sensor placement, and sophisticated data analysis techniques now enables applications to aggregate and act on large amounts of data generated by IoT devices in homes, public spaces, industry and the natural world. This aggregated data can drive innovation, research, and marketing, as well as optimise the services that generated it. IoT techniques will effect large-scale change in how people live and work. A thing in IoT can be an inanimate object that has been digitised or fitted with digital technology, interconnected machines or even, in the case of health and fitness, people's bodies. Such data can then be used to analyse patterns, to anticipate changes and to alter an object or environment to realise the desired outcome, often autonomously.

More generally, the IoT allows for tailored solutions, both in terms of production and services, in all industry areas. For example, insights provided by IoT data analytics can enable targeted medical treatment or can determine what the lot-size for certain products should be, effectively enabling the adaptation of production processes as required. In the context of manufacturing this would enable greater use of customised outcomes rather than trying to predict mass market demand. The IoT can also empower people in ways that would otherwise not be possible, for example by enabling independence for people with disabilities and specific needs, in an area such as transport, or helping meet the challenges associated with an ageing society. Those countries that anticipate the challenges while fostering greater use will be best placed to seize the benefits.

The incorporation of the IoT into people's lives will require evaluating implications for their safety and privacy, including the security of their personal information and the development of appropriate safeguards. Appropriate legal privacy and consumer protection frameworks will be fundamental enablers of acceptance and trust.

The IoT promises to enable firms and public authorities to meet their objectives in new and innovative ways. The IoT is already empowering people to interact with technology and improve their lives. All stakeholders can only gain from sharing good practices to harness the benefits of the IoT while addressing the related challenges. Significantly, this will be in an environment of rapid commercial, technological and social change around the potential of the IoT. Accordingly, principles such as flexibility, transparency, equity, and, to the extent possible, farsightedness will be critical to avoid barriers to the diffusion of the technology.

The IoT will place different demands on communication infrastructures and services. Underlying these developments will be policies that promote the availability, quality and use of such infrastructures and services. In this regard, international governance and norms may need to be reviewed to ensure the performance and security of communication networks and services and thus contribute to building trust in the IoT.

With this in mind, this paper highlights good practices to help policy makers move ahead and promote the positive elements of the IoT while minimising challenges and ensuring broader goals, including the following:

- **Encourage private sector innovation** taking advantage of the IoT and improve the conditions for the creation of new firms and business models that are built around the opportunities created by the IoT. In some cases, value chains could leverage the IoT opportunities across firms and cost sharing could create multiplier effects. For example: the IoT allows firms to more widely deploy service-based business models. Enterprises both small and large will increasingly lease their product and compete on the total cost of ownership, instead of on the initial purchase cost.

- **Adapt research and innovation policies** across a broad range of sectors and applications so that the IoT is a prioritised part of the overall research effort, including by providing funding. This will, for example, help measure and evaluate progress so that policies are adapted to current and future IoT developments. While gains from improvements in the base components of IoT, such as better M2M communications, data processing, sensors and actuators will be visible and measurable, the measurement of returns to investment in innovation, application and integration of IoT is, as with many emerging research topics, more challenging.

- **Evaluate and assess existing policies and practices** to see if they are suitably supportive of the IoT, and do not constitute unintentional barriers to potential IoT benefits. There may be a need to consider adaptation of existing regulations and practices if they are based on assumptions that may inhibit the application of the IoT. For example: health care rules that reimburse medical practitioners for a physical visit or require a physical signature might need to be reviewed in the light of the use of remote monitoring and treatment.

- **Promote the use of global technical standards for the IoT** developed by standards setting bodies or industry consortia. Standardisation plays a key role in the development of an interoperable IoT ecosystem, and is essential for stimulating the emergence of new systems, boosting innovation and reinforcing competitiveness. Over time, technological maturity and end-user choice will ultimately identify the most promising standardisation approaches.

- **Evaluate spectrum resources to satisfy IoT needs**, both current and future. Different elements of the IoT, from machines to sensors, need a variety of spectrum resources that is fit for purpose. Relevant authorities should assess future demands for spectrum and review the mechanisms by which spectrum could be made available for a range of uses, including for the IoT.

- **Promote skills to maximise opportunities in the labour market** and support workers whose tasks become displaced by IoT-enabled and robotic machines and systems, with adjustment assistance and re-skilling programmes. For example: new jobs in IoT-related services will be created, e.g. in data analytics, while existing tasks may be enhanced through the availability of new tools. In an area such as warehousing, the IoT may improve the quality of jobs, though fewer employees may be required in increasingly "roboticised facilities".

- **Build trust in the IoT** by managing digital security and privacy risks in line with the OECD 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* and OECD Privacy Guidelines. Trust would benefit from increased cross-border and cross-sector interoperability of policy frameworks, particularly for IoT products in the consumer market. Privacy, security, liability, consumer protection and safety are affected by the pervasiveness and longevity of the IoT. Governments could encourage further dialogue across regulatory agencies and with industries that traditionally were not closely involved in communications, such as transportation or utility services. For example: what rights or controls should a consumer be able to exercise over data collected by a connected automobile or a smart-meter and what is a satisfactory level of granularity for rights or controls?

- **Further develop open data frameworks** that enable the reuse of government data sets and encourage industry to share their non-sensitive data for public benefit. This could require updating the roles and processes of public authorities and the infrastructures they administer to make use of the IoT. For example: transportation companies could benefit from real-time data on road conditions, but can also report such data back to the drivers of road maintenance machines as well as those responsible for maintaining such infrastructures. In urban planning, for instance, connecting traffic lights could optimise traffic flow across a city. These efforts should take into consideration the security and privacy challenges that may arise.

- **Flexibility is essential for numbering** as different services or M2M users may have different requirements. Industry makes use of national numbers in an extra-territorial way (e.g. extra-territorial use of national numbers) as well as of international numbers in order to deploy IoT connected services. Furthermore, regulators should carefully assess introducing additional, and remove existing, restrictions or administrative barriers related to the assignment and use of numbering resources, as it could act as a barrier to the roll-out of a global M2M market.

- **Stimulate the deployment of IPv6 as an enabler to the IoT.** With the current address depletion scenario, deployment of IPv6 is inevitable and promoting the IPv6 transition is the most effective way to support the IoT. Many governments have already established promotion programmes, adapted government purchasing and established task forces with industry to further accelerate IPv6 support to the IoT.

INTRODUCTION

This document examines the current state of the Internet of Things (IoT) and identifies a set of areas for stakeholder engagement specifically designed to facilitate its deployment by all stakeholders and particularly for the private sector.

In this document, the IoT is considered both as an evolving technology, and also as an emerging catalyst for innovation. The form of the innovation, the sector in which it is applied and the potential benefits achieved depend to a large extent on the capacity of innovators to conceive and implement novel IoT approaches and on the capacity of governments to create policy and regulatory frameworks in key areas including telecommunications, privacy, security and consumer policy. Member countries can benefit from understanding best practices and policy approaches in the emerging IoT environment.

Further work on this topic by the OECD could deepen analysis of IoT technologies, applications, products and services and highlight their economic and social effects on market structures, regulation and behaviours. Several specific areas of interest arise: helping policy makers in further understanding any need to adjust policy and regulatory frameworks to tackle technical barriers; analysing initiatives and policy approaches linking the IoT to data-driven innovation; and developing metrics necessary to measure the effects of the adoption of IoT solutions in areas such as economic growth, employment and education needs, analysing privacy and security implications, or consumer protection.

The document is organised in three main sections. Part I introduces the building blocks of the IoT as an emerging platform for innovation and situates it among other ICT trends. Part II discusses the benefits and associated risks of introducing IoT techniques and methods in several industries and sectors. This part highlights the positive aspects for both the private and public sectors and presents several risks that are today preventing its widespread adoption. Part III focuses on what actions could be taken to facilitate the deployment of IoT techniques and processes. This part identifies a number of policy areas in which different stakeholders have an active role to play and provides a roadmap of actions that can facilitate its implementation.

SECTION I: THE INTERNET OF THINGS, AN EMERGING PLATFORM FOR INNOVATION

IoT refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. In the Internet of Things, devices and objects have communication connectivity, either a direct connection to the internet or mediated through local or wide area networks. In addition to IoT, another related topic is Machine to Machine (M2M) communications, most notably characterised by autonomous data communication with little or no human interaction between devices and applications[1]. In that case, M2M would not require human mediation because intelligence is built into the system to facilitate automated decision and action. The broader concept of IoT may include sensors just providing information for use in other systems. A number of other terms are also evolving which has led some to coin the term Internet of Everything. In some ways, the term Internet of Everything is the most accurate, as the Internet-connected sensors and actuators are not just linked to things, but also monitor health, location and activities of people and animals, monitor the state of the natural environment, the quality of food and much else that would not be considered a thing per se.

IoT exists as part of an emerging technology ecosystem with cloud and big data analytics. Interactions occur among and between people and objects in computer aware environments that can avail themselves of new and innovative services delivered through the cloud and supported by an ever more powerful set of analytical tools. Sophisticated data analysis techniques will enable applications to aggregate and act on large amounts of data generated by devices in homes, public spaces, industry, and the natural world. This aggregated data can drive innovation, research, and marketing, as well as optimise the services that generated it. The ecosystem must be considered to be an overlapping continuum where it is impossible to isolate the impacts of one technology from the others. To that end, the policy issues should consider and address the ecosystem impacts.

Visions of smart, communicating objects are not new, and were imagined well before the World Wide Web, for example, became commonplace.[2] By the early 1990s, ideas about ubiquitous or pervasive computing and embodied "virtuality" were well advanced at Xerox PARC, where they imagined that "specialised elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence."[3] Similarly these concepts were being raised in APEC by both Japan and Korea in the late 1990s and early 2000s under the term U-Computing. Still, the consumer products that many have envisaged for the IoT have been a long time coming. Even today, as more and more IoT products reach the stores, their manufacturers are still not entirely sure what features may be those that will attract consumers (Harwell, 2014). By way of example, there are now websites dedicated to collecting unexpected "smart" devices from toothbrushes and baby pacifiers through to luggage and all manner of devices found in kitchens to bedrooms.[4]

As an event and outcome driven technology, IoT could drive consumer demand. The current outlook is positive, with some studies projecting more than threefold growth on the number of global M2M connections, from 3.3 billion in 2014 to 10.5 billion by 2019.[5]

The IoT is still evolving, and is at a similar stage as the World Wide Web two decades ago as it was emerging to become a commercial network, when there was considerable diversity in experimentation across industries, with competing standards and unclear expectations from consumers. The wireless capabilities of smartphones, from NFC to low energy Bluetooth, and their pervasive adoption in such a short timeframe mean that the devices to read and interact with the IoT are available at scale for the first time. Many IoT applications and techniques will be in manufacturing and industrial settings. In the subset of IoTs that are consumer-facing, smartphones play an important role in bringing the IoT to the consumer (Yared, 2013).

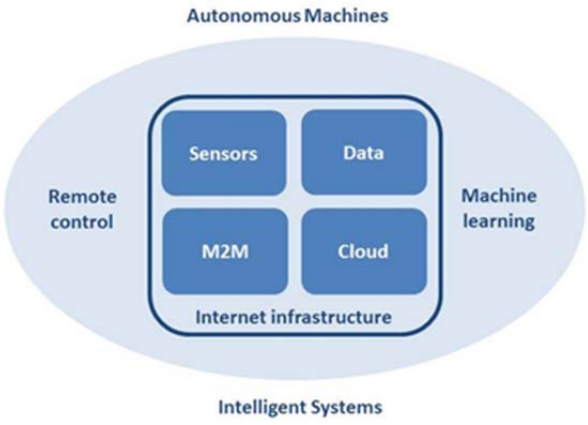
A definition of IoT is not a simple matter. In a previous report (OECD, 2011) the term IoT was said to be mainly associated with applications that involve RFID. In that report the term M2M was used for:

> "Devices that are actively communicating using wired and wireless networks, that are not computers in the traditional sense and are using the Internet in some form or another. M2M communication is only one element of smart meters, cities and lighting. It is when it is combined with the logic of cloud services, remote operation and interaction that these types of applications become "smart". RFID can be another element of a smarter environment that can be used in conjunction with M2M communication and cloud services."

Since 2011, the term IoT has gained prominence to describe a wider variety of developments where "things" are connected to the Internet. Traditional M2M solutions typically rely on point-to-point communications performing actions without the manual assistance of human interaction using embedded hardware modules and either cellular or wired networks. In contrast, IoT solutions rely directly or indirectly on IP-based networks to interface device (object or things) data to a cloud or middleware platform.

Four main elements can be seen as underpinning the development of the IoT –data analytics, cloud computing, data communication and sensors or actuators (Figure 1). Cloud computing and data analytics include improved machine learning applications, operating at a new level of artificial intelligence. IoT also incorporates the notion of sensing and data analysis driving remote control. For example, a smart transportation scenario might include sensing and analysis of a city's current traffic flow, followed by control responses to adjust traffic stop lights or congestion tolls. In the case of remote control, human interaction may still be needed, but is typically limited to very specific actions. The combination of remote sensing and actuation, along with advanced machine learning will lead to the development of autonomous machines and intelligent systems, including robots.

Figure 1. The IoT ecosystem: enablers and applications

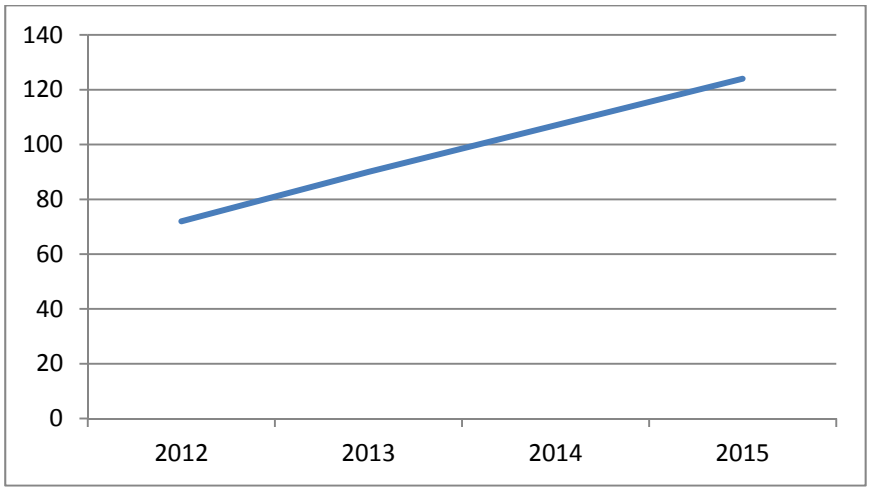


The contributions of sensors and actuators to "Green Growth" were considered in a previous report (OECD, 2010). It stated that sensors measure multiple physical properties and include electronic sensors (accelerometers, hygrometer and so forth), biosensors, and chemical sensors. These sensors can be regarded as "the interface between the physical world and the world of electrical devices, such as computers".[6] The counterpart is represented by actuators that function the other way round, i.e. whose tasks consist in converting the electrical signal into a physical phenomenon (e.g. displays for quantity measures by sensors such as speedometers, temperature reading for thermostats, but also those that control the motion of a machine).

In early sensor and actuator systems, such as a vehicle engine, the data were measured, processed, and acted upon largely in isolation, and then discarded. Today, however, more and more of the data generated is communicated to other machines for storage and for integration and analysis with other data, potentially from very different types of sensors. This cross-analysis of data can usefully integrate together data from different types of sensors using advanced machine learning techniques to support sophisticated cross-analysis. The type of communication used can be varied – wired and wireless, short or long range, low or high power, low or high bandwidth. Many of these options are discussed in (OECD, 2012a) and (OECD, 2013) and this paper will not repeat an examination of the various networks that could be used but offer suggestions for reviewing current telecommunication policies, which assume prior knowledge of the types of networks used.

An important aspect in the development of the IoT is the ability to create "big data" ecosystems, potentially increasing the value of the service provided. For example, a smartphone application could empower individuals with a specific allergy, to provide information on symptoms as they move across different locations. Correlating thousands of geotagged datasets with environmental sensors could alert residents of high risk areas in real time. Alternatively, the allergy data could be correlated with socio-economic data producing maps for health and urban planning authorities. Collecting, compiling, linking and analysing very large data flows in real time requires powerful data analytics techniques, which can be provided by cloud computing platforms in a flexible, elastic and on-demand way with low-management effort.

Figure 2. M2M SIM card subscriptions in the OECD area, millions



Note: The data are estimates. 2015 data are estimates from June 2015. There are 4 countries in the OECD area for which data are not available.

Measuring the growth of the Internet of Things is not a simple task because the IoT does not have clear boundaries. Several alternatives can be used, such as the number of sensors per device, communication chips or the number of M2M SIM card subscriptions. That being said, there are other difficulties, such as counting sensors/devices deployed by private firms inside corporate networks or manufacturing plants. Efforts to develop metrics are still in their infancy but the OECD has explored several proxy measurements (OECD, 2015). One of the most accurate measurements though not complete, is the number of M2M subscriptions[7]. The OECD has collected data from regulatory authorities since 2012. This enables the number of M2M SIM subscriptions observed in the OECD area to be tracked and in that time they have grown from 72 to 124 million (Figure 2). Examples of use cases for such subscriptions are smart-meters, points of sale and connected cars among others.

SECTION II: SEIZING THE BENEFITS OF THE IOT

Benefits of the IoT

Facilitating private sector innovation with the IoT

IoT techniques support a wide range of innovative businesses. In addition to using IoT approaches to build applications for smart transportation, health, and other sectors, IoT techniques may also support more responsive business models in which more granular and frequent data reported by IoT services will allow businesses to better assess how their customers use their products. In turn, firms could offer tailored solutions to their customers while contracts between supplier and customer could be dynamically adapted so that the actual functioning of the service is the main focus for any business. While such transformations have been on-going for several decades, IoT techniques can accelerate this process.

Using IoT approaches also allows firms to fundamentally integrate sensing, analytics, and automated control into business models. Some firms have called it the 'Industrial Internet' and have estimated gains of USD 10-15 trillion to global GDP over the next 20 years.[8] Moving towards equipping machines with a range of sensors in order to be able to do predictive maintenance, firms are improving processes, becoming smart and more efficient. The effects do not have to be large to be noticeable: a 1% efficiency increase in the aviation industry could, for example, save commercial airlines globally USD 2 billion per year.[9] According to a study by a network operator, the average cost saving for industry in general is 18%, and nearly 10% of M2M adopters have reduced their costs by over 25% (Vodafone, 2015). Apart from cost savings, firms mention the following areas where improvements can be identified after adoption of IoT-measures: processes and productivity; customer service, speed and agility of decision-making; competitive advantage; innovation; consistent delivery across markets; sustainability; transparency/predictability of costs; revenue; and performance in new markets (Vodafone, 2015). A report of a stakeholder organisation states that in 2020 benefits of the IoT could be at USD 2 trillion, where USD 1 trillion could be based on cost reductions (e.g. by increasing energy efficiency using smart meters in large quantities - analysts forecast that 1.1 billion smart meters could be in use in 2022 (Navigant Research, 2013)) and another USD 1 trillion could come from improved services such as remote monitoring of chronically ill patients (GSMA, 2014). These figures are outnumbered by an analysis which predicts that for the car industry alone annual global savings of over USD 5.6 trillion could be achieved by cars based on advanced connectivity technology such as semi-autonomous and autonomous cars (Morgan Stanley, 2015).

The IoT might facilitate the so-called "next production revolution" (NPR). Three key trends – the spread of global value chains (GVCs), the increasing importance and mainstreaming of knowledge-based capital, i.e. software, data, intellectual property, firm-specific skills and organisational capital, and the rise of the digital economy – have been identified as ushering in the NPR (OECD, Forthcoming). This implies a potential step-change in the way goods and services are produced at the global level, with many possibly disruptive IoT technologies holding the promise of higher productivity, greener production, and new products, services and business models that could help meet global challenges. At the same time, these technological changes could contribute to shifts in global value chains, as reshoring to advanced economies might become more attractive as labour cost advantages diminish.

Already warehouses are becoming increasingly robotic. Today, manufacturing largely limits its reliance on robots to well-defined, carefully programmed areas, such as making automobiles but could

expand to consumer electronics if more flexible reprogrammable robots can be built. Hon Hai Precision Industry, a multinational electronics contract manufacturing company employing over 1.2 million people and best known for assembling Apple's devices, has stated that it is looking into deploying over one million robots in its business in the coming years. Substantial changes are also in the process of being deployed in the areas of product storage and distribution related to employing IoT in the design and operation of warehouses. Modern warehouses use digital technologies such as barcodes to direct human workers to what shelves to visit and what items to pick. Other warehouses use conveyer belts for workers to put products on and these employees are directed by computers as to the tasks they undertake. In Amazon's warehouses, for instance, shelves are transported by small self-driving robots, so that employees are stationary and the position of the shelves is dynamic.

Optimised warehouses will need fewer human workers to handle the same amount of orders. The Baxter Research Robot is an open source platform enabling researchers to customise a range of applications for robots and drive robotics innovation.[10] For the immediate future, people will still be needed for maintenance, quality control, training robots and many other aspects of production processes. Combined with robotic advances in manufacturing, it might lead one day to a fully automated production process from design to delivery (Box 1). New tasks could offer more job satisfaction as opposed to the current repetitive nature of some tasks, even though in some sectors a net loss of jobs might be possible.

Autonomous machines and the use of big data are increasingly present in agriculture. Robots can now sort plants based on optical recognition, harvest lettuce and recognise rotten apples. Tractors are being used today that steer themselves and only need minimal operator intervention to spray fields as they use algorithms to vary the spraying of pesticide and fertiliser based on yield data from previous years. Combine harvesters are also able to operate semi-autonomously or work together with a lead-harvester. Sensor-equipped machinery can independently improve working processes and inject real-time data on Internet platforms during the working process. When all units involved in the harvesting process are networked, they can exchange data and coordinate the current harvesting process among themselves.[11] In today's world, even cows are often autonomously milked using sensor-based IoT systems (McKinley, 2014). Robots clean the stables and ensure that grass for feed is pushed back to the cows, so that it does not get wasted.[12] While robotics and IoT techniques are distinct, they overlap in the sense that cloud-connected autonomous robots can be viewed as IoT sensors or actuators in large, distributed, intelligent systems.

The automotive industry is one of the sectors most affected by interconnectivity and enhanced efficiency in both production and operation of vehicles. In this respect, the development of highly automated and connected vehicles is at the forefront. Recent studies illustrate that automated and connected driving will dramatically change the global automotive market during the next two decades. While only tens of millions of cars are said to be connected to the Internet today, this is expected to become hundreds of millions in the near future (T-Systems, 2015). Meanwhile companies from PricewaterhouseCoopers to CISCO expect that both the market and market share of automated/autonomous cars will rise sharply in the coming decades (e.g. for CISCO from 0.1% in 2020 to over 35% in 2040) (PricewaterhouseCoopers, 2014).

Box 1. IoT and the "next production revolution" (NPR)

The recent productivity slowdown has sparked interest among academics and policy makers alike, with the debate centering on the extent to which the slowdown is temporary or a sign of more permanent things to come. Productivity (principally labour productivity) drives the large differences in income per capita currently observed across countries and it is expected to be the main driver of economic growth and well-being over the next 50 years (OECD, forthcoming d).

The spread of global value chains (GVCs), the increasing importance and mainstreaming of knowledge-based capital and the rise of the digital economy are ushering in the "next production revolution". Countries need to seize this opportunity to harness innovation to boost economic growth and spur job creation. In the near future, maybe as early as 2025, the process of manufacturing could become an almost completely autonomous activity with little human interaction. Though hypothetical and stylised, the process could work along the lines of the following example:

In 2025, a group of designers have created a new device. They showed a number of 3D printed prototypes to potential buyers and, as a result, received a contract from a retailer in a different country. The design, packaging and component list is uploaded to an online marketplace where manufacturers compete against each other for the contracts to create the parts and assemble the device. One contractor wins the contract to assemble the device. This contractor uses a cloud-based computer-aided design tools to simulate the design and manufacturing of the device. Machine learning algorithms test which combination of robots and tools is the most efficient in assembling the device which may lead to further optimisations of the product. Some components, such as systems-on-a-chip and sensors, can be sourced from manufacturers. Other elements have to be specifically created for the device. Specialist manufacturers that 3D-print the initial molds for the design and then mass-produce the elements using a variety of technologies to produce these elements. Robotic devices execute mass production of the components.

All the components and the associated data are then sent to the assembly facility. On the assembly line, the robots in the line retool and arrange themselves. Robotic vehicles move the components across the floor to the correct robot workstations and the robots start assembling the devices. Every time the robots assemble a device, the machine learning algorithms in the cloud analyse the sensor data and compare this to the simulations, re-simulate and establish whether the process still fits the parameters and whether the process can be optimised. If something goes wrong in the process, the machines can work around the problem, based on what is necessary. The finished product is packaged by a robot and put into a box, which is loaded by a further robot onto a pallet and then loaded by another robot on a self-driving truck, which takes it to the retailer.

At the retailer, robots unload the truck, move the product in the warehouse and then place it in the correct storage location. When the product is ordered another robot picks it up, delivers it to picking and packaging, where robots pick and package the widget and send it to a robot that puts the package on a self-driving truck. The truck is equipped with a smaller delivery robot that carries the product to the front-door of the customer.

In this hypothetical example, the sales of the product prove much better than expected with orders increasing around the world. The designers need more production capacity and again turn to the market, where manufacturers in the regions where the product has been ordered, compete for larger or smaller batches of the product. The results of the earlier machine learning algorithms are communicated to the factories around the world, where different robots, with similar functionalities assess how to manufacture the product in the factory. When a factory is done with the batch of widgets that it was hired to do, the robots reorganise and retool for a different product, until another batch of the widget is demanded.

From the moment the design was finalised until it arrives at the customer, no worker has been employed to manufacture the device. There were employees monitoring the manufacturing process. However neither in the plastics molding nor the assembly nor the logistics surrounding the device were humans necessary.

Facilitating innovative public sector delivery with the IoT

Public authorities have a number of roles, processes and infrastructures that they need to execute and maintain, including: roads and public spaces, emergency services, and safety and security. In many countries, they are either directly or indirectly responsible for health care, energy provision, public transport, garbage collection and sewage. These roles can be made more efficient by the IoT and authorities should actively investigate how the IoT can help them better achieve their objectives and measure the effectiveness of their policies and implementation. According to Cisco forecasts, the economic

opportunity of the implementation of IoT in the European public sector is USD 2.1 trillion (Pepper, 2015). As a comparison, the estimation for the private sector is USD 4.3 trillion.

Innovation in healthcare practice and delivery

Health systems today are predominantly facing chronic diseases instead of acute care. In the introduction of the OECD publication '*Health Reform, Meeting the Challenge of Ageing and Multiple Morbidities*" it is stated that:

> "*When the OECD was founded in 1961, health systems were gearing themselves up to deliver acute care interventions. Sick people were to be cured in hospitals, then sent on their way again. Medical training was focused on hospitals; innovation was to develop new interventions; payment systems were centred on single episodes of care. Health systems have delivered big improvements in health since then, but they can be slow to adapt to new challenges. In particular, these days, the overwhelming burden of disease is chronic, for which 'cure' is out of our reach. Health policies have changed to some extent in response, though perhaps not enough. But the challenge of the future is that the typical recipient of health care will be aged and will have multiple morbidities."* (OECD, 2011)

According to the publication, this calls for an approach to health care that focuses on prevention and disease management, because the causes and effects of the disease can be the result of life style choices and environment. The role of a medical practitioner has been changing from being primarily a healer to placing more emphasis on advice in managing cause and effect because of the new tools available.

The IoT can support changes in the delivery of healthcare. Smaller sensors, smartphone assisted read-outs, big data analysis and continuous remote monitoring can enable new ways of managing care. Sensors now exist that can be swallowed with a pill and are being used to improve the accuracy of clinical trials by monitoring and managing participants' use of medication (Box 2).[13] Such a digital health feedback system includes wearable and ingestible sensors that work together to gather information about medication-taking, activity and rest patterns. Weight management can benefit too from regular monitoring.[14] Other devices can measure the amount of sleep a person has over time, activity and blood pressure, glucose levels and heart rate, which are the types of measures medical practitioners need to monitor their patients.

Implementing these new technologies in a health system may be challenging. The health management chain, as well as regulation in this sector, may need to be adapted to take advantage of the potential benefits. One example might be to switch from reimbursement for physical visits to payments for packages of treatments.[15]

Box 2. Digital Health Feedback System and Anonymised Big Data Analytics

The ingestible sensor technology is made entirely of ingredients found in food and activated upon ingestion. Patients take it alongside their medications, capturing the exact time of ingestion. The patient's own body powers the ingestible sensor. With no battery and no antenna, their stomach fluids complete the power source and their body transmits the unique number generated by the sensor. The patch, body-worn and disposable, captures and relays their body's physiologic responses and behaviours. It receives information from the ingestible sensor, detects heart rate, activity, and rest, and sends information to the patient's mobile device. Using a Bluetooth-enabled device a patient can access secure applications that display their data in context and support care in a variety of different ways.

In the United States, for example, asthma and chronic obstructive pulmonary disease (COPD) are said to be the 5th and 6th most costly conditions estimated at USD 50 billion annually, each. Improved self-management through use of the IoT could reduce the cost of treating them by eliminating unnecessary hospitalisations or other medical visits. Also, by gathering information on the symptoms, triggers and use of medications and making that information readily available on devices such as smart-phones, patients can be better informed for their own action as well as communicating this information to caregivers and clinicians.

By providing direct and rapid validation of the quantity of medication a patient ingests and the time of ingestion, the information can help lower the risk of clinical trial failures by identifying medication adherence issues early, improving dosage decisions, and enhancing drug safety.

The benefits of taking advantage of 'big data' related to the use of IoT in healthcare could be substantial. Information on health issues and diseases could be used on an anonymised basis in order to draw conclusions in relation to disease prevention, forecasts of epidemics, customised treatments and locations where a certain disease is more widespread, which in turn can be used for cause studies. Not only could health professionals have more information about the environment and the use of medical devices at certain locations. IoT devices linked to smartphones can not only enable people to better monitor their own situation but to also share such information in a way that can be used by others to avoid locations or for authorities to identify why people experience more incidents in one area than another

Source: Proteus Digital Health at http://www.proteus.com/technology/digital-health-feedback-system and http://propellerhealth.com

The proliferation and absorption of health-related IoT devices by health systems will allow all patients to receive the kind of real-time monitoring once reserved only for urgent cases in specialist wards (Murray, 2015). It will allow clinicians and other medical professionals to tailor and adjust treatment specific for every patient. In addition, once all aspects of healthcare from devices to treatments have their own digital identification these data can be cross-referenced to improve processes and available combined data, overcoming technological hurdles facing the sector, such as the lack of connections between medical systems (Murray, 2015).

Smart cities, smart street lighting and traffic flow optimisation

In the context of smart cities, a municipality can control, administer and plan public infrastructures, utilities and services by means of the IoT so that cities are managed more efficiently and in a more environmentally friendly way. Smart city plans explore the ability to process huge masses of data coming from devices such as video cameras, parking sensors and air-quality monitors to help local governments achieve goals in terms of increased public safety, improved environment and better quality of life. Examples for IoT-managed public infrastructures and services are lighting, public transportation, parking, garbage collection as well as smart meters for residences (Box 3).

Box 3. Energy provision: smart meters and smart grids

The energy sector is under transformation with the introduction of smart meters informing consumers of their energy usage and patterns, and driving down their consumption and saving energy as a result. Following the result of a cost-benefit analysis required by the European Commission for all member states, 16 members have started to implement smart meters in 80% of the positively assessed locations by 2020. Even in countries with negative or inconclusive analysis, rollout will begin for a selected group of customers. In some countries such as in Germany, a differentiated rollout-approach will be taken, that will commence with some groups of customers and with regard to the individual cost-benefit-relation of that consumer group.

Decentralised generation of energy and delivering it to the grid is a development that is also furthered by smart grids. Prior to communication technologies being used it was sometimes difficult to adequately remunerate the energy generated, including differential payment for energy. Communication makes Smart Grids possible, where demand, input and market prices are known on a continuous basis. In liberalised energy markets this is now so common, that a fifth of electricity capacity used in the Netherlands comes from combined heat-power exchange generators (CHP) in greenhouses where flowers, plants, vegetables and fruits are grown and where the heat and CO2 are essential for the growing of produce. Renewable energy sources such as solar and wind, which do not provide energy on a continuous basis as they depend on the weather conditions as well as hydrogen vehicles which can deliver energy back to the grid will only add to the need for Smart Grids.

Dublin (Ireland), Oslo (Norway) and Chattanooga, Tennessee in the United States have started to use smart street lighting systems.[16] Often triggered by replacing municipal lighting with LED solutions to save on energy costs[17], smart street lighting can offer combined savings of up to USD 100 per streetlight per year because the status of each lamp is known in real-time and maintenance can be scheduled when needed. By integrating two-way communications new functions also become available, such as selectively to dim or brighten the lights depending on the weather, traffic flows, time of day or based on requests from emergency services. Streetlights could become a communication hub that is fitted with or communicates with nearby sensors, such as parking bay sensors, rubbish bin sensors or noise and pollution sensors.

In the same manner, smart traffic lights in larger cities can be instrumental in optimising traffic flows. The SCOOT system developed by Transport for London uses data on road usage with real time control of traffic lights in the city to deliver on average a 12% improvement in traffic flow.[18] Other large cities, like Beijing, São Paulo, Toronto or Preston have introduced SCOOT and similar systems will be increasingly developed to improve in-city traffic flows.[19] Scientists are even looking further and believe that with fully automated vehicles it might be possible to operate intersections without traffic lights. Instead vehicles book a path over the intersection with a central control system. This may in the future allow vehicles to traverse intersections without significantly reducing speed or having to come to a standstill, which would speed up traffic flow, reduce emissions, and save fuel which is wasted in acceleration.[20]

In some ‘smart cities’, public authorities have a full view of how infrastructure and services are functioning. In Korea, the smart city of Songdo has extensive and high-bandwidth fibre connectivity to enable low-latency communication for the different computer systems that keep the city running. Telepresence is installed in homes, offices, hospitals and shopping centres so that people can make video calls wherever they want. Sensors are embedded in streets and buildings to monitor everything from temperature to road conditions. Residents can monitor the pollution concentration in each street of the city. It is also possible for the authorities to optimise the irrigation of parks or the lighting of the city. Water leaks can be easily detected or noise of vehicle traffic can be monitored in order to modify the city lights in a dynamic way. Traffic can be reduced with systems that detect where the nearest available parking spot is, saving time and fuel. Finally, rubbish bins can report their status, enabling more efficient collection only when required.

Unlike Songdo, which has been built top-down as a new city, most existing cities will instead become smart gradually through small-scale experimentation and optimisation of the parameters of the machine learning systems. Traffic lights, road conditions, and other data sources will enable the organic growth of "smartness" in the city, as it incorporates and adjusts IoT elements. Cities may be able to do similar experimentation with lighting levels, for example to see whether they increase or decrease crime and accident rates. What may work best for a city may depend on its unique characteristics (Box 4).

Box 4. Smart-city projects in Denmark

Copenhagen Solutions Lab is the City of Copenhagen's incubator for smart city initiatives and a new governing body for smart city projects working across all sectors in the capital. New ITS solutions, reduced carbon emissions, implementation of sensors that create real time data and information on current situations in the city as well as the build-up and architecture of a new 'Big Data Digital Infrastructure Platform' that shares data across public and private sectors are all focus points for the work within the Lab.

Copenhagen Street Lab situated around the city hall is Copenhagen's test area for smart city solutions in real urban space. It will be a showcase for the newest technologies within smart city and IoT, to demonstrate the potential in these technologies to citizens, decision-makers and companies, and provide a proof of concept for scaling the qualified solutions to larger parts of the city, as well as to other cities in the region, nationally and abroad.

Source: Danish Energy Agency, part of the Ministry of Energy, Utilities and Climate.

Smart governments

According to a market research company, big data, cloud and the IoT are three strategic technology trends affecting governments. In their view, "smart government" integrates information, communication and operational technologies to planning, management and operations across multiple domains, process areas and jurisdictions to generate sustainable public value (Gartner, 2014). For instance, a local government might want to explore the ability to process parking sensors, air quality monitors and video cameras to achieve goals such as increased safety and better quality of life. Even the internal organisation of governments is likely to change as the IoT progresses. For example, in the Netherlands the Department of Defence is moving from 6 000 departmental vehicles[21] to 4 800 of which 3 500 are part of a pool of shared cars, vans and different types of small trucks. Where personnel or units once had dedicated vehicles, they can now reserve vehicles online for official purposes and choose any vehicle available that fits that requirement. The identity card of the person ordering a vehicle unlocks the vehicle. All trips are logged via GPS ensuring that vehicles are used correctly and delivered on time and can report their technical status. In the future vehicles can be used for one-way trips and do not need to be delivered back to their home base. As a result the utilisation of vehicles is higher, malfunctioning vehicles are not a burden to a specific part of the organisation, all trips are now accounted for, no informal or unauthorised lending of vehicles is possible or necessary and all trips are properly insured (van Lisdonk, J. R., 2014).

Challenges relating to the deployment of the IoT

Digital security and privacy risks

The growth of the IoT and the realisation of the economic and social benefits related to its use will in part depend on the extent to which potential users will trust the technology and the products and services that rely on it. This means that users will have to come to terms with the fact that connecting any physical device to the Internet exposes them to some degree of digital security risk, and when personal data is involved, to potential privacy challenges.

The digital security challenges posed by the IoT are largely the same as those associated with industrial control systems: digital incidents involving IoT can have significant physical consequences in addition to affecting other aspects such as an organisation's finance and reputation. Experience shows that this is not a new phenomenon (Box 5). In this respect, the OECD 2015 Recommendation on Digital Security for Economic and Social Prosperity provides an effective framework for managing digital security risk. However, managing digital security risk may become an even greater policy imperative as the IoT connects a much larger number of devices, in industrial and consumer contexts.

The privacy challenges posed by the IoT are also similar to those posed by existing digital technologies which generate and capture data, particularly cloud computing and radio-frequency identification. The OECD Privacy Guidelines provide a framework for addressing these issues, especially as IoT devices become ubiquitous and users have less visibility into how and what data is being collected.

According to the OECD Recommendation on digital security risk management, leaders and decision makers should address digital security as an economic and social risk rather than solely as a technical issue. When carrying out an activity that relies on digital technologies, including the IoT, they should consider the potential economic and social consequences of a possible digital security incident affecting the availability, integrity or confidentiality of the information in the information system. These consequences can damage revenues (e.g. through disruption of operations), undermine reputation (e.g. through the exposure of personal data, or website defacement), or affect market position (e.g. through theft of innovation).

As do industrial control systems, the IoT bridges the digital and the physical world: through various types of sensors, connected objects can collect data from the physical world to feed digital applications and software, and they can also receive data to act on the environment through actuators such as motors, valves, pumps, lights and so forth. Thus, digital security incidents involving the IoT can have physical consequences: following a breach of integrity or availability, a vehicle might stop responding to the driver's actions, a valve could liberate too much fluid and increase pressure in a heating system, and a medical device could report inaccurate patient monitoring data or inject the wrong amount of medicine. As with the industrial control systems that have long operated in some sectors, the potential exists that such physical consequences as human injury and supply chain disruption could result from digital security incidents affecting IoT devices. (Box 5).

Box 5. Examples of digital security incidents with physical consequences

In 2000, a disgruntled former employee of a software development team released 800 000 litres of raw sewage into nearby rivers and local parks, after hacking into the system controlling an Australian sewage treatment plant (Abrams and Weiss, 2008).

In 2003, the computer worm "Slammer" crashed an Ohio nuclear plant network. The worm penetrated a private computer network at the plant and disabled a safety monitoring system for nearly five hours (Poulsen, 2003),

In 2005, DaimlerChrysler automobile manufacturing plants went offline for an hour stopping all work after being hit with the Zotob Worm (Cisco, 2015b).

In 2006 in Harrisburg, Pennsylvania, a foreign-based hacker planted malicious software in a water treatment system by infiltrating the laptop of an employee. The hacker used the employee's remote access as the entry point into the system.[22]

In 2007 in Willows, California, an intruder sabotaged the industrial control system of a water canal, damaging the system used to divert water from the Sacramento River (McMillan, 2007).

In 2008, a teenage boy in Poland hacked into the track control system of the Lodz city tram network, derailing four vehicles and injuring 12 passengers (SANS, 2008; Cisco, 2015b).

In 2009, in Austin, Texas, hackers changed the messages on multiple digital road signs; one sign was altered to read "Zombies Ahead" (Goodwin, 2008).

In 2011, the water treatment system in Illinois was shut down. A hacker managed to remotely disable a utility's water pump used to pipe water to thousands of homes in Illinois. The hacker broke into a software company's database and obtained user names and passwords of control systems (Rushe, 2011).

In 2014, hackers attacked a German steel mill control system such that a blast furnace was unable to shut down resulting in massive damage (SANS ICS, 2014).

In 2015, researchers took control of a Jeep Cherokee remotely, without prior access to the car. They wirelessly interfered with the accelerator, brakes and engine. Following this experiment, Fiat Chrysler recalled 1.4 million vehicles (Greenberg, 2015; Greenberg, 2015b).

Depending on the use scenario, breach of confidentiality can also be an issue with the IoT. For example, a competitor could steal innovation by taking control of networked cameras in a factory or boardroom (Pelroth, 2012). A breach of confidentiality of personal data would raise privacy issues. Here again, the level of risk will depend on use scenario and, in particular, the nature and sensitivity of the data. For example, intruders could remotely access simple home devices such as smart televisions equipped with microphones and listen into households' living rooms. They could also hack into IoT health and fitness devices or more professional medical devices, collecting more sensitive location and health data.

It is important to address digital security risk related to the IoT within the context of the broader computing ecosystem rather than in isolation. In fact, the IoT is rarely a standalone building block isolated from other digital components. Instead, all digital components in an organisation or on a personal network will often need to be considered as interconnected and interdependent. Vulnerabilities or incidents affecting parts of an organisation's information system that may seem unrelated to the IoT can affect it, as much as the exploitation of IoT components can have consequences in other parts of a system. For example, in 2015, a security firm investigated a hospital information system where attackers exploited a vulnerability in a networked blood gas analyser to ultimately infect the entire hospital IT department's workstations (Storm, 2015). As the common metaphor goes, a chain is only as strong as its weakest link, so it is important that we learn from the example of the industrial control systems and ensure that IoT devices

incorporate appropriate security measures from the start. In general, decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment, and that security measures are appropriate to and commensurate with the risk. Digital security risk management should be integrated to the broader risk management framework of the organisation and become part of economic and social decision making, rather than being addressed in silo.

In industrial environments, some digital components that used to be standalone or isolated from IP networks have been progressively upgraded and connected to the Internet, either directly or indirectly, without embedding at the same time basic technical security measures to protect them against simple well-known attacks. For example, some equipment still has easily guessable or hardcoded default passwords, or lacks sufficiently strong authentication or cryptographic protections (Potoczny, 2015). In some cases, this situation can be aggravated by the fact that some of these devices that are not software upgradeable are deployed in remote places where they are difficult to upgrade physically, or have limited or no user interface for remote maintenance. In some cases, the drive for efficient use of resources (memory, processing power and energy) has left security concerns on the side.

The absence of basic security measures or the presence of well-known vulnerabilities also appears in consumer IoT devices and applications. For example, a 2015 study by Hewlett Packard Enterprise Security Research which reviewed 10 of the most popular devices in some of the most common IoT niches revealed a high average number of vulnerabilities per device. 70% of devices used unencrypted network service, 60% provided user interfaces vulnerable to basic attacks, 80% used weak passwords (HP Enterprise, 2015). In 2015, security researchers reviewed nine models of baby monitors with remote access capability, and determined that all but one were vulnerable to the most trivial attacks. This report coincided with a report that someone had hacked a couple's baby monitor, attracting widespread media coverage (CBS, 2015). This situation reflects some level of insufficiency in security practice. In 2013, one of the first cases of a regulator charging an IoT firm occurred, following lax security practices that exposed the private lives of hundreds of consumers to public viewing on the Internet (Box 6).

Box 6. Enforcement action in the IoT space by the United States Federal Trade Commission (FTC)

In 2013, the FTC charged that TRENDNet, a maker of video cameras designed to allow consumers to monitor their homes remotely, had lax security practices that exposed the private lives of hundreds of consumers to public viewing on the Internet. In its complaint, the FTC alleged that, from at least April 2010, TRENDnet failed to use reasonable security to design and test its software, including a setting for the cameras' password requirement. Under the terms of its settlement with the FTC, TRENDnet is prohibited from misrepresenting the security of its cameras or the security, privacy, confidentiality, or integrity of the information that its cameras or other devices transmit. In addition, TRENDnet is required to establish a comprehensive information security programme designed to address security risks that could result in unauthorised access to or use of the company's devices, and to protect the security, confidentiality, and integrity of information that is stored, captured, accessed, or transmitted by its devices. The settlement also requires TRENDnet to notify customers about the security issues with the cameras and the availability of the software update to correct them and to provide customers with free technical support for two years to assist them in updating or uninstalling their cameras.

Source: United States Federal Trade Commission.

The 2015 OECD Security Risk Recommendation notes that all stakeholders – governments, public and private organisations, and individuals who rely on the digital environment for all or part of their economic and social activities – have a role in managing the digital security risk to their own activities. However, those who are in charge of developing and maintaining the digital environment "should also implement appropriate security measures in their goods and services, where possible, to empower their users to manage digital security risk." This may be challenging for manufacturers and designers of products in areas that have not previously focused on digital security such as health devices makers, energy

providers, or automobile manufacturers. For example, the automotive sector is moving quickly to make cars into IoT devices. Ford and BMW recently announced that the same software security updates that personal computers receive today will be sent to cars wirelessly.[23] Support for ongoing updates can mitigate many of the security vulnerabilities mentioned above. Connectivity has security implications of its own, however, as underlined by the early-2015 Chrysler recall of 1.4 million vehicles after vulnerabilities in their UConnect Internet-connected hub were disclosed by security researchers (Greenberg, 2015). The application of a digital security risk management approach in the design of a product or service that was not previously networked requires a change in the engineering culture. Nevertheless, product design methodologies should address digital security risk reduction measures as they do with other categories of risk.

Several stakeholders are developing IoT digital security guidance. They include, for example, the GSMA set of security guidelines to promote best practice for the secure design, development and deployment of IoT services[24], the European Commission "Alliance for Internet of Things Innovation (AIOTI)" which published ten policy recommendations in relation to privacy which could be adapted to a greater geographical scope, the Open Web Application Security Project (OSWAP) Internet of Things Project[25], and the Cloud Security Alliance "Security Guidance for Early Adopters of the IoT".[26] In the United States, other recommendations and standards documents are being developed by specific agencies, such as by the Federal Trade Commission[27], the Food and Drug Administration with respect to medical devices (FDA, 2016), or NIST with respect to smart grid (NIST, 2014). The FBI, as well as other United States law enforcement agencies, is conducting ongoing research into the ways that criminals exploit IoT systems and other computer resources remotely, and provide advice and data to help consumers and businesses to avoid these intrusions.

Comprehensive data collection

The promise of IoT technologies is dependent on the data generated by the connected 'things'. Data about how customers in a given region actually use energy can make for more efficient use of scarce resources as well as providing guidance on the best way to heat and cool for individual users. The data generated for medical devices can drive widely-applicable research even as it alerts doctors to the need for different treatment or the presence of malfunction. Data about traffic patterns in relationship to any number of factors already contributes to the way the traffic system operates.

Data processing in the IoT can take place in a variety of ways ranging from locally, on the device itself, to remotely, with information being sent for processing to servers elsewhere. Governments, businesses and data protection authorities around the world are trying to anticipate the possible potential privacy implications of having an extraordinary amount of data points that could be collected, aggregated across devices and analysed not only by the device owners, but also by other third parties unknown to the individual. A key challenge for using the data, and in particular personal data, obtained through the IoT, is in developing approaches to accountability, transparency, and consent for data use.

Inference and the loss of control

Privacy principles dictate that users should be able to keep control of their data as well as to opt out of the "smart" environment without incurring negative consequences. There are a number of means that individuals use to protect their own privacy. Intuitively, the most obvious way is to withhold or conceal information relating to them. However, the ubiquitous nature of IoT, coupled with technological advances in data analytics, makes it increasingly easy to generate inferences about individuals from data collected in commercial or social contexts, even if these individuals never directly shared this information with anyone.

An example is geolocation data from mobile devices, which on the one hand can be used to improve the location-based services on which many rely today, but at the same time leaves a trail of an individual's daily routines and movements, which are increasingly used for other services including for process improvements. Tracking enables businesses to enhance their practices by providing them with an enhanced means to "know" the customers and can be used in multiple ways to expand customer behaviour analysis. Value is derived from the rich information about the individual, their activities, their movements, and their preferences.

With the IoT, sophisticated tracking and profiling can occur, involve third parties that individuals may not be aware of, and result in a combination of online and offline information such as location patterns (inside a store or across a city), online browsing, purchase history and social media activity.

In September 2014, Europe's Article 29 Working Group – composed of data protection authorities of European Union member countries – issued an Opinion on Recent Developments on the Internet of Things. In the opinion, the Working Group emphasised the importance of user choice, noting that "users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific."

Some privacy issues are not specific to the IoT context. For example, the question as to what constitutes personal data becomes particularly important when there are combinations of online and offline tracking. There are some cases where organisations may advise that they are not collecting personal data such as names and addresses, but they do collect IP addresses or other identifiers which could be considered personal data depending on the context and what other data is being collected. In addition, while some have argued that the information at issue in the Internet of Things environment is anonymised or pseudonymised, there are difficulties with anonymisation in this context. As the Article 29 Working Party noted, even pseudonymised or anonymised data may have to be considered personal data.

Data analytics extracts information from data by revealing the context in which the data are embedded, including patterns, correlations among facts, interactions among entities, and relations among concepts (Merelli and Rasetti, 2013). Thus, data analytics enables the "discovery" of new information.

Data analytics is not a new phenomenon. However, as the volume and variety of available data sets increase, as well as the capacity to link different data sets, so does the ability to derive further information from these data, for example for profiling purposes. Advances in analytics now make it possible to infer sensitive information from data that may appear trivial at first, such as past purchase behaviour or electricity consumption. The IoT will likely accelerate this trend, generating a large number of diverse but inter-linkable data sets that directly or indirectly relate to economic and social activities.

Transparency and purpose of data collection

Promoting transparency and the rights to access and correction have been part of the OECD Privacy Guidelines since their initial adoption in 1980, and have been incorporated to varying degrees, into many national laws around the world. Transparency and access have long been recognised as powerful tools to enable data subjects to make informed decisions and to ascertain the basis on which decisions about them are taken, thereby reducing the potential for discrimination. The Council of Europe recommends that, in some circumstances, transparency requirements include the logic underpinning the processing (Council of Europe, 2010). However, devices in the IoT may often be designed to operate in the background as part of home or living environments so that individuals may never know they are there. As a result, individuals may have difficulty knowing what information about them is being collected, used and disclosed by such devices.

In the retail environment, for example, passive in-store tracking and profiling raises questions as to how individuals are made aware of the purposes of the collection of their personal data, how transparent the information management practices of all the stakeholders involved are, how individuals are notified about such practices, and how these communications are presented to them in order for them to give meaningful consent.

As a 2016 report by Canada's Office of the Privacy Commissioner (OPC) notes[28]: "binary, one-time consent and traditional definitions of personal information are increasingly perceived as outdated because they reflect a decision at a moment in time in the past, under specific circumstances and are tied to the original context for the decision. Simplistic, "on/off" personal data management policies may be neither flexible, nor appropriate, in the fast-developing IoT environment". In addition, the 2015 report by United States' Federal Trade Commission on the Internet of Things recognised the practical difficulties of providing consumer choice where there is no consumer interface and suggested new options, including choices at point of sale, tutorials, during device set-up or codes on the device.

There are challenges with the current consent model and further work is needed to identify, explore and validate possible options to deal with these challenges so that concerns raised both by individuals and organisations are addressed.

Raising individual awareness and promoting responsible use by organisations

These considerations require implementing a user-centric approach that empowers users to play a meaningful and active role with respect to the collection, use and disclosure of their data, including by providing them the ability to make informed choices. This requires education and awareness, which are specifically identified in the revised OECD Privacy Guidelines' call for "complementary measures".

Focusing more explicitly on promoting responsible usage by organisations could also complement efforts to improve transparency and consumer empowerment. Policy makers and enforcement authorities may need to play a role in helping organisations to identify appropriate substantive limits. Examples can be drawn from guides to credit scoring, policies against the use of genetic information by insurers, and prohibitions on the use of social networking data by employers.

The White House Big Data Report recently concluded that, putting greater emphasis on a responsible use framework has many potential advantages.[29] It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.

Accountability and privacy risk management

Accountability is a key new provision in the Privacy Guidelines. To be accountable, an organisation needs to be able to demonstrate what it is doing and what it has done, with personal data and explain why.

The revised OECD Privacy Guidelines introduce risk management as a key approach for implementing privacy protection, especially in the context of developing privacy management programmes for accountability. Risk assessment can consider data sources and quality as well as the sensitivity of the intended uses. In addition to mitigating the risks of misuse, the assessment can also examine the process by which the data have been analysed; this can help identify where errors or mistakes may have been introduced into the analytical process itself. To be effective, the scope of any privacy risk assessment must be sufficiently broad to take into account the wide range of harms and benefits, yet sufficiently simple to be applied routinely and consistently.

The IoT environment may make risk assessment challenging, due to the many stakeholders, such as device manufacturers, social platforms, third-party applications and others. Some of these players may collect, use or disclose data, and can have a greater or lesser role in its protection at various points, though where to draw the line between them can be challenging at the best of times. For example, who is ultimately responsible for the data which the smart meter broadcasts? The homeowner who benefits from using the device, the manufacturers or power company which provided it, the third-party company storing the data, the data processor who crunches the numbers, all of the above, or some combination thereof? And to whom would a privacy-sensitive consumer complain? Should privacy be breached, where does the responsibility of one party end and another begin?

Thus, the extent to which a comprehensive risk management approach can strengthen application of the OECD Privacy Guidelines' principles is a topic for further work that could also consider aspects that may be specific to the IoT.

Interoperability of technologies and policy frameworks

As a result of the vast diversity of IoT application topic areas and the vast heterogeneity in their goals and requirements, many IoT devices and techniques will exist, and interoperability is crucial. While for some the current explosion of products and services is the signal of a growing IoT marketplace, a fragmented ecosystem with non-interoperable technologies could undermine the efficiencies achieved by large economies of scale. The IoT ecosystem will employ hardware and software from many different vendors, and the ability to employ functionality from many devices and vendors is key to IoT techniques reaching their potential. An effective approach to solve this problem is to rely on global, voluntary standards developed by standards development organisations and industry consortia. The diversity of potential IoT applications, device technologies, business and operational models will require flexible approaches, so it is important to not tie the IoT ecosystem prematurely to burdensome or conflicting standards, particularly those of a one-size-fits-all nature. Furthermore, rapid technology innovation in this domain may mean that early approaches will be quickly surpassed.

Functional interoperability must take into account radio technologies, RFID and mobility. As opposed to data and service portability, feature/function portability in the IoT might not always be possible because this is the way innovation occurs across products. A balance must be found between proprietary non-interoperable systems and unified systems which, in turn, could enable the sharing of information across services generating a loss of privacy and control if not carefully designed. Such a fragmented ecosystem in which users requires multiple systems which do not interoperate does not encourage consumer adoption and stresses the need for compatible systems. In France, for example, a survey reported that 74% of people found the multiplicity of applications to control IoT objects a barrier to buy one.[30]

There are a number of issues related to the interoperability of policy frameworks across borders and sectors, in areas such as consumer protection, safety, privacy and security, particularly when products are designed, manufactured and sold in countries with different approaches. It is necessary to address the gaps between different approaches and practices. It is also important to identify and highlight the responsibilities of different actors. For instance, the consumer experience in IoT connected services will likely fall under the responsibility of the private sector. In the case of consumer protection or safety, the role of governments may be more prominent. To foster policy interoperability, governments could encourage further dialogue across regulatory agencies and with industries that traditionally were not closely involved in communications, such as transportation or utility services.

Investment

According to industry experts, the adoption of the IoT in homes, cities and industries is not expected, in the short term, to dramatically increase the demand on current networking infrastructure.[31] Thus, the traffic increase due to the IoT adoption would be gradually absorbed by connectivity providers with their network upgrade investment cycles. However, it is necessary to ensure a continuous stream of investment in several areas such as sensor technology development, energy-saving techniques and interoperable software platforms.

An increasing number of large ICT companies are investing significantly in IoT projects. Some governments are looking for ways to promote this activity while others prefer to take a technology neutral approach. Multinational firms are advocating for more transparent, predictable, and technology neutral laws and regulatory requirements to avoid impeding the pace of IoT innovation and economic growth. The European regulatory framework for electronic communications can be mentioned as a good example as it enshrines the principles of predictability and technological neutrality. Its pro-competitive regulatory approach promotes investment when imposing proportionate and appropriate regulatory measures. Many firms engaged in IoT development and businesses argue, however, that the global nature of IoT services and the need to promote innovation in the private sector require a "light-touch" regulatory approach.

Some OECD countries may take actions to reduce the barriers to entry for new players, while other countries are likely to refrain from influencing current market conditions, especially where IoT applications may compete with existing licensed services. One consumer-related example is a home security service provided through a mobile operator versus a set of Internet-connected devices owned and controlled by the homeowner. The mobile provider may want to maintain its revenue stream from the subscription service rather than allowing consumers to perform those functions themselves. Many regulators, such as in the United States, may be reluctant to attempt to influence markets by creating incentives for competition among vendors. For the larger economies, such industrial policies may not be necessary. Six of the 10 largest IoT investments in the world to date are being made by United States based companies, where the federal government adheres to a policy of technology neutrality in most instances.[32]

Jobs and skills

A question that arises around the IoT concerns its implications for employment. The competitiveness of the market of an economy is dependent upon having the most efficient tools and processes. It is likely that countries that invest more in the development of sensors/actuators and autonomous systems, data analytics and machine learning, and data communications will benefit more greatly from them. Whether this will lead to economic growth or will influence jobs is a source of debate among economists - see, for instance (OECD, Forthcoming a). It is likely, that if robotic warehouses perform as well as suggested by those implementing them, then jobs in the warehouse sector will decrease and firms will try to compete on building more efficient warehouses.[33] This will lead to efficiency, reducing costs and prices, and which could in turn lead to greater purchasing power for consumers. It also could lead to job loss and frictions in the economy.

There are many other "routine" jobs that might decline in the coming years. If fully autonomous vehicles were successful, then autonomous taxis, buses and trucks would be likely candidates for reduced employment. For example, one automobile manufacturer has estimated a return on investment in a self-driving truck in 2025 of less than 24 months, or significantly less than the economic life of such a vehicle.[34] The effect could be that some jobs that in the past absorbed unskilled or low-skilled workers may not exist to the same degree in the future. There will still be jobs associated with providing these functions. But many of them will require higher skills, such as for repairs and programming of robotic functions. Having a skilled labour force is therefore crucial (OECD, Forthcoming b) though even here some

traditional jobs may be eliminated. On the other hand, there are also cost savings associated with autonomous machines, which may allow the re-employment of people in other parts of the economy. In addition, greater efficiency in transport may support increased demand across the whole economy enabled by these gains.

Brynjolffson and McAfee mention in their book "Race against the Machine" a possible future in which machine learning allows robots to replace humans in many "lower skilled" jobs. Their work aimed at bringing technology into the discussion on unemployment and the global financial recession. The "End of Work" as this hypothesis is known, after a book by Jeremy Rifkin, has in the past been proposed by many economists, but has not received much attention as technological changes have generally been accompanied with increases in employment in other parts of the economy, such as the services economy and the IT-industry. To many economists, the proposition is therefore also known as the Luddite fallacy (Economist, 2011). While there are different views on the implications of technological change for employment, the IoT promises to increase the discussions of this topic. Brynjolffson and McAfee point to the introduction of mechanisation at the start of the 20th century, which led to an almost complete replacement of the use of horses in only two decades. In many ways, the world is today at the dawn of machine learning similar to where it was in 1994 with respect to the Internet. Practical commercial examples are now available, but much is still to be learned. Technology has moved quickly and the integration of low-cost electronics, large scale processing power and ubiquitous networking has allowed new generations of autonomous and semi-autonomous machines. These machines are moving into every part of the economy and are displacing work in various sectors. This could theoretically lead to workerless factories. Even if it causes only temporary friction problems in the economy, as Keynes once suggested, it is a development that policy makers need to consider. Machine learning is as much about the competitiveness of the economy as it is about labour policy.

Even though the effects of the IoT cannot be evidenced yet in changes in employment, it is illustrative to make use of studies of a broader "digitalisation" in businesses. Recent studies with regard to the German market show that a majority of companies do not expect negative effects of digitalisation on the number of jobs offered by their company.[35] In the cited study 23% of the interviewed companies even expect new hires to manage the digital transformation. In summary, while the introduction of digital technologies into businesses could bring more jobs in the short term, the long term effects on jobs are rather unclear.

Measuring the adoption of IoT systems by firms and consumers is an area hardly explored at the moment due to the emergence of operational IoT platforms. There is a lack of appropriate metrics to gauge the penetration and effects of the IoT on the labour market. The measurement of the digital transformation should incorporate the IoT among its elements. Stakeholders could provide data that could help in the measurement efforts, for example, the number of sensor networks or devices installed and the benefits (economic, social, environmental and so forth) involved, or the skills required to develop in order to fully adopt and seize the benefits. Concrete actions to consider could be the development of measurement guidelines based on knowledge gaps identified.

SECTION III: AREAS FOR STAKEHOLDER ACTION

Evaluate and assess existing policies

Authorities should evaluate existing policies and practices to see if they are suitably supportive of the IoT, and do not constitute unintentional barriers to potential IoT benefits. Some regulations or practices have assumptions that inhibit the application of the IoT, and consultations with the sector's main stakeholders may highlight such barriers. The incorporation of IoT in people's lives will also require evaluating the implications for privacy and security with the current international frameworks, and work towards ensuring sufficient safeguards in the context of consumer protections.

The IoT provides opportunities to promote public interest through public policy, including those that empower consumers to a greater extent than may have been possible in the past. The challenge with encouraging the development and use of novel and innovative uses of IoT, however, may sometimes be that existing actors may see the current rules as a shield protecting their interests from easier entry in a market by competitors. These actors will raise questions associated with changes in opening markets and will often raise valid points that need to be addressed (e.g. public safety, consumer protection). Governments will need to find a balance between these interests and the objective to foster innovation, competition and growth through the IoT sector.

One example of an industry where regulations need to be adapted in order to benefit fully from the possibilities of IoT is the health sector. In some countries, medical practitioners may receive reimbursement based on the number of visits by patients. Such visits may be billed according to the average duration of appointments (e.g. increments of 15 minutes), with this time being used for discussion, assessment, tests and so forth. A challenge with this model is that rigid schedule may not necessarily be applicable to an individual's requirements.. The IoT could potentially change that by enabling monitoring and reporting of information to both medical practitioners and patients. Not only could it be used to schedule appointments only when needed but also to aggregate data in ways that could be beneficial to those directly concerned and to the wider community while ensuring that the parties respect legal requirements and specific privacy policies for data processing and transfer among entities.

The IoT has the potential to alter the traditional (legal) understanding of "service attendant" and associated laws, be it healthcare or any vertical where the attendant was previously physically present. Similarly there are a large number of codes, practices, standards and other types of regulations that govern how devices operate, how services are performed and how consumers and businesses interact. Such standards can, for example, be building codes. These codes are often conservative, based on years of experience. However, they can also have the drawback that the codes limit innovations in the IoT to be implemented.[36] Authorities would do well to evaluate such regulations, with a specific focus on the new opportunities offered by the IoT.

Governments could also review their existing telecommunication laws in order to evaluate whether they provide for an adequate regulatory framework for M2M-communications and the IoT. Since telecommunication laws generally date from a time when only voice telephony existed, it is not a given that these laws are fit for purpose in a digital era. For example, this question is one aspect of the Digital Single Market (DSM) Initiative of the European Union. Similarly, the Body of European Regulators for Electronic Communications (BEREC) assessed, in its report on "Enabling the Internet of Things", whether M2M services might require special treatment with regard to current and potential future regulatory issues (BEREC, 2015). Generally speaking, it needs to be determined which players and/or which services in the M2M value chain could be subject to telecommunication regulation, taking into account both the benefits

and the costs of such regulation. While the connectivity service provider is the right addressee of sector-specific regulations, this might not hold true for producers of connected devices, or at least not the majority of them.

Promote the use of global technical standards

When considering standards issues for the emerging IoT, it is important to recall that IoT neither refers to a single technology nor a new phenomenon. Due to the vast diversity of application areas and heterogeneity in their goals and requirements regarding sensing, actuation, data communication and data analytics, there will be many IoT techniques devised, each addressing different aspects of a nearly-limitless design space. The diversity of potential IoT applications and device technologies alone leads many to conclude that it would be detrimental to this ecosystem to be tied at an early stage of technological development to one-size-fits-all type of standards or standards that might prove burdensome or conflicting. Over time, technological maturity and end-user choice will ultimately identify the most promising standardisation approaches.

IoT standards are regarded particularly positive when they offer, as opposed to proprietary solutions, net positive effects in regards to large scale deployment, lock-in prevention and improved security. In the development of the IoT ecosystem and its interoperability, global, voluntary standards developed by standards setting bodies or industry consortia play a key role. Interoperability is essential to stimulate the emergence of new systems, boosting innovation and reinforcing competitiveness. Standardisation efforts, for instance, can also reduce the costs of producing electronic modules for the IoT.

Proprietary solutions, or country-specific standards, on the other hand, tie users to a specific vendor or country requirement to the exclusion of all other vendors. While the solution may be effective in the short term, the lack of competition in the industry can make the solution costly to acquire and maintain, and it may not be interoperable with other products resulting in lock-in issues. Proprietary solutions, may however, provide a competitive advantage in markets such as connectivity. Sigfox, for example, a French-based connectivity provider that uses a cellular-style proprietary system has now deployed nationwide infrastructure in eight European countries and projects expansion to 50 by 2019.[37]

Standards development for IoT interoperability, which encompasses multiple actors (hardware/device manufacturers, software platform providers, communication service providers, application developers and cloud providers) across very distinct sectors such as health, lifestyle, connected home, transport and industrial Internet among others, is still in its relatively early days. Organisations involved in IoT standardisation work include European, American and global standard organisations such as the International Telecommunication Union(ITU), the European Telecommunication Standards Institute (ETSI), the American National Standards Institute (ATIS), the Telecommunications Industry Association (TIA), the International Standards Organisation (ISO) and the International Engineering Consortium (IEC) as well as international fora and consortia such as the World Wide Web Consortium (W3C), the Institute of Electrical and Electronic Engineers (IEEE), the Industrial Internet Consortium (IIC) and the Internet Engineering Task Force (IETF) among others. Industry has also organised itself to ensure interoperability at a functional level, with several initiatives. Some of the relevant work on IoT related standardisation is displayed here (Box 7).

Box 7. A myriad of IoT standardisation initiatives and bodies

International Standard Development Organisations (SDOs) and other technical standardisation bodies involved in telecommunications and the Internet are also involved in the IoT:

- The ETSI focuses on the development of an application-independent M2M horizontal service platform.
- The IEEE has some related work through their P2413 Standard for an Architectural Framework for the Internet of Things.
- ITU-T Study Group 20 studies the development of international telecommunications standards relating to Internet of Things (IoT) and its applications, with an initial focus on Smart Cities and Communities (SC&C).
- The IETF participates in IoT standardisation particularly through Authentication and Authorization for Constrained Environments (ace) and IPv6 over Low power WPAN (6lowpan), which has already concluded.
- The World Wide Web Consortium (W3C) via the Web of Things, “standards for identification, discovery and interoperation of services across platforms”.

Leading industry players are also active developing horizontal standards to enable different architectural modes of IoT functionality.

- The OneM2M initiative was founded in 2012 by seven SDOs including ETSI along with over 230 ICT companies. OneM2M is developing specifications for a common M2M service layer, focused on security and privacy, which can be embedded in various hardware and software to connect a myriad of devices with M2M application servers worldwide. It relies on liaison relationship with other standards bodies such as 3GPP, BBF, HGI, TIA, and ITU-T.
- The Industrial Internet Consortium: formed in 2014 by AT&T, IBM, Cisco, GE, Intel and academic and United States government entities to develop and make more widely available intelligent industrial automation for the public good. The IIC’s work includes influencing the global standards development process and developing new approaches to security for electricity, gas pipeline and water distribution systems and maintenance of manufacturing equipment. It currently has over 200 members.
- The AllSeen Alliance: initiative to enable industry standard interoperability between products and brands with an open source framework (AllJoyn) that drives intelligent experiences for the Internet of Things. The initiative includes more than 185 members such as Microsoft, LG, Canon, Electrolux, Qualcomm, SONY, Phillips, etc.
- The Open Interconnect Consortium: group of industry leaders that have prepared a specification and promote an open source implementation to improve interoperability. The consortium groups more than 50 members, and includes Cisco, GE Software, Intel, Mediatek and Samsung.

In March 2015, the European Commission launched the Alliance for Internet of Things Innovation (AIOTI). AIOTI is an open stakeholder platform encompassing all actors of the IoT value chain, working to address these barriers within the IoT ecosystem and with the support and active involvement of the European Commission. AIOTI’s workgroup (WG3) focused on standardisation recommends the use of standard-based solutions for the deployment of IoT in future projects.[38] The complexity and interdependence of IoT standards is illustrated by the interoperability "plugtests" that are performed by the ETSI for key IETF protocols for the IoT developed on IEEE technologies.

As much as global standards provide a solution to interoperability issues, companies have vested interests in driving the adoption of particular standards. This translates into companies being part of multiple standardisation efforts to ensure their optimal position as the market develops. Given the high degree of standardisation activity, it is also noted that, without careful attention, there is a high risk for

considerable duplication of effort. Because of the degree to which IoT technologies represent the natural extension of other existing technologies, any new policy or standardisation action will almost undoubtedly have significant duplication with existing efforts.

In Europe, for example, the European Commission proposed in the Digital Single Market (DSM) Strategy to launch an integrated standardisation plan to identify and define key priorities for standardisation with a focus on the technologies and domains that are deemed to be critical to the DSM. In this context, the objective is to avoid fragmentation between national initiatives in Europe, allow cross-fertilisation between different application domains, and make sure that the regulatory framework supports seamless up-take across borders. The European Commission is also looking for input on standards in the IoT and related areas such as 5G communications, Cloud computing, Intelligent Transport Systems (ITS), Smart Cities and efficient energy use. A public consultation to gather views on priorities for standards closed in January 2016 and results will be published soon (EC, 2015). The promotion of global standards in these areas would increase the opportunities to deliver interoperable products and services to a global audience using economies of scale for the different elements (sensors, chips, platforms, etc.) across the supply chain.

In summary, standards are essential for IoT devices and services to operate. At the same time there are so many standards families to choose from that it is nigh impossible to determine whether a standard fits a situation well, or whether it will be supported industry-wide and in the future. This is true for both applications for businesses and consumers and for every layer from network to services. Stimulating research into standardisation itself appears to result in more standards, instead of one standard. Researchers of IoT technologies and solutions should acquaint themselves with existing standards and standardisation initiatives to avoid duplication of standardisation efforts.

Evaluate spectrum resources to satisfy IoT needs

Different parts of the IoT need a variety of spectrum resources that is fit for purpose. Because every part of the electromagnetic spectrum is used, developers of new applications find it challenging to obtain spectrum that meets their requirements. Regulators are aware of the general scarcity of spectrum supply for all uses and endeavor to make spectrum available, but existing users often have valid objections to vacating or sharing spectrum. Spectrum needs may be mainly addressed through two different types of spectrum: *licensed* spectrum allocated to commercial mobile networks and spectrum available under general authorisation models or *license-exempt* spectrum (Box 8).[39] In addition, it appears that because mobile networks are not always accessible under competitive terms, some users are looking for regulatory arbitrage, using license-exempt spectrum or alternative bands to satisfy their needs. Particularly, the use of technologies developed in license-exempt spectrum bands, such as Wi-Fi, which can keep prices low for consumers and gives innovators the extra spectrum space to develop new products.

It is illustrative to analyse different wireless technologies and how they relate to specific types of spectrum schemes. Starting from within the home and moving outward, the 2.4 GHz band is probably the most saturated band for all kinds of applications, including for the IoT. The band supports Wi-Fi, Bluetooth, Zigbee, Thread and many other networking protocols. Originally allocated as spectrum for industrial, scientific and medical (ISM) applications, today several applications share this band. This is why spectrum managers decided to allow unlicensed use of the band and would, in many cases, like to make more available when appropriate according to market demand. For IoT manufacturers, the benefit of unlicensed spectrum lies in the low transaction costs of introducing a new innovation. There is no need to negotiate access or face upfront costs from third parties, which makes it effectively a platform for innovation and a greenfield space for technology startups, entrepreneurs and established companies alike. Unlicensed spectrum levels the playing field.

The predicted growth of IoT applications will indeed increase demand in existing unlicensed bands, especially in frequency bands dedicated to short range devices (SRD) below 1 GHz, for example in the 433 MHz band in Europe and 900 MHz[40]. The need for a predictable sharing environment and also the need to find more efficient spectrum sharing solutions for some IoT applications has already led to investigations in the CEPT on more sophisticated technology and application-neutral spectrum access and mitigation techniques. At the same time, other countries are also exploring spectrum issues with respect to IoT. Any evolution of SRD regulation should carefully consider results of sharing studies.

Box 8. Unlicensed spectrum research on congestion and quality of service

A question arises as to the extent unlicensed bands suffer congestion or diminishing quality of service which could be problematic if more IoT devices use technologies operating in such bands. The bands around 900MHz (SRD band 868MHz in Europe, ISM band 915MHz in the United States) provide an example of how different technologies attempt to co-exist and compete in this band: Z-Wave (short range/low power), Wi-SUN (short range/low power), LoRa (long range/low power), Sigfox (long range/low power) and Weightless-N (long range/low power). It will be necessary to monitor whether the technologies can peacefully coexists as the number of users increase.

In 2009, a consultancy report undertaken for Ofcom found that the majority of problems experienced by Wi-Fi users in the 2.4 GHz band were not spectrum-related, but mostly due to configuration issues or problems with the wired Internet. The report said, however, that some inner city locations, such as in central London, exhibited signs of congestion and interference, which they said was expected to increase. Wi-Fi in the 5 GHz band is less congested and has much more bandwidth, enabling non-overlapping channels and higher throughput, and Ofcom is continuing to monitor the use of these license-exempt bands.

In the Netherlands, a study found that in inner cities, shopping malls and high density housing, users of Wi-Fi could find as many as 50 active access points at any given time. These would interfere and significantly decrease the throughput of the spectrum. It expressed concern for the 2.4GHz-band's utility in the future given the extensive use today, but also noted that the 5GHz band offers much better performance and less interference, in part because it is less used and carries less far and less well through objects such as walls than 2.4GHz.

Furthermore, FCC's Technological Advisory Council, an outside group of industry experts, suggested that the planned additions of unlicensed spectrum (predominantly in the 5 GHz band) should be sufficient for IoT evolution but that this could change if image and video were widely used as cheap sensors. It therefore recommended continual oversight of the evolution to monitor spectrum sufficiency.

Source: Mass Consultants Limited and Radiocommunications Agency Netherlands – Ministry of Economic Affairs.

Unlicensed bands also involve requirements, such as mitigation techniques, as the devices should not cause harmful interference or expect protection against interference. Wi-Fi technologies in the 2.4/5 GHz bands and applications in the 800/900 MHz band are the most significant examples of such unlicensed bands. Wireless microphones, radiofrequency identification (RFID) systems, medical equipment, or smart grid communications make use of license-exempt spectrum. The development and use of Wi-Fi is one of the most successful examples of the use of unlicensed and shared spectrum. Today, it is not only used by millions of users around the world but it is also playing an increasing role in areas such as offloading mobile traffic on to fixed networks.[41] In Australia, this type of regulation for spectrum is referred to as "class licensed spectrum". The economic significance of license-exempt spectrum to the future of the Internet is not contested.[42]

Efficiency gains in radio technology are positively affecting the viability of IoT. As radio transceiver technology improves, higher frequencies will be utilised with a better precision and lower costs than before. Current market developments are reducing the power that mobile stations, the most expensive and power

hungry component in the mobile network, require to transmit their signals by improving the amplifiers design with software defined radio technology. [43]

Box 9. Allocating spectrum for V2V communication

Authorities are looking at other spectrum for the IoT for Intelligent Transport Systems and vehicle-to-vehicle communication (V2V), which have the potential to make vehicles safer to use and to allow future innovations for autonomous vehicles. For example, vehicles and roadside equipment, such as traffic lights can signal the state of an intersection, whether vehicles are (abruptly) braking and so forth. The United States and Europe have made spectrum available at 5.9 GHz for V2V and Japan aims to use the 760 MHz band for V2V which is unlicensed but limited only to safe-driving support

In May 2015, the United States Government asked the National Highway Traffic Safety Agency for acceleration of the introduction of V2V technology by the end of the year, in order to make roads safer and facilitate the introduction of self-driving vehicles. In Europe 30 MHz has been designated for Intelligent Transport Systems in the 5.9 GHz band. In the United States, 10 MHz is used exclusively for safety-related V2V communications. It is under discussion in the United States whether it is possible to share the relevant band with other license-exempt services/applications like Wi-Fi.

For its part, the United States favours spectrum sharing opportunities over spectrum segregation per application. Europe has considered whether it is possible to share the 5.9 GHz band with other license exempt services/applications like Wi-Fi. However, according to the feasibility studies undertaken, it is unlikely to make the band available for mobile applications.

Source: OECD delegates and blog post by Mr. Foxx, Secretary of Transport of the United States.

For devices that need coverage over a large area, traditional mobile 2G/3G/4G networks are commonly used. However, because of signaling and mobility requirements of mobile phones and smartphones, these networks are not always optimised for IoT applications (Box 9). Some mobile devices impose high energy overheads on initiating data communications, which means that the intermittent and low data rate transmissions common to some IoT applications has in the past led to higher-than-necessary battery drains. There are technology and standards developments underway to make transmission approaches in mobile networks better suited to IoT requirements. LTE Cat-0 and LTE-M, for instance, are standards that will reduce the modem complexity relative to current LTE (4G) systems by 50% and 25%, with similar costs reductions (Leckie, 2015).

Numerous M2M services are currently served through mobile 2G/3G/4G networks (e.g. credit card machines linked to the 2G network in the 900 MHz). However, users with a high number of devices in operation find that such networks do not always provide a competitive option for M2M. As a result of the potential lock-in and the challenges in achieving coverage, large-scale suppliers and users of the IoT have been examining alternative networking solutions. Telefonica and the Swedish company Connode won a 15-year contract to supply smart metering solutions in the United Kingdom that uses a combination of IEEE 802.15.4 IPv6-based mesh networking and cellular connectivity. The mesh networking allows the smart meters to use other smart meters to get to a hub that has cellular connectivity and if coverage is lost on one node, another node can act as a hub.

As mentioned by a recent CEPT analysis in June 2015, there does not seem to be a strong case for the specific designation of specific frequency bands for IoT, since most IoT applications existing today or foreseen can be carried over commercial mobile broadband networks.[44] Nevertheless, Ofcom has made available frequency bands on a license-exempt basis for IoT applications in the United Kingdom.[45] Moreover, after a consultation launched in September 2015 Ofcom concluded that a new license is not necessary to roll-out new services in the 55 MHz-68 MHz, 70.5 MHz-71.5 MHz, and 80 MHz-81.5 MHz

bands and that the current license is appropriate for providing access to the spectrum for IoT and M2M services.[46] Other opportunities for IoT could come from the development of a fifth generation (5G) of mobile radio technology that would substantially exceed the capacity of existing mobile technologies and would be IoT-ready. In the United States, the FCC expressed that 5G will likely have to use diverse types of radio access technologies, including macro cells, microcells, device-to-device communications, new component technologies, and unlicensed as well as licensed transceivers (FCC, 2014).[47] When developing 5G, requirements from industry such as the automotive (e.g. very low latency time, mission-critical reliability) need to be taken into account.

Adapt research and innovation policies

Many governments have recognised the potential benefits of the IoT and reflect that through a number of public policies, either as an enabler of goals or as an area targeted for research.[48] There is no uniform way that governments approach the IoT, but some examples can be provided. The European Union has made the IoT an essential part of its Digital Agenda for Europe 2020. It focuses on applications, research and innovation and the policy environment. As a result, the European Union has been particularly active in promoting research and innovation.

The Internet of Things European Research Cluster groups together the IoT projects funded by the European research framework programmes, as well as national IoT initiatives. The requirements of IoT will also be fed into the research on empowering network technologies, such as '5G mobile technologies'. The Future Internet public private partnership will develop building blocks useful for IoT applications, while Cloud Computing will provide objects with service and storage resources. On the application side, initiatives like Sensing Enterprise and Factory of the Future help companies use the technology to innovate, while experimental facilities like *FIRE* (Future Internet Research and Experimentation) are available for large-scale testing.[49] A study mandated by the European Union has identified the following IoT research challenges: open integrated architecture, end-to-end connectivity, security by design, semantic-driven analytics (IDC and TXT, 2015).

In May 2014, the Korean government published its plan for building the IoT with the aim of a hyper-connected, "digital revolution" to address policy goals. Among the aims is to attain IoT-driven economic development. Some examples already visible are Songdo Smart City and smart eel farms. It targets the commercialisation of 5G mobile communications by 2020 and aims for Gigabit Internet to achieve 90% of national coverage by 2017. In relation to spectrum, the Korean government's plans would see a total of 1 GHz of spectrum freed by 2023, and IPv6 infrastructure into the subscriber network by 2017. It will promote the development of low-power, long-distance and non-licensed band communication technologies for connecting objects in remote areas (Ministry of Science, ICT and Planning, 2014).

When introducing IoT services in a nationwide manner, conflicts with existing regulation can be a bottleneck. Regulatory uncertainty can also be a large barrier. For example, the current medical related regulations may hamper innovative services by requiring a doctor to be present on both sides of a tele-medicine consultation. With this in mind, the Korean government has established a 'telecommunication strategy council', which will take the initiative to improve general regulations. It will also establish an IoT test bed as a regulation-free zone and aim to improve the legal system.

Further, the Korean government announced the "IoT Promotion Strategy" in December 2015 with the objectives of developing and commercialising IoT-based business models and improving industrial competitiveness by encouraging private investment. The government will invest USD 110 million by 2017. An "IoT Promotion Task Force" composed of officials from different ministries will identify regulations hindering the use of the IoT and suggest reforms. Most, if not all, national governments acknowledge the

need for research in IoT in areas of cybersecurity, interoperability, privacy, energy efficiency, and several other aspects of IoT development.

In Europe, individual countries are investing in research and development on IoT. In the United Kingdom, USD 110 million was allocated in 2014 and previous years (Novet, 2014). France is financing embedded systems and IoT from a USD 55 million fund for digital development, with a new USD 440 million fund expected in 2015 (Barbaux, 2015). In the framework of the German government's "*Industrie 4.0*" strategy, industry-related programmes add up to over USD 500 million during a period of around five to seven years.[50] "*Autonomics for Industry 4.0*" is a technology programme by the Federal Ministry for Economic Affairs and Energy designed to merge state-of-the-art ICT technology with industrial production by exploiting the potential offered by innovation in order to accelerate the development of innovative products.[51] With the 'Smart Service World' technology competition, the Federal Ministry for Economic Affairs and Energy intends to promote research and development activities, thus facilitating innovative ICT-based services.[52]

Canada's largest province, Ontario, launched a new pilot programme to allow for the testing of driverless vehicles on its roads. The province also pledged funding towards the Centres of Excellence Connected Vehicle/Automated Vehicle Programme, which brings academic institutions and business together to promote and encourage innovative technology. In Australia, the State of South Australia has mirrored this approach with the state government introducing legislation to permit on road trials as encouraging R&D and start-ups.[53]

Some governments are providing financial incentives or subsidies (e.g., grants, loans, venture capital support programmes, platforms for industry to showcase new technologies and innovations) to support projects by start-up companies and corporations, many of which utilise IoT technologies. In the United States, the White House announced in September 2015 a new "Smart Cities" initiative. Other major economies such as India and the People's Republic of China have also similar programmes. India's Smart City plan is part of a larger agenda of creating Industrial Corridors between India's big metropolitan cities. These include the Delhi-Mumbai Industrial Corridor, the Chennai-Bangalore Industrial Corridor and the Bangalore-Mumbai Economic Corridor. It is hoped that many industrial and commercial centres will be recreated as "Smart Cities" along these corridors. The Delhi-Mumbai Industrial Corridor (DMIC), which is spread across six states, seeks to create seven new smart cities as the nodes of the corridor in its first phase.[54]

Box 10. The Smart Cities initiative in the United States

Over USD 160 million in federal funds will be invested in research projects and leverage more than 25 new technology collaborations to help local communities address key challenges: reducing traffic congestion, fighting crime, fostering economic growth, managing the effects of a changing climate, and improving the delivery of city services. This initiative includes more than USD 35 million in new grants to build a research infrastructure for Smart Cities by the National Science Foundation and the National Institute of Standards and Technology; nearly USD 70 million in proposed investments to unlock new solutions in safety, energy, climate preparedness, transportation, health and more, by the Department of Homeland Security, Department of Transportation, Department of Energy, Department of Commerce, and the Environmental Protection Agency; and more than 20 cities participating in major new multi-city collaborations that will help city leaders effectively collaborate with universities and industry.

The United States government also hosted a forum coinciding with Smart Cities Week, highlighting new steps and brainstormed additional ways that science and technology can support municipal efforts. The Forum included the creation of test beds for IoT applications and big data analytics, with the intention of helping United States companies to become global leaders in this field.

Source : https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help

A challenge that governments will have when funding research into IoT is measuring returns, but this is analogous to similar challenges in gauging the benefits of other ICT investments. In addition to quantifying gains from improvements in the base components of IoT, such as better M2M, data processing, sensors and actuators will be visible and measurable, there also needs to be measured returns from investment in innovation in applications and the integration of IoT.

Encourage private sector innovation

In several countries, industry has not yet fully utilised the potential of IoT/M2M-solutions. For example, the adaption of IoT by small and middle-sized businesses in Germany takes various degrees: Whereas three out of ten companies state that they have a (very) high degree of digitalisation, while 27.5% state that have not made use of the IoT, or only very little stating that they have a (very) low degree of digitalisation (BDI and PwC, 2015). There are also regional differences with regard to digitalisation as well as differences regarding the different degrees of digitalisation of sales and distribution on the one hand and production on the other hand. Still, due to their size and flexibility, small and middle-sized companies are predestined to implement the ideas of "*Industrie 4.0*". In order to encourage this industry segment, the German government has launched the initiative "Small and Middle-Sized Businesses 4.0 - Digital Production and Work Processes", which aims at supporting these companies with the digital transformation by means of new information and communication technologies and the development of new business areas in the context of the IoT.[55] Several centres and agencies will inform, qualify and support the companies under this initiative. The Canadian government has established a Centre of Excellence for Wireless Communications called Wavefront, which is focussed on the development of M2M and IoT companies in Canada by connecting them with critical resources, partners and opportunities.

The German government has launched innovation clusters that are directly tied to the IoT. For example, the "Cool Silicon" innovation cluster in the south of Germany aims to develop low energy and energy self-sufficient processors and sensors.[56] Another innovation cluster "IT's OWL", in the central part of Germany, focuses on *Industrie 4.0*, where the goal is to create intelligent and autonomous industries through the use of robots.[57] Also in Germany, Microtec Südwest aims to develop microsystem technology, focusing on the areas smart production, smart mobility, smart health and smart energy.[58] A fourth cluster focuses on software for new industries. Each of the research clusters is tied to a large number of businesses, universities, and research centres in this region that combine to deliver the output.

In Denmark, the DOLL initiative in the Copenhagen suburbs is aiming at creating future LED-lighting solutions and to generate jobs. The current initiative, a consortium between Gate 21, Albertslund Municipality, Technical University of Denmark and the GTS institute DELTA, is focusing on energy efficiency and intelligent indoor and outdoor lighting solutions.[59] In June, an extension focused on testing and demonstrating Smart City solutions in DOLL Living Lab was awarded additional funding. The purpose is to look at different types of public services and make them smarter. This could have implications for the operation of roads, sewers, water, energy, traffic and more.

Brazil encouraged the use of IoT by adapting its tax policies. In May 2014, the government introduced a special tax regime for M2M systems without human intervention to foster adoption and use of the IoT. The decree cut fees in SIM activations, and an annual fee for SIM cards, totalling a reduction of 80 per cent. According to the regulator, Brazil now has with 11 million of M2M connections, the fourth most in the world and the most by far in Latin America. Of those, 2.3 million are special M2M connections and 8.7 million are standard M2M connections. The evolution of the number of connections from May 2014, when the Decree took effect, to July 2015 shows large growth of the "special" category, from 161 thousand to 2.3 million; while the "standard" connection have actually decreased from 8.8 million to around 8.7 million. A controversial question is how to separate M2M with human intervention to those without in contexts such as an environmental sensor, a car control system or a home appliance.

Promote skills needed to maximise opportunities in the labour market

The implications of the IoT for labour markets are still uncertain. Understanding how other technological revolutions in the past affected the employment and the global economy may provide some assistance. The introduction and popularisation of the Internet in the 1990s provides a useful benchmark. After 1995, ICT investment increased across the world, with advanced economies and emerging Asia in the lead. By some measures, the contribution of ICT investment to growth roughly doubled in emerging Asia, Latin America, Eastern Europe, Middle East and North Africa, and Sub-Sahara Africa after 1995 (Jorgenson and Khuong, 2010).

Job from ICTs occurs through the mobility of resources – financial capital, knowledge assets and labour – across firms and sectors. By its very nature, this process of structural change takes time and may be hampered by institutional barriers and market imperfections. The diffusion of ICTs is also changing the way work is carried out, raising the demand for different types of ICT skills. In the context of the IoT, the integration of such technologies and methods will require *ICT specialist skills* to be able to develop applications using new frameworks and paradigms or manage new types of IoT networks.

The IoT could bring changes to the labour and workforce in similar ways than the introduction of the World Wide Web has effectively achieved with the media industry, for instance. Traditional media agencies have developed digital expertise in-house to cover customer relationship via the web and social media and new digital agencies have filled up the demand for such services. In such context, there has been a transformation on the skills required to fill these new professional profiles (graphic designers, web developers, social media agents, community managers, and so forth), with a greater opportunity for jobs requiring creativity and more intellectual challenging tasks. As an example, Amazon's AWS IoT platform allows business to connect devices to the cloud and communicate with cloud apps. With such solutions, managers and product developers will require their skills to be upgraded.

In a broader sense, the IoT brings a skills opportunity in several areas such as data curation, open data, big data analytics and cloud computing processing. For each of these areas, there is a need to identify the skills required by future workforce, align the curricula to support the development of the skills and promote training opportunities through a combination of formal and informal methods. Countries that will be able to do so, will be able to position themselves at the forefront of an emerging industry and seize the benefits of the IoT also in the labour market.

Societies influenced under the IoT will create an impetus to change traditional education from one, which in many ways is still designed to fill traditional workforce or assembly line jobs, to one that encourages entrepreneurism, experimentation or invention. Governments and policy makers need to understand how to adapt the education system so that its alignment with industry also improves. Skilling programmes covering both generic and technical skills should adjust displaced workers ensuring that the supply of new skills keeps pace with the new demands in IoT related sector such as sensors, robotics, data analytics and software development. Broad skills strategies, as recommended by the OECD Skills Strategy (OECD, 2012b), will increasingly be required.

Build trust in the IoT

Privacy, security, liability, reliability and consumer rights are affected by the pervasiveness and longevity of the IoT. Policy makers should ensure that the diversity of policy and regulatory frameworks in place globally enable trust in the IoT[60]. These frameworks, both domestic and international, should be interoperable in nature because IoT goods and services will be sold on a global scale and consumers will often want these devices to work wherever they are. Interoperable frameworks could provide consumers and businesses with greater certainty when purchasing and manufacturing IoT goods and services.

The current approach towards different national or regional frameworks is finding compatible regimes that can interoperate. There are already a number of regional and international frameworks that could be built upon such as the *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, the *OECD eCommerce Guidelines*, the *Council of Europe Convention 108* and the *APEC Privacy Framework* (OECD, 2007; COE, 1981; APEC, 2005) to name a few of them. To the extent issues arise that are unique to the IoT, it may be necessary to create additional frameworks or revise the existing ones. An example of current practices in this area is the joint working group of the Article 29 Working Party and the APEC Data Privacy Subgroup on the development of tools that help companies become certified and approved both under the EU Corporate Rules ("BCRs") and the APEC Cross-Border Privacy Rules (CBPRs).

In some ways, many of the IoT objects in people's homes will become household goods that have traditionally had much longer replacement cycle (8 to 15 years for washing machines for instance). Devices are expected to work for these periods and in some countries consumers can lay claim to warranties during the reasonably to be expected lifetime of a device.[61] For consumers, the question with IoT enabled devices is whether their IoT functions will be supported for the lifetime of the device and whether software updates might improve performance or even introduce new features.[62] IoT device makers may gain a competitive advantage by offering such updates. Transparency and truthfulness in advertising should be key consumer policy issues. The information provided to consumers at the time of the purchase should clearly indicate what expectations a consumer should have over the lifetime of a device with regards to the functioning of and updates to the software on the device and to the apps that are controlling it.

The complex structure of the IoT market may obscure which provider is responsible for a particular problem in the value chain, but also which authority can help consumers and be involved in the policy decision-making and enforcement process. In the case of a malfunction for an IoT object, it should be relatively easy to point to a responsible party. A connected light bulb, for example, may work well in a store but not connect to the consumer's home network. This raises the question of who is responsible as the problem may be in the wireless connection of the bulb, in a home network or in the software managing the system. Consumer policies could give some guidance on the responsibility for such issues.

The challenge for regulators is that there is no coherent approach that brings the various elements of this problem together. There are consumer rights issues (liability, longevity, and compatibility), privacy issues (data collection, use and processing) and security issues (vulnerability, upgradeability). Depending on the country there may be multiple agencies involved in dealing with the resulting issues. It is likely that regulators will primarily step in after breaches of security, privacy or consumer rights have happened and regulation may be more incident-driven than from a coherent policy approach. This could also lead to trade issues, when different countries have different rules and it then becomes difficult for businesses to facilitate the various demands.

In the United States, the National Institute for Standards and Technology (NIST), the standard-setting body for federal agencies, released its draft Framework for Cyber-Physical Systems in 2014. The Framework is intended to serve as a common blueprint for the development of safe, secure and interoperable systems, including IoT systems such as smart energy grids, wearable devices, and connected cars.

In the European Union, data protection rules are currently under review and shall be adopted in a future General Data Protection Regulation. The aim of the reform is to strengthen individual rights of citizens and to ensure a high standard of protection adapted to the digital era. Protection is increased inter alia by the following rights: easier access to data, a right to data portability which shall make it easier to transfer personal data between service providers, enhanced transparency (e.g. informing about a privacy

policy in clear and plain language), a right to erasure of personal data and "to be forgotten" as well as limits to the use of "profiling" (Council of the European Union, 2015). It is expected that the new rules will be adopted in 2016 (Council of the European Union, 2015). The Art 29 Data Protection Working Party issued recommendations on the application of current European Union rules on data protection to the IoT. One suggestion is to incorporate privacy issues in the design phase ("privacy by design" process) and make the terms of data collection and processing more user-friendly (Article 29 Data Protection Working Party, 2014).

The ongoing development of separate responses to emerging technology developments risks an overall loss of regulatory coherence, with consequences for industry participants in terms of increased compliance costs. For consumers, increased complexity and regulatory fragmentation can make it more difficult to manage their communications experience. A single regulatory framework, or at least a joint approach, for addressing the changing dimensions of IoT activities would offer a more coherent arrangement for both businesses and consumers engaging in such activities.

Better information for consumers in a digital world should not only be the aim with regard to data collection and processing but also with regard to a company's general terms and conditions. Such consumer information should be simplified and made more comprehensive. This holds in particular true for the use of apps and intermediary platforms (e.g. Google, Facebook). New, simple and creative forms of consumer-information are advisable (e.g. short summaries/"one-pager", icons/pictograms). To strengthen private sector implementation of data protection practices, consumer associations could offer educational programmes with regard to the digital world as well as better interaction with supervisory authorities. The German government programme "More security, sovereignty and self-determination in a digital economy" supports such actions (BMWi and BMJV, 2012).

Further develop open data frameworks

The IoT is built around data, particularly its communication and analysis. Where governments have access to open public-sector IoT data from transportation systems or other infrastructure, they could further develop frameworks that allow for the re-use of public sector IoT data. This would allow industry to share their open data for public benefit and allowing interested parties access to a new range of open data. Government data is generally available under re-use conditions, but these frameworks could encourage broader public use of open data from other sources. Public data reuse is a very appealing area that also requires some degree of care in order to balance against unintended data usage or privacy loss.

Public sector information is defined by the *OECD Recommendation for enhanced access and more effective use of public sector information* as: "information, including information products and services, generated, created, collected, processed, preserved, maintained, disseminated, or funded by or for the Government or public institution" (OECD, 2008b). The OECD Council Recommendation aimed "to increase returns on public investments in public sector information and increase economic and social benefits from better access and wider use and re-use, in particular through more efficient distribution, enhanced innovation and development of new uses." In addition, "to promote more efficient distribution of information and content as well as the development of new information products and services particularly through market-based competition among re-users of information."

Apart from the OECD Council's Recommendation, the value of access to and re-use of public sector information was acknowledged in frameworks such as, the European Directive on the re-use of public sector information (European Parliament and European Council, 2003) and the Freedom of Information Act in the United States. The Internet has made the use of such data easier to access and more widely available. Particularly the development of the site: Data.gov in the United States can be seen as a catalyst in governments publishing and re-using data, with many governments following suit with similar sites.[63]

Such sites have served as a catalyst for other data to be put online. Though the data sets are very varied, they also contain data that could be characterised as IoT generated data or data that can be combined with private IoT data. Many governments have also followed up their sharing of data with contests and "hackathons" to stimulate new and creative use of these data.

Government generated data has been reused in a variety of ways. For example:

- The authorities in London have been very active in opening access to data. Transport for London data has led to a number of apps that support travellers in London. The council of Westminster provides real time access to data from parking sensors.

- Real time data feeds on flights have led to flight tracking websites and mobile phone apps that update travellers on the status of their flights, potentially indicating to passengers their flights are delayed even before airport announcements.

- Meteorological data, such as rain radar websites[64] has become very popular with users. This data often has to be licensed for a fee, but some businesses have created models, which enable them to give access to the data for free.

- The government in the Netherlands publishes every 10 minutes data on water levels throughout the country and the prognosis for expected water levels (Ministerie van Infrastructuur en Milleu, n.d.). Professional users then use such data, such as on ships, as do recreational users, such as divers.

- In the European Union, a harmonisation measure aims at granting access to digital geo-data generated by public authorities (European Parliament and European Council, 2007).[65]

- In France the Government passed a bill with an open-data policy that makes official documents and public sector research accessible to everyone online (French Government, n.d.)_

- The Municipality of Aarhus in Denmark shares real-time traffic information to enable smart city innovation within traffic and mobility, and provides a visual map of the space available at its recycling stations through open garbage data.[66]

The private sector also collects data that can be of use for the public sector. For example, data collected by *TomTom* are actively used by governments to evaluate the effect of changes in road conditions. In Scandinavia, Volvo Cars, the Swedish Transport Administration and the Norwegian Public Roads Administration are working together on a project to enable vehicles to share information about conditions that relate to road friction, such as icy patches. The information will be shared through a cloud-based network – a revolutionary approach to improving traffic safety. It is being tested on a fleet of 1000 vehicles, though this is expected to be expanded to cover all vehicles (Volvo Cars, 2015). Sensor data was available to vehicles for two decades as part of the electronic stability control but since November 2014, such systems are a requirement on all new vehicles sold in the European Union. The IoT only needs to add communication to make the data available to other services. In Norway and Sweden the data will be used to caution other drivers, but also to warn the various road services and their contractors of adverse road conditions.

When there is private data that could be beneficial for public use, authorities need to consider balancing the benefits for the individual market player with a public good. It could be said, for example, that data or road conditions could be beneficial to a corporation to make its vehicles safer than those of

competitors by sharing these data among drivers of that company's vehicles. Certainly innovation that promotes safety should be rewarded. On the other hand, the drivers of these vehicles will almost certainly wish for these data to be shared with the drivers of other brands, as it is in their interest for conditions to be made safer for all drivers. In addition, drivers as consumers would likely not want to see network effects, where their choice of purchasing a vehicle was governed by the wish to access the brand with the most vehicles on the road, and therefore the best data, rather than the one that best suited their other requirements. Hence, there are compelling reasons why drivers are likely to grant their consent to such use of their data. However, it is possible that not all drivers wish to share their data. Even if the public value of preventing accidents must take priority, a public debate is necessary concerning the questions if and to which extent the drivers' data may be used in order to help achieve this aim.

Consider adapting numbering policies to foster competition and innovation

The IoT needs various forms of identifiers to address devices in networks. The type and number of identifiers required depends on their connectivity model: tag identifiers such as Universal Product Codes (UPCs) or RFIDs; Object Identifiers (OID) and Digital Object Identifiers (DIO); layer-2 numbers that uniquely identify the device within a given network, such as MAC-addresses; global routing addresses that allow for routing of data across different networks, such as IPv4 and IPv6 addresses; service specific addressing, such as domain names and telephone numbers and global identity numbers that allow for the identification of the network responsible for the device. In the following paragraphs, there is a description of the identifiers, which might require some form of government attention due to their importance in unlocking larger benefits for the IoT.

IPv6 as a fundamental enabler for the IoT

Increasing demand for IoT applications may accelerate the deployment of IPv6. According to data from Cisco, 21% of M2M connections will be IPv6-capable, reaching 2.2 billion by 2019, a 64% compound annual growth rate. Some argue that the use of IPv6 would also alleviate shortages in telephone numbers and IMSI-numbers. These numbers are, however, still likely necessary to identify a device in a mobile network, over which IPv6 is run.[67] And many applications, especially equipment with personal sensor networks do not use IP at all (health monitors, smart-watches, NFC payment terminals) but a LAN gateway.

Some existing deployments of sensor networks and mobile devices are using the existing IPv4 network. This is seen as a simple pragmatic choice of using what is available. Estimates vary, but there is some level of consensus behind a figure of eight billion to 10 billion Internet-connected devices in 2012. At that time, the Internet had used some 2.5 billion addresses, meaning that the majority of these connected devices are located behind conventional Network Address Translation (NAT) units that allow one IPv4 address to be shared across multiple devices simultaneously. IPv4 addresses are, however, a very limited resource and the five regional Internet registries have either fully assigned those available to them or will do so in the near future. In 1996, the Internet community developed IPv6 in preparation for this eventual exhaustion of IPv4 addresses. IPv6 expands the protocol address space to 3.4×10^{38} addresses instead of the 4.3 billion addresses of IPv4, this is effectively more than 7.9×10^{28} times as many as IPv4.

IoT devices connecting directly to the Internet would greatly benefit from the massively expanded protocol address space that only IPv6 can provide. At the same time, network providers can identify the IoT market as a compelling use case to justify the additional expenditures associated with a widespread deployment of this new protocol. This raises the question of whether IPv6 could be seen as an enabler for IoT systems which otherwise would require to be deployed within today's framework of address sharing of IPv4 and IPv6. Much of the debate over this question relates to the nature of the embedded device and the way in which it communicates within its external environment. In addition, it can be noted that many IoT

scenarios can rely on devices communicating to a local gateway, with only the gateway being Internet-connected.

For some sensors and devices, IPv6 is generally thought to be a necessary precondition. Using IPv6 for dozens of millions of micro devices, however, makes them vulnerable since they are exposed to the whole Internet. This has critical issues relating to security and abuse, and the experience of such devices has highlighted the risk of such addressable devices being co-opted into participating in various forms of high volume distributed Denial of Service (DOS) attacks. The question of whether the larger address space of IPv6 effectively prevents the opportunistic discovery of sensor devices, or whether operational prudence requires that such exposed sensors are equipped with robust security and continual monitoring and maintenance, is at present an open issue for the sensor industry. The technical community is engaged in strengthening the Internet architecture against various forms of abuse, such as efforts to prevent IP address spoofing within access and hosting networks

Not having IPv6 active in many networks makes the discussion moot. Promoting the IPv6 transition is the most effective way to support the IoT. With the current address depletion scenario, the deployment of IPv6 is inevitable for the Internet to continue to operate and is the only future-facing "Internet" in the IoT. It is difficult, however, to see what governments can do to further accelerate IPv6 to support the IoT. Many governments have already established promotion programmes to adjust Internet services for which they have responsibility, adapted government purchasing and established task forces with industry and the Internet technical community.

Telephone numbers for the IoT

Telephone numbers have become so engrained with the operation of mobile and satellite networks that their availability is assumed. Billing systems, customer relationship management systems, network management systems and roaming management systems all assume the existence of a telephone number. In addition SMS, which is often used to wake-up a sleeping device, assumes a phone number, particularly in situations where a device is roaming. The result is that numbering policies may need to be adapted to fit the IoT.

The Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT) published a report on scarcity of E.164 numbers due to M2M, with an outlook to 2020 (ECC, 2010). The report concluded that seven of the 29 countries were expected to face problems with the exhaustion of existing E.164 numbers and another two could face a similar scenario. Several European countries have updated their numbering policies reflecting ECC/CEPT considerations. Netherlands and Norway, for instance, have introduced dedicated M2M number ranges for mobile. Sweden also introduced separate dedicated M2M number ranges for fixed and for mobile whereas Belgium and Spain have a non-geographic, fixed-mobile agnostic network code dedicated to M2M. In addition, Japan is expecting to allocate a dedicated block of mobile numbers for M2M communication during 2016. Whether a country decides to have a dedicated M2M numbering range or not, always depends on the specific national situation regarding number exhaustion.

For numbering, flexibility is essential as different services or M2M users may have different requirements. Both, industry makes use of national numbers in an extra-territorial way (e.g. extra-territorial use of national numbers) as well as of international numbers in order to deploy IoT connected services. Furthermore, regulators should carefully assess introducing additional, and remove existing, restrictions or administrative barriers related to the assignment and use of numbering resources, as it could act as a barrier to the roll-out of a global M2M market.[68]

Solutions to facilitate provider switching and avoid lock-in

When connectivity is provided via SIM over public mobile networks, switching the connectivity service provider is a key issue regarding the development of IoT services and the functioning of the market. At present, switching connectivity provider requires a hardware modification of the connectivity module of the device, which will require technicians to replace SIM cards or communication modules. There are two solutions being researched by industry and/or numbering administrators that could meet M2M user's expectation and solve this issue: the assignment of MNC, and hence a range of IMSI numbers, for large IoT users such as automobile manufacturers or utility companies (energy, water, etc.); and the use of over-the-air (OTA) provisioning of the Subscriber Identity Module (SIM), requiring the use of reprogrammable eUICCs.

Firstly, the assignment of MNC numbers to IoT players would allow them to manage their own range of E.212 IMSI numbers, switch between several MNOs or become an MVNO themselves. Ericsson calls such networks Private Virtual Network Operators (PVNOs) and in principle one user needs only one IMSI-range for it to work globally. Several vehicle manufacturers, consumer electronics companies and energy companies have expressed their interest in this solution to the lock-in issue. The Netherlands has already changed its regulations.[69] The Dutch Ministry of Defence uses a range for its own communications and a utility company, Enexis, used their own range for a 2.6 million smart-meter roll-out (Enexis, 2015). Germany and Belgium have consulted on regulatory changes.[70] Germany opened up its numbering scheme so that besides MNOs also MVNOs and MVNEs may apply for a block of IMSI numbers; however, a corresponding right was not granted to large-scale IoT users.

CEPT ECC has researched the changes and proposes that countries consider relaxing their allocation rules in order to allow for PVNOs. They have also advised the ITU to change the E.212 recommendation to allow for the emergence of PVNOs. This is in order to provide the flexibility to authorities to decide, at a national level, if a PVNO shall be granted a right to request an IMSI–range or not due to any limitations in their availability (i.e. scarcity). Even with their own IMSI-range and the ability to issue its own SIM cards, PVNOs would still need a contract with an MNO or MVNO in order to get access to a mobile network. The main difference is that broadening the possibility for access to IMSI-ranges makes this a decision for each large-scale IoT user to meet their own requirements (ECC, 2014). One automobile manufacturer estimates that the combined savings would be around 1 USD per vehicle per month, which given a life time of 15 years for vehicles, would be the equivalent of 180 million dollar per one million vehicles manufactured per year (or the equivalent of USD 2 billion per year for all vehicles manufactured in Japan or the United States).[71]

A second solution has been suggested in ETSI/3GPP standardisation circles and it entails to use over-the-air (OTA) provisioning to switch service provider. The GSM Association, an industry group of MNOs, is proposing its own *de facto* standard supported by many but not all its members, which is a step forward in standardisation but not yet a global solution (GSMA, n.d.). The OTA solution requires the use of reprogrammable SIM-cards, also called eUICCs. Such a solution would allow large scale users of IoT the possibility to change mobile operators through an over the air update of the IMSI-number and relevant security credentials of the SIM. This approach would be operator led and it could be combined with a multi-IMSI solution, where the credentials of multiple networks are stored on the SIM.

Many large scale IoT users would like to use OTA, either in order to easily update the installed base of their connected devices when they switch service provider or for their own business purposes, for example to be able to sell a business unit and all associated IoT devices and service contracts without having to retain a business relationship. In this light, there is the chance that development towards a standardised OTA process is driven by industry (e.g. Apple, the automotive industry) and developed within ETSI. No dates for an OTA standard are available at the time of writing this report.

Both a PVNO solution and an OTA solution have advantages and drawbacks. An OTA solution is at present more limiting than a PVNO solution for practical reasons. If an IoT user wants to make a change using OTA, it will always depend on the cooperation of mobile operators and it will certainly not be instantaneous for all devices, in part because it takes time to update devices, and because not all devices will be on at all times. For example, vehicles and consumer electronics may be off for long periods of time. In addition, there is limited space on a SIM-card and mobile operators do not want to reserve numbers for potential customers, so for customers that are roaming occasionally the device may not be able to select a less expensive local offer, because the credentials have not been updated. If the PVNO solution is used, switching across connectivity service provider requires seamless transition without interruption. This is particularly important for mission-critical services such as connected cars. Hence, an uninterrupted transition would presuppose that all contracts and routing are changed accordingly at an effective date. To date, no process exists to guarantees such seamless transition. In addition, in order to conclude contracts with multiple mobile networks in a country, national roaming would need to be supported, either voluntarily by network operators or by law. Another important drawback is that the PVNO solution most probably would lead to a scarcity of E.212 resources since in most cases only 100 IMSI-blocks (mobile network codes, MNCs) can be assigned per country, or more specifically per mobile country code (MCC).[72] Even if it is in principle possible for a country to apply for a new MCC at ITU, these resources are not limitless.

If in the near future market players cannot reach a solution on a standardised switching process which is workable, sufficiently secure, transparent and non-discriminatory, governments might want to consider regulatory intervention in order to foster, or to make mandatory, OTA provisioning in order to facilitate switching the service provider in the IoT context (BEREC, 2015).[73] Similar to the provisions on number portability in e.g. Article 30 of the European Union Universal Service Directive, governments could prescribe that the switching process via OTA provisioning has to occur in a synchronised manner so that all connected devices of an IoT customer are switched to the new connectivity service provider at the same time and/or within a short time frame. In order to respond to violations of such provision, it would need to be supported by adequate sanctions.

In the auspices of ECC/CEPT a working group "Project Team Future Numbering Issues" is at present working on a deliverable on the assignment of MNCs (E.212) to other entities (M2M-users) than providers of electronic communications networks and services. Another working group "Project Team Number Portability" is at present working on a deliverable on switching in the M2M-sector (OTA, embedded SIM, soft SIM etc.).

Extra-territorial use of numbers

The IoT will bring many applications that will traverse borders, particularly in transport, heavy machinery and consumer electronics. The numbers that are used by these machines will cross borders with the machines, often for prolonged periods. For regulators this raises the question of whether they allow the use of their national numbers across borders or whether they allow use of foreign numbers in their territorial jurisdiction on a permanent basis ("extra-territorial use"). It has been discussed at international level for quite some time whether extra-territorial use of numbers shall be permitted for M2M services. Until a solution is found, large-scale IoT users would need to check with each national regulatory authority prior to any extra-territorial use of numbers if they want to obtain legal certainty. There is also the risk that a country does not allow such extra-territorial use. This would make it very difficult for a large-scale IoT deployment to function in multiple countries, by using one mobile operator's solution.

The problem of extra-territorial use of numbers arises both for E.164 numbers (typically mobile numbers in M2M) and E.212 numbers (IMSI).[74] Typically, both are used for IoT services. Outside the IoT context, the extra-territorial use of numbers has so far been limited. Mobile roaming is the most well-

known example but given that it is short-term, hasn't attracted a close scrutiny from regulators. There are some VoIP services that allow the nomadic use of E.164 telephone numbers. Regulators have generally frowned upon such use and only allowed it in exceptional circumstances (ECC, 2013). In practice businesses do sometimes use foreign E.164-numbers, to purport to have a local presence.

With regard to the IoT, there appears to be more and more extra-territorial use of numbers. In practice operators are already using international numbers abroad. Statistics collected by the OECD show that Sweden leads the OECD in number of M2M devices deployed per capita. However, when asked about these numbers they appear to be in use by Telenor for its M2M devices, which are deployed globally. It is also reported that numbers from the Netherlands, Malta, Luxembourg and some islands are used globally for M2M purposes. This is because it is possible to buy national roaming and failover for these devices in the countries where they are used, unlike the use of a national number.

Authorities could, however, reconsider their positions and evaluate whether it is possible to open the extra-territorial use of these numbers. Only where there is provable harm, such as the risk of national number exhaustion, should countries restrict how the numbers are used. Currently, work on extra-territorial use of E.164-numbers, including IoT/M2M, is being carried out within CEPT at the "Project Team Future Numbering Issues"(ECC, 2013). In Belgium, the regulator has recommended to allow extra-territorial use of numbers in the M2M context without any further conditions (BIPT, 2015). In the United States, the regulation does not prohibit extra-territorial use of numbers either. Denmark has not yet made a formal decision regarding use of Danish numbering resources on a permanent basis in other countries. Germany is consulting on a numbering plan and requirements to permit the extra-territorial use of IMSIs in the M2M context, with the possibility to intervene in case of harm to public or private interests.

Access to efficient numbering schemes is essential to the operation of the IoT as was underlined by the European Commission's DG CONNECT Director General (Viola, 2015). In this respect they are no different than other identifiers, such as IP addresses. IP addresses are allocated to network operators on the basis of demonstrated need and are governed by allocation policies established through the community processes of the relevant Regional Internet Registry.[75] This regional approach to the management of unique identifiers has resulted in IP addresses with a global scope and has worked for 25 years without difficulty.

In addition, the international shared country codes issued by the ITU to some telecommunication operators with international footprints may play a role in meeting demand for cross-border IoT usage. Such international numbering resources may be used worldwide. For example, it is noted that more and more MNOs and full MVNOs as well as providers of IoT service platforms have become assignees of an MNC under the shared MCC 901 as well as under the shared country codes (CCs) 882/883.[76]

NOTES

1 See for example ECC Report 153, Numbering and Addressing in Machine-to-Machine (M2M) Communications, November 2010, p. 5, section 1: "M2M is a communication technology where data can be transferred in an automated way with little or no human interaction between devices and applications."

2 For an entertaining list of milestones in the evolution of the mashing of the physical with the digital, see Press, Gil (2014).

3 See, for instance, Weiser (1991).

4 See, for instance, "We put a chip in it" blog at http://weputachipinit.tumblr.com/

5 See trend 3 on Machine-to-Machine communications (M2M) from Cisco (2015).

6 See Wilson, J. (2008).

7 The number of M2M SIM cards/modules only indicates the number of M2M devices which use mobile connectivity. However, M2M communication may be based on all kinds of connectivity and mobile connectivity only represents a small part of connectivity used in M2M communication.

8 General Electric adopted this name to describe the innovation and change that could come from the union of physical world and the digital world. Estimations for gains of 10-15 trillion USD to global GDP over 20 years, see page 3 of Evans and Annunciata (2012).

9 General Electric estimates for 1% savings across several industries and segments, see page 4 of Evans and Annunciata (2012).

10 A Baxter robot can be purchased for USD 22 000, which can be far less expensive than comparable robots and can be programmed quickly on the job in a matter of minutes, unlike traditional industrial robots that require days or weeks of highly specific programming by dedicated engineers. This robot is already available across a number of OECD countries and is supported by an active development community, see Rethink Robotics (2014).

11 In a field test, the agriculture machinery producer Claas worked together with Deutsche Telekom AG to digitize the harvesting process. The driver of the harvesting machine could use tablets with constantly updated representations of harvesting operations. The harvester, for example, detects when the grain tank is full and automatically calls a tractor for off-loading. Each machine knows the terrain and all equipment locations and looks for the best possible way to the destination. Here, the system pays attention to time optimization and soil protection. Moreover, the analysis of data on soil, wind, weather or the optimal sowing and fertilizing parameters for each square meter of a field opens the seed and chemical companies new business opportunities. They can evaluate the data of the land and make optimized offers - a package tailored from seed, fertilizers and pesticides to the customer and the field in question.

12 See the websites of John Deere or Lely for many examples of such developments.

13 See Murray (2015) and a description of the technology at: http://www.proteus.com/technology/digital-health-feedback-system/

14 Alexis Normand of 'Withings' emphasised in a presentation at the 2014 OECD Technology Foresight Forum that "measures foster results". He stated that individuals weighing them self, on a daily basis

compared to weekly or monthly monitoring, could improve their management of weight, and change dietary habits.

15 Alexis Normand of "Withings" stated that in some countries, for example, medical practitioners only get paid for a physical visit by a patient, whereas time spent monitoring a patient or interacting with them through other communication tools may not be reimbursed. Instead of "…the fee-for-service model, under which health providers were reimbursed for each consultation or medical intervention", healthcare provision may evolve "…to one where payment is made for packages of care delivered by teams".

16 The DOLL initiative in the Copenhagen suburbs is aiming at creating future LED-lighting solutions. DOLL's aim is to create energy efficiency and intelligent indoor and outdoor lighting solutions, and to generate jobs. DOLL supports municipalities, regions and private companies, in cooperation with scientists, with the development of new and improved lighting solutions. For further information see http://www.lightinglab.dk/UK/About-DOLL/

17 LED street lights are significantly more energy efficient than traditional streetlights, saving up to 50% in energy use, or roughly 30-50 USD per street light/per year.

18 The Vehicle SCOOT system developed by the Transport Research Laboratory in collaboration with the UK traffic systems industry, which uses sensors at intersections to gather traffic data and a computer system that adjusts light timings to allow traffic to flow as efficiently as possible. For further information see http://www.gizmag.com/pedestrian-scoot/31154/

19 See results of introducing SCOOT http://www.scoot-utc.com/GeneralResults.php?menu=Results

20 Autonomous Intersection Management: Traffic Control for the Future, University of Texas, https://www.youtube.com/watch?v=4pbAI40dK0A

21 These are non-operational vehicles, meaning they do not have an active military role, such as cars, vans, small trucks.

22 See (Tudor and Fabro, 2010).

23 Ford announced a switch to over-the-air updates in March 2015 see Sorokanich (2015). and BMW used wireless updates to patch a hackable security flaw in door locks in January. February 2015. https://securityledger.com/2015/02/bmw-fixes-connecteddrive-flaw-with-over-the-air-patch/

24 See GSMA IoT Security Guidelines at www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/

25 For more information on the project, visit www.owasp.org/index.php/OWASP_Internet_of_Things_Project

26 For more information see Cloud Security Alliance (2015).

27 For more information see https://www.ftc.gov/news-events/blogs/business-blog/2015/01/internet-things-ftc-staff-report-new-publication-businesses

28 See Office of Privacy Commissioner of Canada (2016).

29 See White House (2014).

30 Study carried out by the group "La Poste" in December 2014, see http://www.docapost.com/wp-content/uploads/2015/01/infographie-la-poste-generique.pdf

[31] Global M2M Internet (IP) traffic: From 1% (2014) to only 3% in 2019. See Cisco (2015c).

[32] The US based companies are Intel, IBM, Google, General Electric, Qualcomm and Cisco. See http://www.cbronline.com/news/internet-of-things/behold-the-10-biggest-iot-investments-4549522

[33] Wehkamp.nl, a Dutch online retailer, which announced in October 2013 that it would build the world's largest robotic distribution centre to replace its traditional warehouse, exemplifies that the market is moving in this direction. This centre will enable order-to-package times of 30 minutes and same day delivery, which customers will likely appreciate. Robots will manage the warehouse, pick goods and move to and from picking stations, where employees will pick and pack the goods. A clip of the announcement and the new Distribution centre can be seen at http://www.youtube.com/watch?v=Q5eie0IgccY

[34] Thielman (2015) mentions 2025 for a self-driving truck by Daimler.

[35] See for example a recent study by the Association of German Chambers of Commerce and Industry (Deutscher Industrie- und Handelskammertag, DIHK), "Wirtschaft 4.0: Große Chancen, viel zu tun", cf. www.dihk.de/ressourcen/downloads/ihk-unternehmensbarometer-digitalisierung.pdf

[36] An example is revolving doors that have a number of safety sensors integrated. Such sensors have to be connected using wires and cannot be wireless. A manufacturer of such doors suggested that such sensors could be operated wirelessly, simplifying construction and allowing new solutions. However, the codes require a wired solution, though it is for some manufacturers unclear why a wired solution is safer than a battery operated wireless solution. The standard covering powered doors (sliding and revolving) is in Europe En16005. This example was told orally by an engineer at a major manufacturer of revolving doors, when asked where the IoT would be of influence in his business.

[37] Luxemburg follows Portugal, Belgium and Denmark, where plans were announced earlier this year. The network already operates in France, the Netherlands, Spain and the UK (Bourne, 2015).

[38] WG3 has published interoperability documentation to support SDOs and businesses: an IoT Landscape and IoT LSP Standard Framework Concepts, presenting the global dynamics and landscapes; IoT High Level Architecture (HLA) that may be applicable to Large Scale Pilots. The HLA takes into account existing SDOs and alliances architecture specifications; and IoT Semantic interoperability recommendations for IoT LSPs.

[39] "*Unlicensed spectrum*" in understood as a general authorisation, which may contain generic conditions of spectrum use but not addressed to a specific operator (see for example the definition of "general authorization" in the EU authorisation Directive 2002/20/EC).

[40] The regions 2 and 3 have not foreseen the 433 MHz band. With regard to the 433 MHz band in Europe, cf. Radio Regulations Footnote 5.138. "5.138 The following bands: […] 433.05-434.79 MHz (centre frequency 433.92 MHz) in Region 1, except in the countries mentioned in No. 5.280, […] are designated for industrial, scientific and medical (ISM) applications. The use of these frequency bands for ISM applications shall be subject to special authorization by the administration concerned, in agreement with other administrations whose radio communication services might be affected. In applying this provision, administrations shall have due regard to the latest relevant ITU R Recommendations."

[41] See Burns (2011) and http://www.comscore.com/Insights/Press-Releases/2012/4/iPhones-Have-Significantly-Higher-Rates-of-Wi-Fi-Utilization

[42] A study looking at the economic value of license-exempt spectrum estimated that the unlicensed Wi-Fi use provided a consumer surplus of between USD 52 billion to USD 99 billion per annum globally, by enhancing the value of fixed broadband connections. This study estimated a further value of between USD

560 billion to USD 870 billion per annum in 2020 for machine-to-machine communications (M2M) using Wi-Fi (Thanki, 2012).

43 Base stations transmit the wireless power with less than 40% efficiency nowadays, that's more than 60% of their consumed power is wasted as heat by their transmitters, more specifically, mainly by their power amplifier. See http://www.radio-electronics.com/articles/rf-topics/utilizing-sdr-for-greener-wireless-communication-157

44 Minutes 40th ECC meeting, ECC(15)063 Rev1(1), Helsinki, Finland 20th June- 3rd July 2015 with further references. It is noted that there are other views on that, also among CEPT countries. In particular the UK point out the benefits of dedicated spectrum for IoT/M2M applications, cf. Ofcom (2014a).

45 Ofcom (2014b) , p. 7, fn. 4: "The 870 – 876MHz and 915 – 921MHz bands were made available on a licence exempt basis on 27 June 2014. We will also be consulting on proposals to authorise the use of higher duty cycle Network Relay Points in the 870 – 876MHz band. ". See also Ofcom (2015), sections 1.4.1, 1.2.2, 5.1, 5.15.2, 7.15, Annex A A.1 1.1.1.

46 See http://stakeholders.ofcom.org.uk/consultations/radio-spectrum-internet-of-things/statement/

47 FCC (2014), p. 4: There is as yet no consensus definition of 5G, but some believe it should accommodate an eventual 1000-fold increase in traffic demand, supporting high-bandwidth content with speeds in excess of 10 gigabits per second (Gb/s); end-to-end transmission delays (latency) of less than one-thousandth of a second; and, in the same networks, sporadic, low-data-rate transmissions among an "Internet of things" ─ all of this to be accomplished with substantially improved spectral and energy efficiency.

48 See for example: Government Office for Science (2015)

49 CI-FIRE is part of the European Union's programme for experimental platforms (FIRE). This programme has brought Europe large-scale test beds and platforms covering a wide range of applications, services and technologies for the Future Internet. http://www.ci-fire.eu/about-us

50 See http://www.mittelstand-digital.de/MD/Redaktion/DE/PDF/endbricht-industrie-4.0-kurzfassung,property=pdf,bereich=md,sprache=de,rwb=true.pdf

51 Cf. http://www.digitale-technologien.de/DT/Navigation/EN/Foerderprogramme/Autonomik_fuer_Industrie/autonomik_fuer_industrie.html.

52 Cf. http://www.digitale-technologien.de/DT/Navigation/EN/Foerderprogramme/Smart_Service_Welt

53 See http://dpti.sa.gov.au/driverlesscars

54 See http://www.makeinindia.com/article/-/v/internet-of-things

55 See http://www.mittelstand-digital.de/DE/Foerderinitiativen/mittelstand-4-0.html

56 Cf. https://www.cool-silicon.de/

57 Cf. http://www.its-owl.de/home

58 See http://microtec-suedwest.de/en/.

59 See http://www.lightinglab.dk/UK/About-DOLL/

60 The notion of "building trust" can be assimilated to the concept of "building trustworthiness", were trust must be properly earned and can be lost under certain circumstances. See O'Neill (2012).

61 The Netherlands is one such country, where there is no legal limit to the length of a warranty. If a clothes dryer of a good brand fails after four years because of a failure in the control circuits, the vendor may have to replace it without cost. The customer could have reasonably expected it to function and wear and tear should not fundamentally affect a circuit board of an otherwise well-functioning clothes dryer.

62 A positive example is Tesla, the electric vehicle manufacturer, who regularly updates the software on its vehicles to improve their performance, or even to introduce new features, such as self-driving (Rundle, 2015).

63 See for example data.gc.ca, Publicdata.eu, data.gouv.fr, data.go.jp and data.gov.uk

64 One of the most popular sites in The Netherlands is for example www.buienradar.nl

65 The directive covers spatial data sets which fulfill certain conditions, inter alia that they are in electronic format. For example, Germany has transposed this directive by adopting the "Law on Access to Digital Geodata".

66 The Municipality of Aarhus' open data portal is available at http://www.odaa.dk/ .

67 While mobile numbers will continue to be used as identifiers in the medium-term, it is likely that they will not be the only solution in the long-term. As noted in Ofcom's 2015 Statement on IoT: *"1.25 We believe that limits on the availability of telephone numbers will not be a barrier to the development of the IoT as a range of alternative identifiers, such as Internal Routing Codes, equipment identifiers and IP addresses could be used"*.

68 Some traditional consumer protection requirements commonly associated with E.164 numbers, such as number portability, are not needed or appropriate in the IoT context.

69 The Dutch regulations are available at http://wetten.overheid.nl/BWBR0010199/geldigheidsdatum_13-05-2015. Note that the current regulations require PVNOs to share 2 IMSI ranges, one for commercial companies and one for public organisations.

70 The Belgian consultation is available at http://www.bipt.be/public/files/nl/21394/Consult_review_KB_Nummering_NL.pdf

71 Vehicle production statistics per country are available at http://www.oica.net/category/production-statistics/

72 This is due to the fact that in most countries, MNC are only 2-digit long.

73 CEPT ECC is also currently assessing how switching and competition in the M2M sector can be facilitated using OTA provisioning of SIM.

74 With regard to E.212 numbers (IMSI), Annex E of the ITU-T E.212 which provides for an approval mechanism for certain types of extra-territorial use of MNC/IMSI, does not fit to scenarios of extra-territorial use in the M2M context. Rather, it addresses situations like extra-territorial use of MNC/IMSI numbers of a bigger state in a small country (e.g. extra-territorial use of Italian IMSI in Vatican or San Marino).

[75] Five Regional Internet Registries are responsible for coordinating and allocating global Internet resources and related services, including IP addresses: the American Registry for Internet Numbers (ARIN), the Latin American and Caribbean Network Information Centre (LACNIC), RIPE Network Coordinating Centre (RIPE NCC), the African Network Information Centre (AfriNIC) and the Asia-Pacific Network Information Centre (APNIC).

[76] Assignees include international MNOs such as AT&T, Vodafone, Deutsche Telekom, Telecom Italia, Orange and Telenor as well as Jasper Technologies, a provider of IoT service platforms. For the use of international numbering resources, some initial investment has to be made (e.g. conclusion of new roaming agreements, testing). Still, in view of the support of international players it can be expected that ITU numbers will be reachable at a larger scale than before. However, it is noted that the costs associated to the request of ITU numbers, including the level of the membership fee, are regarded as a hurdle by some companies. A list over the current assignments of MNCs under the shared MCC 901 and CCs 882/883 can be found at http://www.itu.int/net/ITU-T/inrdb/e212_901.aspx and http://www.itu.int/net/itu-t/inrdb/e164_intlsharedcc.aspx?cc=881,882,883

REFERENCES

APEC (2005), "APEC Privacy Framework", Published APEC http://publications.apec.org/publication-detail.php?pub_id=390.

Abrams, M. and Weiss, J. (2008), "Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services", *Australia*, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

Article 29 Data Protection Working Party (2014), "Opinion 8/2014 on the on Recent Developments on the Internet of Things", Article 29 Data Protection Working Party, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (accessed on 1 June 2016)

Barbaux, A (2015), "Encore 450 millions d'euros pour financer des projets numériques", *L'usine Digitale*, 19 February 2015, www.usine-digitale.fr/article/encore-450-millions-d-euros-pour-financer-des-projets-numeriques.N314624 (accessed on 1 June 2016)

Bourne, J (2015), "Luxembourg becomes latest country to roll out SIGFOX nationwide IoT network" *TelecomsTech*, 28 July 2015, www.telecomstechnews.com/news/2015/jul/28/luxembourg-becomes-latest-country-roll-out-sigfox-nationwide-iot-network/ (accessed on 1 June 2016)

Burns, C (2011) "AT&T infographic notes massive Wi-Fi use growth on mobile devices", *SlashGear*, 22 July 2011, www.slashgear.com/attinfographic-notes-massive-wi-fi-use-growth-on-mobile-devices-22167040/ (accessed on 1 June 2016)

BDI and PwC (2015), "Die Digitalisierung im Mittelstand", presentation at BDI/PwC Mittelstandspanel, 1 August 2015, Federation of German Industry and Pricewaters House Coopers, www.bdi.eu/download_content/MittelstandUndFamilienunternehmen/Mittelstandspanel_1-2015.pdf (accessed on 1 June 2016)

BEREC (2015), "Draft Report on Enabling the Internet of Things", Body of Regulators for Electronic Communications, pp23-24 http://berec.europa.eu/eng/news_consultations/ongoing_public_consultations/3318-public-consultation-on-draft-berec-report-on-enabling-internet-of-things (accessed on 1 June 2016)

BIPT (2015), "Synthesis and detailed analysis of the answers received to the public consultation concerning the revision of the numbering policies", Institut Belge des Services Postaux et des Telecommunications

BMWi and BMJV (2012), "BMWi/BMJV-Maßnahmenprogramm„Mehr Sicherheit, Souveränität und Selbstbestimmung in der digitalen Wirtschaft", Federal Ministry of Economy and Energy and Federal Ministry of Justice and Consumer Protection, Germany, www.bmwi.de/BMWi/Redaktion/PDF/M-O/massnahmenprogramm-mehr-sicherheit-souveraenitaet-und-selbstbestimmung-in-der-digitalen-wirtschaft,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (accessed on 1 June 2016)

CBS (2015), Baby monitor hacker delivers creepy message to child, *CBS News*, April 2015. www.cbsnews.com/news/baby-monitor-hacker-delivers-creepy-message-to-child/

COE (1981), "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", Council of Europe Convention 108.

Cisco (2015a), "Cisco Visual Networking Index Outlook 2014-2019", Cisco, May 2015, www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html

Cisco (2015b), "The IoT threat environment", Cisco, www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/C11-735871.pdf

Cisco (2015c), "The Zettabyte Era—Trends and Analysis", Cisco, 23 June 2015, www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html (accessed on 1 June 2016)

Cloud Security Alliance (2015), "Security Guidance for Early Adopters of the Internet of Things (IoT)", *Cloud Security Alliance*, 2015, https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Council of Europe (2010), "Recommendation on the protection of individuals with regard to the automatic processing of personal data in the context of profiling", CM/REC(2010)13, 23 November

Council of the European Union (2015), "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach", Council of the European Union,

EC (2015), "Have your say on standards to help achieve a Digital Single Market" European Commission, https://ec.europa.eu/digital-single-market/news/have-your-say-standards-help-achieve-digital-single-market (accessed on 1 June 2016)

ECC (2014), "Evolution in the Use of E.212 Mobile Network Codes", Electronic Communications Committee, European Conference of Postal and Telecommunications Administrations, www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP212.PDF (accessed on 1 June 2016)

ECC (2013), "Extra-Territorial Use of E.164 Numbers", Electronic Communications Committee, European Conference of Postal and Telecommunications Administrations

ECC (2010), "Numbering and Addressing in Machine-to-Machine (M2M) Communications", Electronic Communications Committee, European Conference of Postal and Telecommunications Administrations, www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP153.PDF (accessed on 1 June 2016)

Economist (2011), "Difference Engine: Luddite legacy", *The Economist*, 4 Nov 2011, www.economist.com/blogs/babbage/2011/11/artificial-intelligence (accessed on 1 June 2016)

Enexis (2015), "Enexis kiest voor LTE 4G voor datacommunicatie slimme meter", press release, Enexis, www.enexis.nl/over-enexis/nieuws/enexis-kiest-voor-lte-4g-voor-datacommunicatie-slimme-meter (accessed on 1 June 2016)

European Parliament and European Council (2007), "Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), European Parliament and European Council

European Parliament and European Council (2003), "Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information", European Parliament and European Council

White House (2014), "Big Data: Seizing Opportunities, Preserving Values", White House, May 2014, www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

FCC (2014), "Notice of inquiry", Federal Communications Commission, 17 October 2014, FCC 14-154 http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db1017/FCC-14-154A1.pdf (accessed on 1 June 2016)

French Government (n.d.), "Section 1 : Ouverture des données publiques », Projet de loi pour une République Numérique, French government, https://www.republique-numerique.fr/pages/projet-de-loi-pour-une-republique-numerique (accessed on 1 June 2016)

FDA (2016), "FDA outlines cybersecurity Recommendations for medical device manufacturers". *Food and Drug Administration*, January 2016, www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm

Government Office for Science (2015) ""The Internet of Things: making the most of the Second Digital Revolution - A report by the UK Government Chief Scientific Adviser",, Government Office for Science, United Kingdom,, May 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf (accessed on 1 June 2015)

Greenberg, A. (2015), "Hackers Remotely Kill a Jeep on the Highway—With Me in It", Wired, July 2015, www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greenberg, A. (2015b), "After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix", Wired, July 2015, www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

GSMA (n.d.), "Connected Living", GSM Association, www.gsma.com/connectedliving/connected-living-mobilising-the-internet-of-things/ (accessed on 1 June 2016)

HP Enterprise (2015), "Internet of things research study. 2015 Report", 2015, www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

IDC and TXT (2015) "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination" study prepared for the European Commission, IDC Italia S.r.L and TXT e-solutions S.P.A., http://ec.europa.eu/digital-agenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination.

Evans and Annunciata (2012), "Industrial Internet: Pushing the Boundaries of Minds and Machines", November 2012. www.ge.com/docs/chapters/Industrial_Internet.pdf

Gartner (2014), "Gartner identifies the top 10 strategic technology trends for Smart Government", April 2014, http://www.gartner.com/newsroom/id/2707617

Goodwin, B. (2011), "Hacker Movie: Zombies Ahead", *ComputerWeekly*, March 2011, http://www.computerweekly.com/blogs/it-downtime-blog/2011/03/movie-zombies-versus-hackers.html

GSMA (2014), "Understanding the Internet of Things (IoT)", *GSM Association*, July 2014, http://www.gsma.com/connectedliving/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf

Harwell, Drew (2014), "Whirlpool's 'Internet of Things' problem: No one really wants a 'smart' washing machine", *The Washington Post*, Washington DC, 28 October. www.washingtonpost.com/news/the-switch/wp/2014/10/28/whirlpools-internet-of-things-problem-no-one-really-wants-a-smart-washing-machine/

ITF (2015), "Urban Mobility System Upgrade, How shared self-driving cars could change city traffic", International Transport Forum 2015. www.itf-oecd.org/automated-and-autonomous-driving

Navigant Research (2013), "The installed base of smart-meters will surpass 1 billion by 2022, November 2013, *Navigant Research*, http://www.navigantresearch.com/newsroom/the-installed-base-of-smart-meters-will-surpass-1-billion-by-2022

McKinley, J. (2014), "With Farm Robotics, the Cows decide when it's milking time", *New York Times,* April 2014, www.nytimes.com/2014/04/23/nyregion/with-farm-robotics-the-cows-decide-when-its-milking-time.html

Jorgenson, W.D. and Khuong M. Vu (2010), "Potential growth of the world economy", *Journal of Policy Modeling*, Vol. 32, nr. 5, 2010.

Leckie, A (2015), "LTE Category-0 & LTE-M low power M2M device roadmaps", blogpost, *IoTdevzone*, 18 May 2015, http://iotdevzone.com/blog/2015/05/18/lte-category-0-lte-m-low-power-m2m-device-roadmaps/ (accessed on 1 June 2016)

Merelli, E and M, Rasetti (2013), Non locality , topology, formal languages: New global tools to handle large data sets "International Conference on Computational Science, ICCS 2013 Procedia Computer Science 18 pp 90-99McMillan R. (2007), "Insider charged with hacking California canal system", ComputerWorld, Novermber 2007, www.computerworld.com/article/2540235/disaster-recovery/insider-charged-with-hacking-california-canal-system.html

Ministerie van Infrastructuur en Milleu (n.d.), "Open actuele water data Rijkswaterstaat", Ministry of Infrastructure and environment, Netherlands, http://www.rws.nl/rws/opendata / (accessed on 1 June 2016)

NIST (2014), "Release of NIST interagency report 7628 revision 1, guidelines for smart grid cybersecurity", National Institute of Standards and Technology, 2014, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=917244

Novet, J (2014), "Britain's David Cameron announces more funding for Internet of things research", *VentureBeat*, 10 March 2014, http://venturebeat.com/2014/03/10/britains-david-cameron-announces-more-funding-for-internet-of-things-research/ (accessed on 1 June 2016)

Morgan Stanley (2015), "Autonomous Cars: The Future Is Now", *Morgan Stanley* website, January 2015, http://www.morganstanley.com/articles/autonomous-cars-the-future-is-now/

Murray, S. (2015), "How the internet of things can speed up health delivery", *Financial Times*, April 2015, www.ft.com/intl/cms/s/0/8ad4d226-bdcc-11e4-8cf3-00144feab7de.html#axzz3XDyfx4Kw

OECD (Forthcoming a), "ICTs and Jobs: Complements or Substitutes? The effects of ICT investment on labour demand in 19 OECD Countries."

OECD (Forthcoming b), "New skills for the Digital Economy: Measuring the demand for ICT skills at work."

OECD (Forthcoming c), "ICTs, Jobs and Skills: New evidence from the OECD PIAAC Survey".

OECD (Forthcoming d), "Enabling the Next Production Revolution". Ministerial Council Meeting background paper.

OECD (2015a), "Chapter 6 Emerging Issues: The Internet of Things", OECD Digital Economy Outlook 2015", OECD Publishing, DOI: http://dx.doi.org/ 10.1787/9789264232440-en

OECD (2015b), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

OECD (2014a), "Data-Driven Innovation: Big Data for Growth and Well-Being", OECD Publishing, Paris. DOI: http://dx.doi.org/ 10.1787/9789264229358-en

OECD (2014b), "Technology Foresight Forum 2014 - The Internet of Things", December 2014. Agenda and presentations, http://www.oecd.org/internet/ieconomy/technology-foresight-forum-2014.htm

OECD (2013), "Building Blocks for Smart Networks", *OECD Digital Economy Papers*, No. 215, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5k4dkhvnzv35-en.

OECD (2012a), "Machine-to-Machine Communications: Connecting Billions of Devices", *OECD Digital Economy Papers*, No. 192, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5k9gsh2gp043-en

OECD (2012b), "Better Skills, Better Jobs, Better Lives: A Strategic Approach to Skills Policies", OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264177338-en.

OECD (2011), Health Reform: Meeting the Challenge of Ageing and Multiple Morbidities, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264122314-en

OECD (2010), "Smart Sensor Networks for Green Growth", in OECD, OECD Information Technology Outlook 2010, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/it_outlook-2010-8-en

OECD (2008a), "Radio-frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations", in *OECD Digital Economy Papers*, DOI http://dx.doi.org/ 10.1787/231551650432

OECD (2008b), "Recommendation Of The Council For Enhanced Access And More Effective Use Of Public Sector Information" [C(2008)36]

OECD (2007), "Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", [C(2007)67/FINAL].

Ofcom (2015), "Promoting investment and innovation in the Internet of Things, Summary of responses and next steps", Office of Communications, 27 January 2015

Ofcom (2014a), "M2M in the 700MHz band", ECC PT1(14)106, for CEPT meeting in Zagreb, 01-05 September 2014, Office of Communications, United Kingdom, 27 August 2014

Ofcom (2014b), "Promoting investment and innovation in the Internet of Things", Office of Communications, July 2014, http://stakeholders.ofcom.org.uk/binaries/consultations/iot/statement/IoTStatement.pdf

O'Neill, O (2012), A Point of View: Which comes first - trust or trustwhorthiness?, *BBC Magazine*, http://www.bbc.com/news/magazine-20627410 (accessed on 1 June 2016)

Office of Privacy Commissioner of Canada (2016), "The Internet of Things: an introduction to privacy issues with a focus on the retail and home environments", February 2016, www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp

Perlroth N. (2012), Cameras May Open Up the Board Room to Hackers, *New York Times*, www.nytimes.com/2012/01/23/technology/flaws-in-videoconferencing-systems-put-boardrooms-at-risk.html

Pepper, R. (2015), "The Rise of M2M Devices", Cisco, October 2015, http://berec.europa.eu/eng/document_registe/subject_matter/berec/download/0/5471-the-rise-of-m2m-devicespresentation_0.pdf

PricewaterhouseCoopers (2014), "Strategy Connected Car", September 2014, www.pwc.fr/connected-car-strategyand.html

Press, G. (2014), "A very short history of the Internet Of Things", *Forbes*, 18 June 2014, http://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/

Potoczny-Jones, I. (2015), "IoT Security & Privacy: Reducing Vulnerabilities", Network Computing, February 2015, www.networkcomputing.com/internet-things/iot-security-privacy-reducing-vulnerabilities/807681850

Poulsen, K. (2003), "Slammer worm crashed Ohio nuke plant network", Security Focus, October 2003, www.securityfocus.com/news/6767

Rethink Robotics (2014). "Rethink Robotics' Baxter Research Robot Now Available in Australia and New Zealand", 14 January 2014. www.rethinkrobotics.com/news-item/rethink-robotics-baxter-research-robot-now-available-in-australia-and-new-zealand/

Rundle, M (2015), "Tesla 'autosteer' update will make electric cars self-driving", *Wired*, 31 July 2015, http://www.wired.co.uk/article/tesla-self-driving-cars-update (accessed on 1 June 2016)

Rushe, D. (2011), "Cyber-attack claims at US water facility, FBI and Homeland Security to investigate shutdown of a water pump suspected to be work of foreign hackers", *The Guardian*, Nov 2011, http://www.theguardian.com/world/2011/nov/20/cyber-attack-us-water-utility

Thanki, R. (2012), "The Economic Significance of Licence-Exempt Spectrum to the Future of the Internet", http://download.microsoft.com/download/A/6/1/A61A8BE8-FD55-480B-A06F-

F8AC65479C58/Economic%20Impact%20of%20License%20Exempt%20Spectrum%20-%20Richard%20Thanki.pdf

SANS (2008), "SANS News bites, Volume X - Issue #4", January 2008, http://www.sans.org/newsletters/newsbites/x/4

SANS ICS (2014), "German Steel Mill Cyber Attack", December 2014, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Sorokanick, B. (2015), Ford Partners With Microsoft for Over-The-Air Sync Infotainment Updates, Car and Driver, March 2015, http://blog.caranddriver.com/ford-partners-with-microsoft-for-over-the-air-sync-infotainment-updates/

Storm, D. (2015), "MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks", *ComputerWorld*, June 2015, www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

Thielmam, S (2015), "Nevada clears self-driving 18-wheeler for testing on public roads", *The Guardian*, May 6 2015, http://www.theguardian.com/technology/2015/may/06/nevada-self-driving-trucks-public-roads-daimler-inspiration (accessed on 1 June 2016)

T-Systems (2015), "Automotive IT-Kongress 4.0", *T-Systems website*, www.t-systems.de/news-media/automotiveit-kongress-industrie-4-0-veraendert-automobilindustrie/1339486

Tudor, Z. and Fabro, M. (2010), "What Went Wrong? A Study of Actual Industrial Cyber Security Incidents", 2010.

van Lisdonk, J. R. (2014), "Wagenpark op nieuw spoor", *Defensie Magazine*, February 2014, http://magazines.defensie.nl/pijler/2014/02/pnod

Viola, R (2015), "Machine to machine connectivity in a Digital Single Market", https://ec.europa.eu/digital-single-market/blog/machine-machine-connectivity-digital-single-market, accessed on 1 June 2016

Vodafone (2015), "The 2015 Vodafone M2M Barometer report", http://m2m-mktg.vodafone.com/barometer2015

Volvo Cars (2015), "Scandinavian cloud-based project for sharing road-condition information becomes a reality", press release Volvo Cars, 12 February 2015, https://www.media.volvocars.com/global/en-gb/media/pressreleases/157065/volvo-cars-puts-1000-test-cars-to-use-scandinavian-cloud-based-project-for-sharing-road-condition-in

Wilson, J. (2008), "Sensor Technology Handbook", *Newnes/Elsevier*, Oxford.

Weiser, M. (1991), "The Computer for the 21st Century", *Scientific American*, 265(9): 66–75.

Yared, P. (2013), "The Internet of things, delivered via smartphone", *Venture Beat*, January 2, 2013, http://venturebeat.com/2013/01/02/internet-of-things-via-smartphone/