Council of the
European Union

Brussels, 20 April 2016
(OR. en)

8100/16
ADD 1

IND 75
RECH 103
TELECOM 52
MI 248
COMPET 172
EDUC 108
EMPL 116

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	19 April 2016
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2016) 110 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Advancing the Internet of Things in Europe Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Digitising European Industry Reaping the full benefits of a Digital Single Market

Delegations will find attached document SWD(2016) 110 final.

Encl.: SWD(2016) 110 final

EUROPEAN
COMMISSION

Brussels, 19.4.2016
SWD(2016) 110 final

COMMISSION STAFF WORKING DOCUMENT

Advancing the Internet of Things in Europe

Accompanying the document

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Digitising European Industry
Reaping the full benefits of a Digital Single Market

{COM(2016) 180 final}

STAFF WORKING DOCUMENT

Advancing the Internet of Things in Europe

Table of contents

1. Introduction

The Internet of Things (IoT) represents the next major economic and societal innovation wave enabled by the Internet. With the IoT, any physical (e.g. a thermostat or a bike helmet) and virtual (i.e. a representation of real object in a computer system) object can be connected to other objects and to the Internet, creating a fabric between things as well as between humans and things. The IoT can combine the physical and the virtual worlds into a new smart environment, which senses, analyses and adapts, and which can make our lives easier, safer, more efficient and more user-friendly. The Digital Single Market Strategy for Europe (in short DSM Strategy) underlines the need to avoid fragmentation and to foster interoperability for the IoT to reach its potential[1].

This Staff Working Document (SWD), which builds on a series of studies and consultations organised over the past 4 years[2], is part of the DSM technologies and public services modernisation package. It accompanies the Communication "Digitising European Industry – Reaping the full benefits of a Digital Single Market" (in short Digitisation Communication). The latter calls for actions in line with the DSM Strategy to maximise the benefits that digital innovation can bring to European economy, and to allow faster business growth in the digital economy. The DSM technologies and public services modernisation package also includes the Communication "Priorities for ICT Standardisation for the Digital Single Market" (in short Standardisation Communication). Several of the actions outlined in the Digitisation Communication and in the Standardisation Communication concern IoT directly. This SWD is also related to initiatives already announced in the DSM Strategy, notably the Telecoms Review and the Free Flow of Data initiative.

As pointed above, the Digitisation Communication and the Standardisation Communication highlight the importance of Europe becoming a leading region in IoT products and services. Stakeholders and available expertise point out that advancing work towards these objectives would require action along the following 3 pillars:

1. A single market for the IoT: IoT devices and services should be able to connect seamlessly and on a plug-and-play basis anywhere in the European Union (EU), and scale up across borders.
2. A thriving IoT ecosystem: open platforms used across vertical silos will help developer communities to innovate. As a kick-start, IoT deployments in selected lead markets will be supported.
3. A human-centred IoT: the IoT in Europe is to respect European values, empowering people along with machines and businesses, thanks to high standards for the protection of personal data and security, visible notably through a 'Trusted IoT' label.

---

[1] Communication *A Digital Single Market Strategy for Europe* COM (2015) 192 Final. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192.

[2] Notably: policy papers and books published by the IoT European Research Cluster (IERC) (http://www.internet-of-things-research.eu/); conclusions of the IoT EU Expert Group 2010-2012 and public consultation on the governance of the Internet of Things (IoT) launched in 2012 (https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation); consultation in 2015 on IoT Large Scale Pilots; three dedicated studies in 2013, 2014 and 2015 (available at: https://ec.europa.eu/digital-single-market/en/newsroom/reports-studies-etc/internet-things); results of the Future Internet Public Private Partnership (FI-PPP) under FP7; papers published by the Alliance for Internet of Things Innovation (AIOTI) in 2015 (available at: https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020).

These three pillars are analysed in the remaining of this *Staff Working Document*.

1.1. What is the Internet of Things?

Originally, the Internet was conceived to interconnect computers and transmit messages with limited data exchange capability. With the advent of web technologies, a first revolution took place enabling the linking of documents and the creation of a word wide web of information (web 1.0). In the early years of this century, the Internet evolved towards a universal communication technology making it possible to carry all voice, video, or information content, with social media enabling user-generated content (web 2.0). Based on existing communication technologies like the Internet, the IoT[3] represents the next step towards digitisation where all objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and/or about the status of the surrounding environment. Think for example of a fire extinguisher, which will directly call the fire department when in use and send information about the incident.

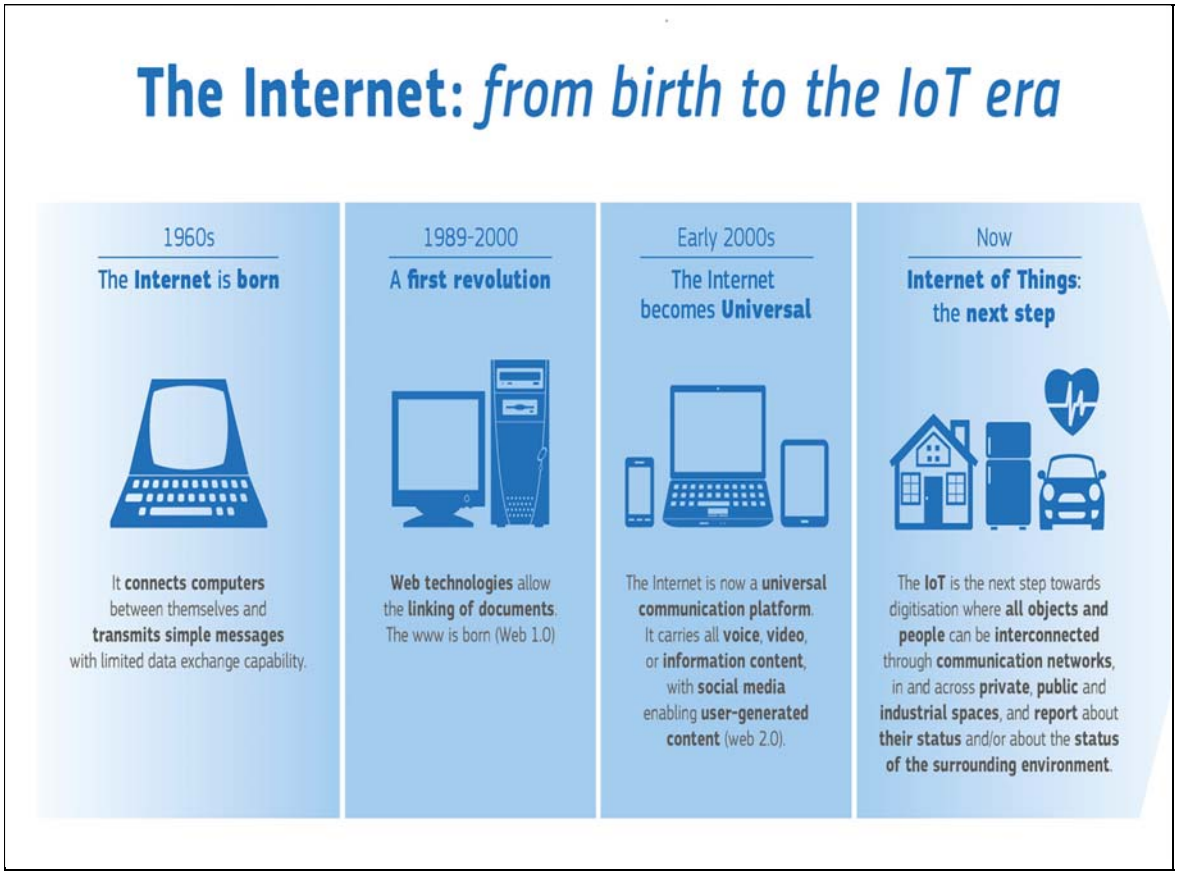

Figure1. The Internet: From birth to the IoT era

[3] The first use of the term Internet of Things is often attributed to Kevin Ashton (Massachusetts Institute of Technology's Auto-ID (for Automatic Identification) Center in Boston), at that time employee of Procter& Gamble. In 2009, he mentioned the need for an Internet for Things as a standardized way for computers to capture information from the real world and to understand it.

The IoT inaugurates a **new age of ubiquitous connectivity and intelligence** in which components, products, services and platforms connect, virtualise and integrate everything in a communication network for digital processing[4].

The IoT is about setting up new ecosystems that cut across vertical areas, and create new markets for hardware (connected devices), software (IoT platforms and systems) and services (IoT applications). IoT has a horizontal and cross-cutting character. It should be understood as an ecosystem where areas that have been developed as vertical silos (manufacturing, transport, healthcare, devices etc.) relate to each other, thanks to common platforms and innovation across areas. IoT ecosystems are, therefore, based on bringing together multiple sectors and stakeholders to cover an increasingly complex value chain.[5] It also requires open platforms that can integrate many different types of equipment and applications. The IoT combines connectivity, data generation, architecture and system, processing and analytics with actuation[6] and new interfaces, including automation and artificial intelligence.

The IoT is based on various disciplines and technologies like sensors, embedded systems, various communications technologies (semantic and security technologies for naming some). It requires a specific configuration for object identification and search, open/closed data sharing, lightweight communication protocols, trade-off between local and networked based information processing, and backend integration. It also requires specific considerations of data security (e.g. location-based profiling), liability (many service providers involved) seamless identification and authentication mechanisms (including those of persons/entities needed for managing contractual relations, attribution and liability) and trust.

Given these specificities and based on the current market developments, one may argue that IoT encompasses different steps of evolution that can develop in parallel.

---

[4] The IERC/ITU official definition states that IoT is "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.". Available at: http://www.internet-of-things-research.eu/about_iot.htm.

[5] See for instance the speech of Samsung Electronics CEO BK Yoon: '*The Internet of Things needs openness and industry collaboration to succeed'*, available at: http://www.samsung.com/us/news/24395.

[6] An *actuator* is a mechanical device for moving or controlling a mechanism or *system*. It takes energy, usually transported by air, electric current, or liquid, and converts that into some kind of motion (definition given by IoT-A project).

Different steps of evolution of the Internet of Things

1. Data driven innovation in vertical sectors

Connected sensors collect data from objects (e.g. a car, a phone etc.) These data are analysed either through embedded systems or through cloud-based and Internet systems enabling the creation of new services and big data analytics. Wearables, sensors, equipment parts in business and smart city environments are examples of solutions put forward in this step. Innovation is data- and product-driven and provides better decision making, increased efficiency and more convenience. This happens at the level of vertical sectors, but cross-cutting exchanges remain limited.

2. Industrial IoT: actuation and semi-autonomous behaviour based on smart connected objects

The data provided by connected sensors and objects allows single and networked objects to perform specific functions derived from sensing, analysis and intelligence gathered. This operates normally within the boundaries of given applications but it is expected, with increasing computing power and sophistication to gain high levels of autonomy in their behaviour and "life". Examples include factory automation, logistics and robotics.

3. Programmable world: data exchange and service creation across large vertical applications

The third step combines steps one and two by using complex systems, intelligence and actuation. Sensors and Smart connected objects are not only designed and optimised to perform certain functions on the basis of vertical business models. They become part of a bigger connectivity network which creates new opportunities to combine more intelligence and actuation across vertical markets (verticals), to provide a whole new set of services and to coordinate smart objects in their original or other functions. Technical and semantic interoperability are the key factor of success. It enables the programming of complex systems to integrate a number of device- and service providers to deliver complete IoT solutions e.g. at home, in cities, between industries.

4. The age of the digital nature

Connected objects of all sorts become autonomous, using artificial intelligence to learn and self-improve. Natural and cyborg interfaces link people with their hyper-connected environments and optimise these objects' functionalities seamlessly, like in a new stage of nature. This stage implies objects making decisions on their own to simplify our everyday life. The basic design is intended to meet the needs and preferences of individuals and society.

1.2. Expected benefits from the Internet of Things

Less than 1% of objects are currently connected to the Internet. The number of IoT connections within the EU is estimated to increase from approximately 1.8 million in 2013 to almost 6 billion in 2020, leading to the EU IoT market being higher than one trillion euros by 2020[7]. This growth in connectivity is expected to bring vast economic benefits, whereby the IoT significantly reshapes industry structures, with borders between products and services, as well as borders between industrial sectors becoming less obvious than today. This may materialise through, for example new innovative IoT services or applications; improved products thanks to the addition of new services or applications coming from connectivity; increased efficiency in processes; reduced consumption of resources and energy; better understanding of customers' needs; increased flexibility and possibility for sharing and co-creation.

Economic benefits are also expected to derive from a series of solutions addressing societal challenges, as can be seen in the following examples:

- Barcelona's Energy-Saving Smart Streetlights[8]: sensors are installed in streetlights, enabling automatic control of brightness by analysing the levels of noise, air pollution, and population density. Result: at least 30% energy savings per year;
- UK's Intelligent Transport System that Reduces Traffic Congestion: UK built an responsive transport system on the M42 motorway and reduced travel time by 25% and traffic accidents by 50%[9];
- In the Netherlands, IoT based solutions supporting health monitoring and independent living at home for people with multiple chronic conditions have demonstrated efficiency gains of care efforts of more than 20%[10].

1.3. Europe's strength in digital technologies in a global context

In the opinion of Commission services, Europe's future digital industrial strengths will depend on the capacity of its industry to seize the opportunities coming from the wider diffusion of digital innovation across sectors. Given Europe's current strengths in vertical markets, the development of the IoT offers a unique opportunity for Europe, since it has the potential to lead to the establishment and reinforcement of the new digital value chains in Europe attracting investments and innovators. The digitisation of all industrial sectors will be important to keeping a strong European industrial base and to manage transforming value chains and business models. For example, digitisation and the use of the IoT are essential to the development of smart farming or the development of traceability and safety of food.

---

7 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, study for the European Commission. Full text here: http://www.telit2market.com/wp-content/uploads/2015/02/TEL_14016_P_112-114.pdf ; 26 billion "things" may be connected globally by 2020

8 More details at: http://smartcity.bcn.cat/en/growsmarter.html

9 http://www.roadtraffic-technology.com/projects/m42/

10 http://www.greenpeak.com/Company/PressReleases/PR201503ContractZTEHealth.html

Although the digital transformation of industry is creating tremendous opportunities for Europe, available expertise points out that a series of leading industries are confronted with huge challenges[11].

In March 2015, the European Commission together with IoT industry players launched the Alliance for the Internet of Things (AIOTI)[12]. AIOTI aims to give EU the lead in the IoT field creating a dynamic European IoT ecosystem. AIOTI follows an approach to European platforms that entails cross-sectorial partnerships and collaboration, and promotes a European strategy for IoT in response to international initiatives such as Industrial Internet Consortium (IIC). The Alliance also offers an opportunity to discuss regulatory and legal obstacles to further IoT take up, and to forge consensus on standardisation matters through the European Telecommunications Standards Institute (ETSI)[13] and oneM2M[14].

Given the very high potential of the Internet of Things, it is not surprising that a number of regions and countries (notably USA, China and Japan) are trying to become global leaders in IoT.

1.4. Challenges for the implementation of the Internet of Things

Major challenges to the wide deployment and exploitation of the IoT potential are:

(a) In many industrial sectors, digital transformations are leading to radical changes in companies' roles and beneficiaries throughout the value chain and to the creation of new markets. Monopolising or ring-fencing of new IoT areas may be an obstacle to the development of these markets, and to the development of open digital platforms.

(b) At the moment, many companies are still cautious when it comes to the IoT and Industry 4.0 implementation as it may involve radical structural changes and radical shift in value creation. This could explain why established large players often find it difficult to adapt to new business models and engage in new types of alliances. In that respect, agile players like SMEs, especially entrepreneurs and start-ups, are considered to have the potential to seize new opportunities brought up by the IoT.

---

[11] See, e.g. Manyika et al. (2015) *Unlocking the potential of the Internet of Things*; McKinsey Global Institute - June 2015; available at: http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world;
Manyika et al. (2015) Internet of Things: Opportunities and challenges for semiconductor companies; McKinsey; available at: http://www.mckinsey.com/industries/semiconductors/our-insights/internet-of-things-opportunities-and-challenges-for-semiconductor-companies.

[12] For more details on AIOTI, please check the link: https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti.

[13] www.etsi.org

[14] http://www.onem2m.org/.

(c) There is a lack of common standards and interoperable solutions throughout the products and services life cycles[15]. Interoperability will be essential for the deployment of the IoT and for ensuring seamless flow of data across sectors and value chains.[16]

(d) There is a lack of consensus on EU policy coordination in this area[17]. According to stakeholders this lack of consensus creates at least five major risks:

1) Risks of fragmentation and a need to address a coordination failure between Member States. Member States are starting to develop national policies in favour of IoT. National barriers could prevent the IoT from operating on a genuine Single Market basis, which is recognised by the DSM Strategy[18].

2) Risks of fragmentation between industries. At industrial level, a number of areas[19] are already adopting the IoT by adding connectivity to products and processes. However, as in many cases each industrial actor acts unilaterally, adopting separate architectures, standards and business models, this reality does not encourage cross-cutting approaches, risks reinforcing silos, and prevents innovation across areas.

3) Risk of lock-in in proprietary ecosystems, through restraint interoperability and access to data and applications.

4) Risk of users being forced to compliance and data sharing instead of developing a human-centred IoT where users can trust that the IoT systems around them operate according to understood principles and guarantees for their integrity, privacy and security.

---

[15] See Guillemin, P. (2014), Chapter 4 Internet of Things Global Standardisation, in Friess & Vermesan (editors) *Internet of Things, from Reserch and Innovation to market deployment*, downloadable at: http://www.internet-of-things-research.eu/pdf/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdf

[16] AIOTI's report on IoT standards available at: https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020; reports from the workshop on IoT standards and architectures organised on 4/11/2015, available at: https://ec.europa.eu/digital-single-market/en/news/standards-and-architecture-iot-path-convergence-main-outputs-workshop-iot-standardisation-and.

[17] See e.g. results of the public consultation held between April and July 2012 available at; https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation; and the study on Europe's policy options for a dynamic and trustworthy development of the Internet of things (2013) available at: http://bookshop.europa.eu/en/europe-s-policy-options-for-a-dynamic-and-trustworthy-development-of-the-internet-of-things-pbKK0113297/.

[18] SWD *A Digital Single Market for Europe*, op. cit. p.7. "The scale provided by a DSM is also important for the deployment of high-speed infrastructure to enable advanced digital services and the development and adoption of new technologies in Europe, such as the Internet of Things, big data analytics or cloud computing. Companies may refrain from investing in the deployment of these technologies if they have to use different costly specifications or have to invest in new infrastructure (e.g. cloud based data centres), as regards the transfer of data or cross-border service delivery, making it unprofitable to innovate".

[19] Areas of application we see today for IoT include but are not limited to: multi-modal mobility and smart road infrastructure, smart agriculture and food traceability, smart assisted living and wellbeing, smart manufacturing, energy management at home and in buildings, worker safety, environmental monitoring and management, load-aware power generation and demand response, smart living environment, smart public safety, smart design, open platforms for the audio-visual industry.

5) Risk that the uncertainty about business models and standards could generate information asymmetries and market failures, preventing investment and risk-taking.

The challenges mentioned above lead to the general discussion on the need to ensure a proper balancing of different actions in view of their compliance with the rights enshrined in the European Charter of Fundamental Rights[20].

[20] Any policy initiative in relation to IoT needs to ensure the respect of the rights enshrined in the Charter of Fundamental Rights, like for example the right to private lift (Article 7), and the protection of personal data (Article 8), or the freedom to conduct a business (Article 16).

2. A single market for the Internet of Things

Stakeholders point out that for achieving a large uptake of the IoT in Europe a functioning single market for the IoT is key. It would ensure that IoT devices and services are able to connect seamlessly and on a plug-and-play basis anywhere in the EU and scale up without obstacles through national borders. Besides connectivity, and as outlined in the Digitisation Communication, a DSM for IoT would also need to address issues relevant to numbering and addressing, telecom networks, data flows and liabilities.

Mastering of all the key elements of the technology and value chain and their integration into horizontal platforms also requires a focused standardisation effort on the delivery of reference architectures, as recognised in the Standardisation Communication.

2.1. Setting the scene: key features of the IoT in a single market

The IoT starts from a connected device, while at the same time IoT is based on an architecture that recognises devices and organises their interactions.

Machine to Machine (M2M) connectivity

In terms of connectivity, there are a number of available standards, commonly referred to as Machine to Machine (M2M). The IoT is built on an underlying multi-protocol communications framework that can easily move data between embedded "things" and systems located at higher levels of IoT architecture[21]. M2M is the most basic requirement for the IoT single market.

Devices can be connected simply through a fixed telecommunications line using protocols like Ethernet. They may also be connected through wireless protocols and there is a plethora of short-range or local area, wireless technologies available including RFID, NFC, Wi-Fi, Bluetooth, XBee, ZigBee, Z-Wave and Wireless M-Bus. There are also low-power longer range options, like LoRa, Sigfox and a forthcoming narrow-band LTE standard (LTE-NB). GSM and 3G can also be used to connect devices. In the future, 5G promises to even better serve IoT devices to offer scalability for M2M, low latency, better quality of service and improved spectrum efficiency.

At present no evidence exists of any market failure in this area, as there is currently sufficient choice in the market and strong consistency between the choice of M2M connectivity protocols and the function of connected devices. The telecom industry has created a global standards initiative for M2M communications, oneM2M, to avoid that

[21] More details at:https://www.linkedin.com/pulse/connectivity-options-internet-things-iot-brijesh-kumar

connectivity protocols constitute barriers to the development of IoT systems through parallel standardisation initiatives. The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

IoT architecture

Reference architectures provide a common language allowing several actors to build infrastructural and functional IoT platforms, and on top of these value-added applications and services. They allow cooperation of industry across the value chain, across industrial sectors and across functional layers. In particular, a number of stakeholders point out that reference architectures for IoT platforms, on which applications and services can be built based on open interfaces and allowing cooperation of industry across the value chain, could be useful[22]. This would also help to mobilise an increasingly dynamic and growing community of innovators and entrepreneurs in the domain.

AIOTI has already developed a reference architecture to explain how different IoT systems operate and how its various components are linked. The functional model of the AIOTI reference architecture is composed of three layers:

- **The Application layer**: contains the communications and interface methods used in process-to-process communications.
- **The IoT layer**: groups IoT specific functions, such as data storage and sharing, and exposes those to the application layer via interfaces commonly referred to as Application Programming Interfaces (APIs). The IoT Layer makes use of the Network layer's services.
- **The Network layer**: the services of the Network layer can be grouped into data plane services (providing short- and long-range connectivity and data forwarding between entities), and control plane services (such as location, device triggering, Quality of Service or determinism).

This model highlights that, if not consistently used, there may be obstacles for IoT systems to properly operate across Member States borders or across technological domains.

Data handling

The IoT generates large amounts of data, and conversely IoT systems rely on a proper handling of data, collecting and combining data from different sectors and/or different sources[23]. There are already several business models encompassing these layers of a data component in the IoT solutions available on the market[24] as described in the subsequent box.

---

[22] See for instance the workshop of 4 November 2015 on "IoT Standardisation and Architectures" (op.cit.)

[23] For instance, combining data coming from a smart meter with data coming from a washing machine to minimise energy costs; combining data from the sensors in a street with data collected from the rest of the city or other cities and from different sectors: meteorological data, data about traffic, about the activity in the factories and so on to respond to various city challenges.

[24] E.g. https://hbr.org/2014/07/how-the-internet-of-things-changes-business-models.

IoT business models and their specificities in relation to data handling

a) In most IoT solutions, e.g. a daily home device (thermostat) is transformed into a smart object with the help of an embedded sensor. In such a case, the data (1) generated by the sensor is directly (2) transmitted by using a traditional wired Ethernet of Wi-Fi connection to an (3) Internet cloud service (e.g. an application service provider) where it is (4) processed to analyse our home energy consumption. How can the user make use of the (5) data service element obtained (the analysis of their home energy consumption)? In this case, the cloud connection enables the user to obtain remote access to their thermostat via a smartphone or a Web interface[25].

The problem with such a model relates to interoperability challenges when attempting to integrate devices made by different manufacturers. Under current market developments, the device and cloud service are from the same vendor. If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers[26]*. This is commonly referred to as "vendor lock-in''. Often, in this model the data each IoT sensor produces remains a data silo, as the model does not allow for aggregation of other data sources.*

b) Another possible model would be one that allows access to the sensor data to third parties. The approach is an extension of the above described model, to also include access to third parties. All data sensors coming from a particular infrastructure (local/distributed one: e.g. a building/a city) would be stored in a cloud infrastructure and further on processed and transformed into data services. For the moment, the take up by the market of this model where data are shared with other parties is limited. In most cases, the generation, collection and processing of data is ensured by the same actor.

c) Another model, also available on the market, is based on smart devices (carrying a sensor or actuator) that directly communicate with one another, and no longer through an intermediary application server. In doing so, they use certain communication protocols. This model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. The problem with such a model is the risk of lock-in.

To deliver a single market for the IoT, the Commission services consider that it is essential to facilitate the flow and transfer of data across a series of steps[27]:

---

[25] The cloud provider also supports software updates to the thermostat.

[26] Industry efforts to solve this issue, e.g. the AllSeen alliance, see https://allseenalliance.org/

[27] See also e.g. GSMA (2015) *Unlocking the value of IoT through Big Data*, http://www.gsma.com/connectedliving/wp-content/uploads/2015/12/cl_iot_bigdata_11_15-004.pdf; *Key Conclusions and Recommendations*, Meeting European Commission and European Round Table of Industrialists, Brussels, 20 July 2015.

1) generation of data
2) transfer of data
3) storage of data
4) processing of data
5) provision of data services

As indicated by a number of stakeholders, obstacles may emerge at each step, which could prevent the effective functioning of IoT systems and solutions on a pan-European basis. To allow for flexible and interoperable systems, at each step, data should be made available, accessible and easily aggregated, processed, as well as trusted, thus combining quality, reliability and security.

2.2. Connectivity obstacles: spectrum, network coverage

Some framework conditions could become an obstacle for the development of a single market for IoT, notably spectrum availability and network coverage.

Spectrum availability

Spectrum is one of the key enablers of the IoT. While the need for additional speed and capacity for wireless data traffic (Enhanced Mobile Broadband[28]) is booming, the number of connected devices is also estimated to increase very rapidly. As an example, there were 52 million machine-to-machine (M2M) connections across Europe as of September 2014, and their total number is forecast to grow at a compound annual growth rate (CAGR) of 23% between 2014 and 2020, bringing the total to 190 million[29]. As these connections are mostly wireless, to accommodate the resulting traffic between connected devices, the amount of available spectrum will have to be increased.

ETSI identifies around 20 different frequency bands[30] between 25 MHz and 1000 MHz for the usage by Short Range Devices (SRD). This results in a fragmentation of this resource. However, this is due to the fact that these bands are category-specific and cater for different usage conditions and uses; not all devices will have to support all these bands in parallel.

To avoid introducing any undesirable obstacles, the Commission services take full account of the particularities brought about by IoT when discussing the review of the spectrum policy with Member States.

---

28 ITU categorization of the future IMT: http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

29 GSMA Intelligence (2014): https://gsmaintelligence.com/

30 ETSI EN 300 220-1: http://www.etsi.org/deliver/etsi_en/300200_300299/30022001/02.04.01_40/en_30022001v020401o.pdf

Network coverage

Another key issue for the broad deployment of the IoT is the availability of communication networks as all devices should be able to plug and play wherever they are in the EU. Depending on the use case the connectivity needs may however be satisfied through different technologies: for example, small, low-powered sensors need a different type of connectivity as connected cars. To facilitate the wide availability of IoT solutions, it is important, in the opinion of the Commission services, that European broadband policies are designed with IoT specificities in mind.

2.3. Numbering, addressing, identification and discovery

A potential obstacle for the achievement of a single market for the IoT has to do with the capacity to handle a large number of different connected devices. There is a need to securely identify them and to be able to discover them so that they can be plugged into IoT systems.

Numbering and addressing

Billions of objects will be connected via the Internet to gather data and to remotely enable value-added services. These billions of objects will likely not have a predefined static location (e.g. being tracked all the way from cradle to usage and to recycling) or are meant to be able to move around throughout the EU and beyond (e.g. connected cars, fishing vessels, cruise ships etc.) while being connected seamlessly.

Following the work that the European Conference of Postal and Telecommunications Administrations (CEPT)[31] has done on the topic, the Commission services consulted with Member States through the Body of European Regulators of Electronic Communications (BEREC)[32] in 2015 to establish how they see the emerging needs for a European numbering range in view of the experience with ETNS[33]. More specifically, the Commission services wanted to examine how Member States plan to address the availability and the extra-territorial use of E.164 and E.212 numbers for M2M services in their national numbering ranges. The public consultation[34] on the EU Telecoms Review, which included questions on numbering, highlighted the need for further harmonisation to

31 www.cept.org

32 http://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/5091-request-from-the-commission-to-berec-for-input-and-opinion-on-the-review-of-the-rf-for-electronic-communications

33 ETNS was a shared Country Code (+3883) for Europe that was intended to be a complement to existing individual country codes.

34 https://ec.europa.eu/digital-single-market/en/news/high-quality-and-high-speed-internet-access-vital-achieve-digital-single-market

support the deployment of infrastructure in line with future market needs and that industry is supportive of a more co-ordinated approach. The current numbering scheme seems to be too limited to support the wide range of future M2M applications and the Commission services are of the opinion that it would need to be developed further. The Commission services continue to monitor work in technical fora (e.g. Internet Engineering Task Force (IETF)[35] and Réseaux IP Européens Network Coordination Centre (RIPE NCC)[36]) in view of ensuring that the technical feasibility of a European/international numbering scheme for IoT and that this option remains implementable for the case it would receive considerable backing in the future.

Identification and discovery

The availability of mechanisms for the identification of physical and virtual/logical objects is a key prerequisite for the development, deployment and operation of IoT applications and services. An IoT identification framework comes with naming, addressing and discovery mechanisms. These identifiers operate at different layers and serve different purposes.

As outlined in the IERC Position Paper on IoT Identification[37], a wide array of identification technologies are deployed by EU organizations for different types of applications. These include IPv6, tag identifiers (UPC, RFID), DOI/Handle, as well as several application identifiers. The Commission services acknowledged the importance of providing IPv6 infrastructures and have taken measures to encourage IPv6 deployment. However, IPv6 deployment remains very small comparing to IPv4. Furthermore, IPv6 is generally present in core networks, but has still very low penetration in the access part.

The Commission through Horizon 2020 IoT Focus Area[38] is funding research into IoT integration and platforms that will address notably authentication, identification and discovery.

2.4. Standardisation and Interoperability

[35] IETF's working group MODERN (Managing, Ordering, Distributing, Exposing, & Registering telephone Numbers) is tasked to define a set of Internet-based mechanisms for the purposes of managing the acquisition and resolution of telephone numbers in an IP environment. The Commission raised the issue of a possible European/international IoT numbering, to be studied by the group.

[36] www.ripe.net

[37] Available at: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_EU-China_IoT_Identification_Final.pdf

[38] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-iot-2016-2017.html#c,topics=callIdentifier/t/H2020-IOT-2016-2017/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc

Standardisation is the critical element to deliver a single market for IoT where any device can plug and play anywhere. It can facilitate the interoperability, compatibility, reliability, security and effective operations on a global scale among different technical solutions, softening (or even eliminating) such fragmentation, stimulating the emergence of new ecosystems, enabling R&D, boosting innovation and reinforcing competitiveness. IoT standards may support the emergence of business models unleashing the commercial capabilities of systems and device integration.

Existing standards and alliances

IoT standardisation encompasses standards for connectivity, interoperability, APIs, data ontologies, data sharing (e.g. cloud services), protection of personal data and security. As opposed to proprietary solutions, open standards are considered a solution in the IoT landscape, because of their net positive effects as regards large scale deployment, widespread adoption and preventing lock-in. Open standards are also key in creating innovative ecosystems cutting across silos. However, standards identification is not enough to ensure interoperability.[39] Reference implementations that can be shared by industrial actors are of utmost importance.[40]

In addition, a large number of proprietary or semi-closed solutions to address specific needs have emerged, leading to non-interoperable applications, based on different architectures and protocols. Consequently, the deployment of IoT applications (i.e. where information of connectable "things" can be flexibly aggregated and scaled) has been limited in scale and in scope, actually limiting the IoT to a set of "intranets of things – or goods".[41]

Several standardisation initiatives currently co-exist, in individual Standard Development Organisations (SDOs) or partnerships (e.g. ETSI SmartM2M[42], ITU-T[43], ISO[44], IEC[45], ISO/IEC JTC 1[46], oneM2M[47], W3C[48], IEEE[49], OASIS[50], IETF[51], etc.) and also in conjunction with a number of industrial initiatives (e.g. All Seen Alliance[52], Industrial

---

39 See e.g. http://www.etsi.org/images/files/SOSInteroperability/SOSinteropIpresentation16.pdf

40 This approach was notably followed in the context of the Future Internet PPP (FI-PPP)."

41 Rolling Plan for ICT Standardisation 2015 available at: https://ec.europa.eu/digital-agenda/en/news/rolling-plan-ict-standardisation-0

42 Smart Machine-to-Machine communications (Smart M2M), see: https://portal.etsi.org/tb.aspx?tbid=726&SubTB=726

43 ITU Telecommunication Standardization Sector (ITU-T), see: http://www.itu.int/en/ITU-T/Pages/default.aspx

44 International Organization for Standardization, see: www.iso.org

45 International Electrotechnical Commission, see: www.iec.ch

46 ISO/IEC Joint Technical Committee 1 Information technology, see: http://www.iso.org/iso/iso_technical_committee?commid=45020

47 www.onem2m.org

48 World Wide Web Consortium, see; www.iec.ch

49 Institute of Electrical and Electronics Engineers, see; www.ieee.org

50 Organization for the Advancement of Structured Information Standards, see: www.oasis-open.org

51 http://www.ietf.org/

52 http://allseenalliance.org/

Internet Consortium (IIC)[53], Open Interconnect Consortium (OIC), Platform Industrie 4.0[54] etc.). It is important to understand the global dynamics of IoT standardisation in order to leverage existing standardization activities and to ensure a thorough understanding of market needs and requirements, via a gap analysis.[55]

Large-Scale Pilots in Horizon 2020

Against the background of global competition and risks of fragmentation and delay, the Commission has created a dedicated Focus Area on IoT as part of its Work Programme 2016-17 under Horizon 2020. The Commission will invest more than 100 M€ in demand-driven large scale IoT pilots and lighthouse initiatives in areas such as smart cities and homes, smart living environments for ageing well, driverless cars, wearables, smart city, agro-food or manufacturing. Examples of Large-Scale Pilots (LSPs) are presented in the Annex to this SWD. LSPs will lead to technology integration and also to validation of business models and standards. LSPs on IoT will support innovative experimentation and testing activities with a focus on cross-border collaboration facilitating access of SMEs and mid-caps to technology and EU-wide markets.[56]

Most of the relevant work on IoT related to standardisation has been analysed by the Alliance for Internet of Things Innovation (AIOTI). The AIOTI has provided 3 key documents[57]:

- *IoT Landscape and IoT Large Scale Pilots Standard Framework Concepts*, presenting the global dynamics and landscapes;
- *IoT High Level Architecture (HLA)* that may be applicable to LSPs. The HLA takes into account existing SDOs and alliances on architecture specifications;
- *IoT Semantic interoperability recommendations for IoT LSPs*.

AIOTI identified a very significant number of IoT alliances, which have a specific positioning and sometimes overlap in their aim. This may characterise the still emerging nature of the IoT but it may also represent a risk of fragmenting the IoT landscape, as illustrated in figure below.

[53] www.iiconsortium.org/
[54] http://www.plattform-i40.de/I40/Navigation/DE/Home/home.html
[55] Rolling Plan for ICT Standardisation 2015 (op cit.)
[56] For more details see Horizon 2020 Work Program 2016-2017: http://ec.europa.eu/digital-agenda/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots
[57] Available at: https://ec.europa.eu/digital-single-market/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

Figure 2: IoT SDOs and Alliances landscape

It is therefore important to promote cooperation between the different SDOs and alliances to ensure appropriate leverage of resources and efficient IoT standardisation.

Mapping and fostering convergence

It is also essential to understand users' demands on standardisation and how coordination within the IoT standards landscape could take place. A gap analysis could help achieve such coordination. The Commission was instrumental in setting up (and participates in the steering and supports financially) ETSI's Specialist Task Force 505 (ETSI STF 505[58]) to perform an IoT Standards landscaping and gap analysis, and to develop supporting references for the LSPs that will be funded by the Commission under the Horizon2020 IoT Focus Area[59]. ETSI STF 505 is tasked to analyse the status of current IoT standardisation; to assess the degree of industry and vertical market fragmentation; and to point towards actions that can increase the effectiveness of IoT standardisation, improve interoperability, and allow for the building of IoT ecosystems.

Testing and interoperability

The complexity and interdependence of IoT standards is illustrated by the interoperability tests (called "plugtests") that are performed by ETSI (with EC funding) for key IETF standards for IoT, such as 6lo (IPv6 over Networks of Resource-constrained Nodes) and

[58] https://portal.etsi.org/stfs/ToR/ToR505v02_SmartM2M_EC_2015-02_IoT_Analysis.doc

[59] https://ec.europa.eu/digital-agenda/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots

6TiSCH (IPv6 over Timeslotted Channel Hopping, Time-slotted Channel Hopping having in turn been developed by the IEEE).

LSPs have been proposed through Horizon 2020 to test standards through wide scale operational testing of IoT solutions. These LSPs should support the deployment of IoT solutions, by enhancing their acceptability and adoption by users and citizens and by fostering new market opportunities for EU suppliers. Implementing real-life IoT LSPs is essential to test standards at work in real-life conditions and to support the appropriate reference implementations.[60]

An open standards environment is important for the IoT. To achieve interoperability, voluntary implementation of IoT Reference Architectures and interfaces and of open APIs is necessary towards a true IoT Digital Single Market.

In parallel, the Commission services continues the monitoring of the Internet standardisation process and maintains contacts at the highest level with key European and international SDOs, notably through the Multi Stakeholder Platform, and high-level events.[61] The Commission services also hold a process of international dialogue and consensus-building on IoT standardisation with the US, South Korea, Japan and China, notably through the Horizon 2020 joint international calls and the bilateral ICT Dialogues.

Intellectual Property Rights Licensing

Using multiple technologies and standards inherent to the deployment of complex IoT systems may naturally involve patented or protected technologies. It can be anticipated that service or higher layer technologies may be deployed under "free" licensing schemes (e.g. APIs to stimulate creation of large communities of developers). At the same time, a number of stakeholders have underlined that other technologies, having necessitated huge investment in research and standardisation development, may be licensed under fair, reasonable, and non-discriminatory (FRAND) terms; the latter ensure fair access to the standard for the implementers and fair return for the standard essential patents holders. However, certain stakeholders point out that with the multitude of technologies involved in implementing a complete IoT value chain, there are possible risks of uncertainty in particular in relation to i) who is the relevant community of essential patent holders, ii) the cost of the cumulated Intellectual Property needed to implement the IoT system; iii) the methodology applied to calculate the value introduced by the patented technology for the use in question; and iv) the regime regarding the settlements of disputes. .

---

60 This includes domains of strategic European interests such as health care, connected vehicles, smart energy application, smart cities.

61 See for instance the workshop of 4 November 2015 on "IoT Standardisation and Architectures", with participation of SDO key figures, policymakers EU and global industry and the Commission, https://ec.europa.eu/digital-single-market/en/news/standards-and-architecture-iot-path-convergence-main-outputs-workshop-iot-standardisation-and.

Against this background, industrial efforts are ongoing[62] to develop a transparent, innovative and globally acceptable licensing scheme for all players of the value chain and for the relevant protected technologies of an IoT system.

2.5. Possible obstacles to data flow and access to data

The Digital Single Market strategy already announced that the Commission would adopt a Free Flow of Data[63] initiative, to ensure that data can circulate without obstacles within the Union by removing unjustified restrictions to the location of data and by addressing emerging issues on 'data ownership', (re)usability and access to data (including research data), and liability amongst others in relation to the Internet of Things.

Certain stakeholders are of the opinion that the following are aspects that seem particularly relevant in the context of fostering the wide availability of IoT solutions:

- Uncertainties as regards data ownership in relation to non-personal data;
- Uncertainty as regards data ownership;
- Restrictions to data location; and
- Obstacles linked to data interoperability and reliability.

Among the issues listed above, the concept of data ownership seems to be the most controversial one among the IoT community. Indeed, while the term "ownership", when understood as a property regime on data, cannot apply in respect to personal data (which have to be processed in compliance with data protection rules), it has sometimes been referred to in relation to non-personal data.

Today there is little clarity today as to who "owns" or should "own" machine-generated data or whether there should be an "owner" at all. Depending on the specificities of the IoT-based device/services and the various business models involved, different contractual arrangements may exist, whereby data can be accessed, transferred or used in any other form by different actors in the chain. Certain stakeholders claim that a property regime on data, similar to the one granted on intellectual creations by the Intellectual Property Rights law, would provide more incentives for companies willing to monetise their investments in the creation of data-based services or products.[64]

---

62 See, for instance, http://www.ericsson.com/news/150910-ericsson-invites-industry-players-to-join-its-licensing-effort-for-internet-of-things_244069645_c

63 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN, p. 15

64 For instance, in the agriculture sector, large agricultural corporations such as Monsanto and John Deere offer precision farming technologies and machinery on condition that farmers make the data resulting from such operations available to the corporations themselves. The risk (for farmers) is that such data can be used not only to offer better, tailor-made solutions but also monetise it in ways that disadvantage farmers and provide disproportionate advantage to "first to market companies" benefiting from a large quantity of data in order to optimise their business offers towards a certain market domination.

Contractual practices have led to the creation of a certain ownership regime that defines rights and obligations of the parties involved in the collection and processing of data, including the scope of usage rights to data[65]. Current business models providing for various case scenarios in this respect deserve to be taken into account. These business models show that data generated by an IoT-based device (including data generated by sensors) is not always the property of the owner of the device (or of the owner(s) of the sensors).

According to findings pointed out by certain stakeholders, current contractual arrangements may lead to restrictions in relation to sharing of data with third parties, or to lock-in situations, dynamics that are very relevant during the stages of data processing when IoT data are transformed into valuable data. The Commission services are analysing existing business models and underlying contractual relationships in the data value chain, with a view to better understand 'ownership' models and the contractual conditions under which access is given to data and data are transferred.

Furthermore, data ownership may also lead to obstacles in accessing data. Some public services may in the future increasingly rely on access to data that is privately-owned. For instance, as discussed in the C-ITS platform[66], traffic management systems would be more effective if access to data coming from private vehicles is granted. In particular, certain stakeholders point out the need to further explore whether access to and re-usability of privately-owned data used for public policy objectives should be guaranteed by law, and under which conditions of remuneration, like it has been decided for the public sector information through the PSI directive. The Research Data Alliance[67] has proposed a set of principles for research data that could be relevant also for machine-generated data. The Fair principles on data stipulate that Data should be: (F)indable, (A)ccessible, (I)nteroperable, (R)e-usable.

The potential of technologies, such as blockchains or deep-learning, in the field of IoT could be further explored too. Such distributed architectures could offer alternative and more efficient ways to meet the challenges of interoperability but also of trust and data ownership/usage.

2.6. Safety and liability

Stakeholders and available expertise point out a number of novel liability aspects that appear with the emergence of IoT, which are explained in the following paragraphs[68].

The IoT creates sophisticated interdependencies between product and service producers. Due to the high complexity of the IoT ecosystem (physical objects, software, Internet infrastructure, behaviour of the final user, etc.), the variety of actors involved (product

[65] Such views were expressed by C-SIG members (e.g. business users of cloud services e.g. EuroCIO) in C-SIG plenary sessions and within various working groups.

[66] http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf

[67] https://rd-alliance.org/group/data-fabric-ig/wiki/recommendations.html

[68] Software and mobile applications which qualify as medical device (when they fulfil the definition of medical device) are already explicitly covered by the Medical Device Directives.

manufacturers, sensor manufacturers, software producers, infrastructure providers, data analytics companies and other actors involved in the supply of different services, final users), any actor participating in this ecosystem could potentially have a share of liability. However, assigning liability in such an intricate ecosystem may be difficult. These dependencies are not static: they can increase and become more complex, over the life of the product/service. Any interdependency gives rise to a number of questions, such as:

- Who is responsible for guaranteeing the safety of a product?
- Who is responsible for ensuring safety on an on-going basis?
- How should liabilities be allocated in the event that the technology behaves in an unsafe way, causing damage?

The IoT interdependency can also give rise to challenges in identifying the root cause of product failures, and in determining where responsibility lies in the event of a problem. The IoT may thus aggravate existing problems of proof concerning non-conformity/defectiveness/unsafety of a product, and issues of causation. Furthermore, under existing EU laws, products and services are treated in a distinct manner. Providing data through an IoT system is considered as a service, and thus falls outside the product liability and safety regimes. Where damage or harm is caused by supply of false data or by failure to supply data, liability often may become unclear, and claims potentially difficult to enforce.

Certain academic legal experts are suggesting that current EU acquis might no longer be fit for purpose and needs revision. Possible gaps were identified notably in relation to Directive 2000/31/EC on electronic commerce and the Liability for defective products Directive 85/374/CEE.[69] In this respect, it is important to note that the Radio Equipment Directive 2014/53/EU provides a consistent approach for the safety of the radio equipment including where it incorporates software, the interwork of radio equipment via network with other radio or wireless equipment and the conditions under which the same devices can be considered compliant to the law after this placement on the market.

With the view to better understand aspects of contractual and non-contractual issues surfaced by IoT-based products and services, the Commission is now gathering evidence thorough studies and public consultations.

As far as contractual liability in IoT is concerned, legal uncertainty may arise from machine-to-machine contracting, when smart objects enter into contracts with each other on the basis of autonomous decisions. Questions fuelling the legal uncertainty relate, for instance, to whether and under which conditions the person on whose behalf an IoT-powered device places an order is bound by this.

[69] Findings were highlighted by the experts attending the workshop "Digital Revolution: Challenges for Contract law in practice", organised by the University of Munster, 1-2 October 2015. The findings of this workshop are summarised in Reiner SCHULZE, Dirk STAUDENMEYER (eds), *Digital revolution: challenges for contract law in practice*, Nomos, 2016.

The analysis of use cases is a possible methodology to assess the challenges in this field. In this context, a mapping exercise to clarify to what extent (parts of) these use cases are already covered by existing (legal) frameworks could provide a good starting point. This may also be a basis for an assessment to what extent existing legal frameworks, including sectorial legislation, may still be fit for purpose. An analysis of the existing contractual arrangements between the user and the service provider could be considered a useful baseline in helping to identify whether a liability regime is needed and how it should be designed. Commission services are of the opinion that further investigation may also be needed until envisaging any policy solutions (e.g. in terms of proposing model contracts for the B2B environment, legislation clarifying horizontal or specific liability regimes and/or requiring specific compliance with standardisation frameworks that could tackle liabilities through specific technical requirements).

3. A Thriving IoT Ecosystem

The IoT includes both a vertical and a horizontal dimension. A vertical dimension refers to applications belonging to a single area and a horizontal dimension refers to establishing new use cases (applications) across verticals. A key feature of the IoT ecosystem is therefore the dynamic interaction between the providers and users of horizontal IoT platforms and applications and the providers and users of vertical solutions/domain-specific environments.

The horizontal character of the IoT has to be recognised to avoid fragmentation between industrial and/or domain specific application areas, between standards, between regions and institutional frontiers, thus preventing the full IoT vision to be realised. Also, the IoT requires the development of a new cross-cutting business reality exploiting the momentum to create market impact and establish European industrial leadership.

For this to happen, Commission services are of the opinion that an IoT policy should address specific policy challenges linked to a harmonised DSM, notably to interoperability, ubiquity, end-to-end security and trust. The creation of thriving IoT eco-systems is needed to accelerate IoT developments, to foster innovation and take-up of the IoT in the EU, to avoid that vertical silos develop around established industrial players and other sector specific actors in given sectors slowing down speed and scale of market adoption. The intrinsic nature of IoT requires alliances between multiple sectors, and stakeholders, to cover an increasingly complex value chain and to prevent IoT solutions from reaching economies of scale. It also requires open platforms that can integrate many different types of equipment and applications. The figure below depicts the various actors part of this complex chain.

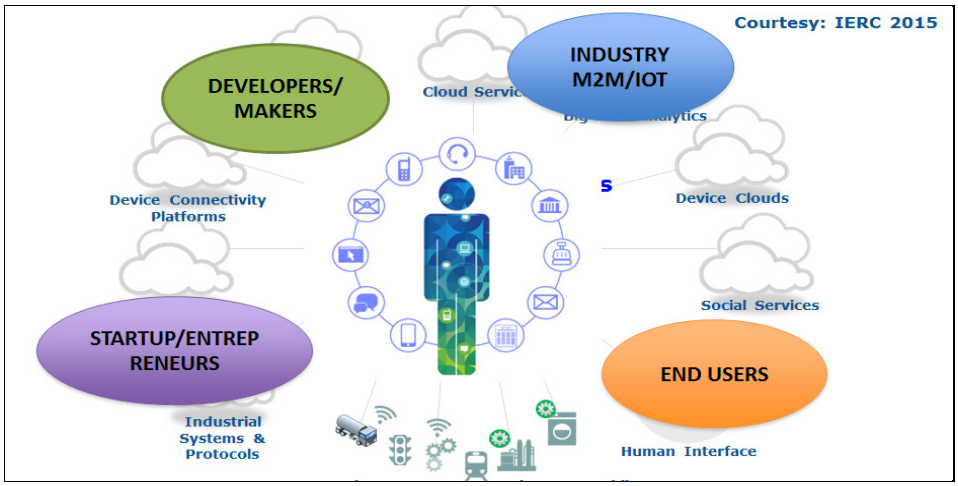

Figure 4: IoT ecosystems

The IoT is to become a major innovation engine and to allow the creation of new ecosystems. Experience from the mobile sector has shown that time and scale are important to be successful in the market. Although it can boast a world class expertise in mobile systems, European companies has not been able to create ecosystems around smartphones. The advent of the IoT will bring to the market new devices, around which innovation ecosystems will take shape. The IoT will act as an essential driver for innovation and competitiveness. More jobs are expected to be created, driven by the need for developers generated from the emergence of IoT ecosystems. While today there are just 300,000 developers worldwide contributing to the IoT, a new report by VisionMobile[70] projects 4.5 million developers by 2020, reflecting a 57% compound annual growth rate and a massive opportunity. This growing need for well-educated employees having the necessary digital skills has implications in terms of education and training in the EU.

This is an opportunity for Europe. One lesson from the smartphone revolution is that market leaders did not actually win through product features, but by creating networks of entrepreneurs. These networks unlocked new demand by fostering the emergence of countless apps and devices that no single company could have created on its own. Future actions could build on the positive experience gained from networks of start-up accelerators in StartupEurope[71] and FIWARE[72].

Given the importance of new initiatives in the IoT area and as stated in the *DSM technologies and public services modernisation package*, the Commission has launched a study to identify and map the most promising clusters across the European Union. In addition, the Commission services are already engaged in working with the Knowledge and Innovation Communities[73] of European Institute of Technology Digital KIC, which bring together leading partners from higher education, research and business, to develop IoT solutions to challenges. The impact of the IoT in various public services (as user,

[70] Available at: http://www.visionmobile.com/product/IoT-breaking-free-internet-things/
[71] https://ec.europa.eu/digital-single-market/en/startup-europe
[72] http://www.fiware.org/
[73] http://eit.europa.eu/activities/innovation-communities

provider or, for example, certification authority) asks for an early involvement of the public sector in the development of the IoT ecosystem.

In 2015, the Commission has launched a series of projects supported by €53 million of EU funding[74]. The aim is to create ecosystems of "Platforms for Connected Smart Objects" and to overcome the fragmentation of vertically-oriented closed systems, architectures and application areas. Up to €10 million are targeted to SMEs and start-ups working with these platforms.

Moreover, in March 2015, the Commission launched the Alliance for Internet of Things Innovation (AIOTI), to assist in the creation of a dynamic European IoT ecosystem unleashing IoT potential[75].

3.1. Promoting open platforms to foster IoT innovation

Promoting open platforms to foster IoT innovation is a key element to achieve leadership in IoT. For this purpose, several cross-sectorial initiatives that will complement the sectorial approach of ongoing PPPs will be launched. Commission services are of the opinion that the development of reference architectures both at EU and national level is essential for industrial leadership in next generation platforms. IoT platforms combine a set of IoT technologies, interface standards, APIs and protocols with development and deployment tools.

Today, the bulk of connected objects' market is predominantly integrated vertically, mainly in non-consumer goods including in buildings, cities and industrial machines. However, there are signs of emerging platform-building in other sectors like automotive and home. In the future, the economies of IoT markets are expected to be driven by platforms setting the standards and controlling market dynamics. Platforms thrive, in principle, when many firms, developers and customers use them.

There are already signs of platform-creation in IoT markets with the arrival of integration solutions offered by companies like Apple, Google or Amazon, and attempts to standardise software layers, as with the AllSeen Alliance. It is a fact that many of these existing or emerging platform initiatives are conceived as proprietary platforms to lock consumers into specific interface standards. However, as Gartner[76] expects there will be no dominant ecosystem of platforms in the next two years (i.e. until 2018), and this would let open the possibility for European IoT platforms to emerge.

According to the Digitisation communication, European companies should strive for leadership in IoT platforms allowing them to manage an ecosystem including SMEs, researchers, entrepreneurs and innovators that is anchored in Europe. Successful platforms should as well be open. This way they can achieve critical mass, allowing platform owners

---

[74] For more details, see: https://ec.europa.eu/digital-agenda/events/cf/ictpd14/item-display.cfm?id=12597.

[75] For more details on AIOTI, check reference box in section 1.3.

[76] Gartner report (2013) "Predicts 2015: The Internet of Things." Newsroom available at: http://www.gartner.com/newsroom/id/2970017, STAMFORD, Conn., December 12, 2013

to encourage third party developers, suppliers and users, as well as competitors to build application and services that run on them – while also preserving the role of leading European stakeholders in key markets.

One example of an open platform is FIWARE, supported through the Future Internet Public Private Partnership (FI-PPP[77]). The recently launched openFIWARE Foundation[78] further develops FIWARE components in the context of digitising industries, starting with three business sectors: Smart City, Industry 4.0 and Smart Agriculture. This is expected to accelerate the industrial use of open digital platforms and reinforce related innovation ecosystems.

3.2. Spurring innovation in lead markets

Tangible business opportunities for the IoT, cloud and data analytics technologies can be found across all the "smart environments" identified by several studies. By combining the estimated market size and the expected market growth of these environments, some market sectors have emerged as those offering the most realistic opportunities now and/or in the coming five years. According to IDC[79], these include Smart Manufacturing, Smart Homes, Smart Personal Health and Wellness. Each of these smart environments is already producing (or will produce by 2020) a number of use cases, which are successfully exploiting IoT technologies, or will do so in the coming years. The following verticals are discussed in greater detail in the Annex:

- Smart Homes will offer business opportunities in home security, energy applications and household appliances.
- Personal Wellness applications and wearable devices for both generic and health-specific purposes are a big opportunity in the area in Smart Health. They will be accompanied by remote health monitoring.
- In Smart Manufacturing, operations and asset management already represent fertile ground for IoT solutions and applications.
- Smart Cities are equipped with sensors, actuators and other appliances providing information that, properly valorised, will improve the living conditions of their inhabitants.
- Smart Mobility will require new mobile ecosystems based on trust, security and convenience in order to ensure the security and convenience of consumer-centric transactions and services.
- Smart Energy: smart meters and smart grids are powered by IoT and can optimise energy consumption, whereas IoT solutions and services can help change behaviour and consumption patterns.
- In Smart Farming data gathering, data processing, data analysis and automation technologies jointly orchestrated allow for improved operation and management of a farm.

---

77 https://www.fi-ppp.eu/

78 https://www.fiware.org/foundation

79 Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination by IDC and TXT, see: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9472

- Earth and ocean observation systems and the future blue economy: IoT can help maximise the use of ocean's potential, in terms of fishing, marine platforms and aquaculture notably.
- Circular Economy: IoT can facilitate the transition to new business models in the circular economy where all actors of the value chains are closely interconnected and use collaborative platforms to share data on resource flows, and end-users are empowered in their consumption patterns.

The AIOTI has established a number of working groups on the areas that it considers more mature for IoT innovation and where there is a greater potential for cross-cutting business models. The Alliance also set the goal to spearhead some markets.

In addition, also supporting creativity-based innovation is essential, in the view of Commission services, giving the strategic position of cultural and creative industries to foster smart, sustainable and inclusive IoT services and products.

4. A Human centred IoT

Strengthening trust, security and end-to-end personal data protection and privacy by taking into account the needs of the digital and digitised industry in the field of IoT is a priority for the European Commission.

4.1. Guiding principles for IoT and avoiding a new digital divide

It is commonly recognised that IoT has the potential to drastically improve our personal lives, our work places and our industrial / manufacturing efficiencies and capabilities. There is, however, a concern that IoT may lead to alienation because of objects capable of 'talking' to one other and to lose sight of human preferences. In order to ensure that IoT improves lives by empowering people instead of transforming them into hostages of technology, Commission services are of the opinion that certain safeguards might need to be put in place or current safeguards need to be made more specific.

The IoT can build connections between human beings and smart, dynamic objects. ICT technologies and objects can minimize isolation; mobility and security solutions support people's participation in society. On the other hand, the 'smarter' the objects in our lives, the greater the scope for misuse. Where in the IoT data are processed that relate to identified or identifiable natural persons, then these qualify as personal data in the meaning of the EU Data Protection Directive 95/46/EC, triggering the application of the data protection rules[80]. Always being connected to the things around us has the potential to lead to more surveillance or more profiling by public authorities and private entities. More generally, without appropriate legal, technical and organisational safeguards, the IoT may facilitate the emergence of a de-humanised world, where machines enforce rules

[80] See Article 29 Working Party "Opinion 8/2014 on the on Recent Developments on the Internet of Things" (WP 223). This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. Website: http://ec.europa.eu/justice/data-protection/index_en.htm

stringently, reduce human freedom, and room for fantasy and contact among them by controlling their behaviour.

A human centred IoT would imply an environment where IoT will empower people and not transform them into hostages of technology. The Commission services are of the opinion that the following questions are important for further reflection in this context:

- How can we ensure end-users fully understand the role, functioning and impact IoT services can have on their lives, choices and environment?
- What precautions should we put in place to make sure our medical information can be accessed electronically, but not by the wrong people?
- How can all users stay in control of their data; how can they all, without specific knowledge of underlying technologies, understand the impact[81] of their decisions on what data is shared with whom[82]?

It is commonly recognised that in order to have a positive impact on people's lives, IoT technologies and their application need to be *trusted, accepted, wanted, accessible and usable*. The Commission services are of the view that IoT should be designed in view of preventing the users from:

(1) failing to use the services (there are many potential causes for it, technology-related but also user-related), or being locked-in by service providers;
(2) substituting completely face-to-face services and interactions (or moving significantly to virtual environments and unreal worlds);
(3) misunderstanding technology, especially its usefulness and impact on the main user and his/her environment and choices, and
(4) mistrusting technology-based systems and services.

In addition, without an appropriate training on the use of IoT, as already highlighted by the *DSM technologies and public services modernisation package* some people can be left behind and may not entirely benefit from the IoT. This can lead to a lack of trust in these new technologies, especially in specific IoT devices (e.g. connected glasses), although other technologies are already used and well accepted (e.g. smartphones). Users would benefit from access to an intuitive interface, from comprehensively evolving Human-Machine Interfaces and from systems respecting the particular context of the user when starting an interaction.

In line with data protection legislation, IoT must be designated and operate so as to comply with the requirements established therein. As regards personal data and privacy, the EU is committed to the highest standards of protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights. In particular the General Data Protection Regulation

---

[81] For example, can our car be tagged to improve mobility and traffic safety? If yes, what precautions do we want in place to ensure that data on our traffic behaviour does not fall in the hands of our e.g. insurance company without our consent?

[82] Some business models currently in place offer "free" data services which are not in reality "free" of charge since they are provided in exchange of the user's personal data.

(GDPR)[83] will increase trust in digital services and IoT, as individuals, public administrations and businesses will profit from clear data protection rules that are fit for the digital age, that give strong protection and at the same time create opportunities and encourage innovation in a European Digital Single Market. Under the GDPR, 'Data protection by design and by default' will become an essential principle. It is expected that it will incentivise businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data. Used in conjunction with data protection impact assessments, data protection certifications, seals and marks, businesses will have effective tools to create technological and organisational solutions for the Internet of Things. The General Data Protection Regulation promotes techniques such as anonymisation (removing personally identifiable information where it is not needed), pseudonymisation (replacing personally identifiable material with artificial identifiers), and encryption (encoding messages so only those authorised can read it) to protect personal data. This will encourage the use of IoT, which can be done using anonymised or pseudonymised data.

The GDPR highlights possible work threads to clarify these issues, and notably:

- The adoption by the IoT industry of specific data protection codes of conducts and certification schemes
- The further development and elaboration of new Data Protection Impact Assessment frameworks and guidance[84]
- The Commission and Member States support and industry involvement in research and development activities for privacy by design and by default technologies and solutions, and in the creation of a viable European market for these technologies.

Special data protection rules apply to electronic communications services directive (e-Privacy Directive[85]) which is in the process of being reviewed, in particular to adapt it to the new general data protection framework and to ensure consistency with the General Data Protection Regulation.

4.2. Trust in the IoT

---

[83] In December 2015, the European Parliament and Council have reached agreement on the data protection reform proposed by the Commission. Once the General Data Protection Regulation and the Data Protection for Police and criminal justice authorities receive formal adoption from the European Parliament and Council, the texts will be published in the Official Journal of the European Union in all official languages. The new rules will become applicable two years thereafter. See http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[84] The Commission facilitated the development of the RFID PIA framework http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf. Another example is the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force: https://ec.europa.eu/energY/en/topics/markets-and-consumers/smart-grids-and-meters.

[85] Directive 2002/58/EC.

In the opinion of the Commission services, the main challenge for the acceptance of the IoT remains therefore users' trust in a broad sense, be it for private, business or governmental use[86]. In this respect, the following challenges should be addressed:

- Ensuring a context-based security and privacy, which reflects different levels of importance (e.g. emergency crisis, home automation);
- Necessary computing capacity to implement sophisticated security protection solutions like Trusted Computing, or Cryptography in Cyber-Physical systems and IoT hardware;
- Trustworthy identification both of users and devices in a distributed environment, where governance structures are not always clear;
- Compliance with data protection rules regarding profiling. Correlation and Information Retrieval, which may support new types of security mechanisms, but also allow for intrusive profiles;
- Anonymisation of both user data and protocol metadata is a challenge in a distributed and mobile environment during data collection and processing;
- Scalability for the billions of devices in IoT and mastering of a wider heterogeneity of connected systems, communication technologies and resource constraints;
- Secure setup and configuration methods for the IoT, as device and software installing present a potential attack surface to Hardware Objects and to applications depending on them;
- Critical infrastructures and the use of IoT where new technologies and devices at home and in everyday life may lead to new security or privacy concerns;
- Conflicting market interests as one of the appealing features of IoT from a business perspective through collection and correlation of data from different sources to increase revenue.

Trusted IoT Label

Security, liability, privacy and data protection are critical challenges for the IoT. Ultimately trust will emerge as a derived characteristic. Industry-led incentives guaranteeing a proper use of data and security to users can be important in this context.

Co-legislators have reached a political agreement in December 2015 on the Network Information Security (NIS) directive[87] that calls for cybersecure solutions in critical sectors, such as energy, transport, health and finance. The NIS directive will require operators in critical sectors to be identified by Member States to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems they use in their operations; the Directive will also require them to notify, without undue delay, the national competent authority or to the Computer Security Incident Response Team (CSIRT) of incidents having a significant impact on the continuity of the essential services they provide. These measures,

86 http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

87 https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation

which may be based on national or international standards, will be subject to audit by national authorities. It is possible that in response to such emerging requirements, operators using the IoT may wish to adopt the Trusted IoT label as a demonstration of compliance, where relevant, to the NIS Directive's requirements.

More generally, a Trusted IoT label could be developed for consumer products, providing transparency about different levels of privacy and security[88].

4.3. Security

Security and the protection of personal data issues are a key concern for a successful take up of the IoT. Whilst IoT deployment is in its infancy, several recent examples of object hacking have shown that the number of attacks is bound to grow exponentially if known vulnerabilities persist as connected objects are increasingly used.

An important issue has to do with secure authentication. Networked devices that exchange data with other IoT devices need to be properly authenticated to avoid security problems. This may need to include certain authentication protocols, and to use integrity-secured or encrypted channels of communication.

The Commission services consider important to reflect upon possibilities for certification of networked devices that would provide a minimum level of secure authentication, from the hardware level to network integrity. This would entail some analysis of the functions with which each device is equipped, secure data processing and secure connectivity for the devices to which data are transmitted.

5. Annex

This Annex describes in greater detail the lead markets introduced in Section 3.2 of this SWD. An investment in IoT technologies is expected to particularly spur innovation in the following areas:

1. Smart Homes
2. Personal Wellness and Wearables
3. Smart Manufacturing
4. Smart Energy
5. Smart Cities
6. Automated Driving / Smart Mobility
7. Smart Farming
8. Circular Economy

[88] Such a labelling system has been implemented as regards energy-efficiency across the EU

9. Earth and Ocean Observation Systems and Future Blue Economy

Areas 1, 2, 5, 6, 7 will each be supported through a Horizon 2020 IoT Large Scale Pilot[89]. Area 3 will be supported through the Horizon 2020 Factories of the Future Public Private Partnership[90].

1. Smart Homes

Powered by consumers' demand, Smart Homes constitute a clear business opportunity thanks to the widespread use and affordability of smart phones, tablets and other mobile devices. The IoT is already enabling a wide range of home automation solutions making homes a "mini IoT environment" in their own right. Home automation solutions (including centralized control of lighting, heating, ventilation and air-conditioning, remote control of appliances, security locks of gates and doors and other systems) are already a reality and, to some extent, an established market. Big players (like Deutsche Telecom, Legrand, IBM, Cisco, and Microsoft among many others) are already experimenting in this area and more interesting developments are expected in the next few years.

Home Security (i.e. video cameras and multiple sensors that can track motion, temperature, air quality, vibration, sound, and any other activity inside a building) is by far the most important use case in Smart Homes today. It is followed by the case of Smart Energy, where IoT solutions are used to improve climate control and heating, ventilation and air conditioning (HVAC) methods and technology to lower energy usage, monthly expenses and greenhouse gas emissions. Smart Home, however, is a much wider concept as IoT solutions can be extended to the varied world of home appliances. For the time being, IoT seems to cover primarily small appliances (Small Smart Appliances, such as wireless blenders, portable refrigerators, mini meteo-stations). In the future, big Smart and Connected Appliances will be more and more connected with sensors and actuators, thus making our fridges, ovens, laundry machines even smarter. Smart homes may also adapt energy consumption based on dynamic tariffs and optimise the management of self-consumption, storage and feed-in to the grids.

When it comes to smart homes as the preferred environment for ageing well,[91] IoT solutions can integrate a range of different devices, data sources and services to increase the efficiency of care, promote independence and improve the quality of life of senior citizens and their caretakers. IoT can support a range of services helping people live

---

89 For more details see Horizon 2020 Work Program 2016-2017: http://ec.europa.eu/digital-agenda/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots

90 Further information available at https://ec.europa.eu/digital-single-market/en/factories-future and http://ec.europa.eu/research/industrial_technologies/factories-of-the-future_en.html.

91 The continuously growing population of elderly people needs support for staying active, independent and out of institutional care settings for longer, while at the same time reducing the costs for care systems and providing a better quality of life for vulnerable categories of citizens.

independently, such as motion sensors that trigger a response from a call centre. The responses may range from a phone call to the person, to alerting a local carer, neighbour, the social services or the emergency services. Other examples include services that alert the person in the home to a particular hazard, such as a water-level monitor in a bath, tele-monitoring for chronic diseases, telecare for people with cognitive decline or remote rehabilitation programmes and supporting adherence to treatment. There is also a great potential in using a range of behavioural and physiological data for early risk detection and prevention of diseases, cognitive decline and frailty.

In the opinion of Commission services, unless Europe provides for more smart and age-friendly homes in the existing residential building stock, many citizens might remain dependent on institutional health and long-term care, with the unsustainable costs that this carries to public spending. Conversely, the investment in the creation of age-friendly homes (AFHs) building on IoT could unlock a previously untapped economic potential bringing better quality of life to individuals, supporting sustainable spending by governments and boosting industrial growth and jobs.

Furthermore, Horizon 2020 foresees the support of IoT Large Scale Pilot activities in this field for strengthening the global position of European industry in IoT developments for ageing well. They will allow the use of IoT platforms and tools for creation and management of integrated IoT products and services for elderly people, including personalised health and energy management at home. They are expected to also cooperate also cooperate with the EIP for Active and Healthy Ageing,[92] including its Silver Economy aspects[93].

2. Personal Wellness and Wearables

It is foreseen that wearables will be a lot more present in our lives. While many technological challenges have been overcome (near-field communications, energy use, miniaturization etc.), others remain, many of which are not technological (e.g. access to the data and data ownership). Barriers to the adoption and acceptance of wearable devices should be identified and overcome if the benefits of large scale deployments are to be achieved.

Wearables are most effective when they move beyond the collection of data and the simple monitoring of data readings to actuating and, ultimately, to the creation of a closed loop system. Already there is an example of LED lighting being used to create pain relief[94], this being triggered when the device receives the appropriate signals from the wearable. Typical healthcare challenges in Europe and elsewhere (such as increasing expenditures and an increasing number of patients) will be more and more enabled by IoT solutions. It is expected that the IoT will play an even greater role in the coming years

92 https://webgate.ec.europa.eu/eipaha/actiongroup/index/what

93 https://ec.europa.eu/research/innovation-union/index_en.cfm?pg=silvereconomy&section=active-healthy-ageing

94 E.g. https://www.elixa.com/light/healing.htm

when personal wellness solutions for generic purposes (e.g. devices measuring daily calorie in-takes, hours of sleep etc.) will become more popular.

We should also consider cases whereby a device can perform more than one function thus addressing different interest groups. For example, a medical sensor taking or recommending an action might also serve as a security verification tool, opening doors to restricted areas depending on the user's level of security clearance.

3. Smart Manufacturing

Smart Manufacturing is projected[95] to be the number one IoT use case in Europe in the logistic chain and production line. The proliferation of machine-to-machine devices enhances the functionalities of smart products and smart services, and leads to global plant floors and autonomous factories. In the future, all forms of advanced industry will have to become more intelligent to compete effectively. This intelligence may rely on advances through IoT and advanced connected objects that provide sensing, measurement, control, power management and communication. IoT will enable new levels of factory automation for greater efficiency, higher flexibility, agility and lower operational costs.

Direct customer input to design will increasingly enable companies to produce customised products with the shorter cycle-times and lower costs associated with standardisation and mass production. Intelligence should also be built into even the smallest steps of the process. Intelligent monitoring also enables better predictive maintenance, enhancing the stability and safety of the production process. Vibration sensing, for example, can give an early warning when motors, bearings or other equipment need maintenance. Algorithms enable mechanical engineering firms to predict possible machine outages and hundreds of data points help optimize numerous production workflows.

Physical production processes are increasingly at the centre of much wider value chains. Intra-plant and extra-plant logistical processes are integrated reducing the cost for warehousing to zero. Interconnecting the entire value chain via mobile or fixed-line high-bandwidth telecom networks synchronizes supply chains and shortens both production lead times and innovation cycles.

Communications both wired and wireless, is frequently the gating factor in systems for automated manufacturing. Increased bandwidth will also be important, especially for wired communications, pointing to greater use of Gigabit Industrial Ethernet. The smart factory represents a fundamental change in how production processes are set up and organized. It may also lead to the decentralization of manufacturing, may provide greater intelligence where production activities take place, and create an overall system that is cognitive and resilient.

4. Smart Energy

[95] https://ec.europa.eu/digital-agenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

Digital technologies are an essential ingredient of the transition to the 21st century low-emission energy and can support the new panorama of the service-oriented energy system responding to new expectations of the customers for high-quality, personalised services available 24/7. As a first step, the current roll-out of smart meters and smart metering infrastructure in Europe will open up wide opportunities for connecting the smart homes, smart buildings and industry 4.0 with the energy grids.

The availability of cheap connected IoT sensors is the basis for more refined and decentralised real-time monitoring and control of energy supply and demand, on the basis of accurate measurements and forecasting. This contributes to the adoption of renewable energy, which requires controls with faster reaction times and needs to be balanced with flexibility of generation, active demand and storage.

The energy system infrastructure is based on large expensive technical assets with long life-times. Smart asset management and condition-based maintenance based on the information distilled from IoT sensor data allows optimised investments in operational and capital costs of the European energy infrastructure.

The smart management of energy systems based on IoT data also enables the development of optimised decentralised solutions based on a closer integration of various elements of the energy system, exploiting the combined capacities and flexibilities of electricity, gas, heating and cooling, and transport sectors.

5. Smart Cities

Towns and cities across the European Union provide a home to more than 70 % of the EU's population. Cities, in particular, are seen as both the source and solution to economic, environmental and social challenges and are therefore central to achieving the Europe 2020 goals of 'smart, sustainable and inclusive growth' in Eurostat terms[96].

IoT technology merges the distinct pillars of the modern city (energy, mobility, buildings, water management, lighting, waste management, environment, etc.) into a structured, interconnected ecosystem supporting the city's population. These technologies should integrate robust respect security features as well as privacy by design and by default, reduce cost, emissions and energy consumption while being reliable, long lived, future proof and scalable. The aim is to create a city centric ecosystem of state-of-the-art to increase the efficiency of the city by enabling unobtrusive, adaptable and highly usable services at the points of network-edges, gateways and cloud storages.

The Smart City of the future should be capable of many of the functions we normally associate with a living entity; it will need to sense its own state, identify unusual or threatening circumstances and then create and execute plans to maintain people's safety and its own functionality. Doing this requires highly scalable, connected systems capable

[96] http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_European_cities

of sensing, acting, controlling, balancing and forecasting in an uncertain and unpredictable environment.

In this context, the Smart City is becoming one of the biggest fields of application for IoT technologies. Cities are increasingly filled with devices equipped with sensors, actuators and other appliances providing information that, in the past, was either impossible or relatively difficult to gather. Their main purpose, among other functionalities, is to gather information about various parameters of importance to management of day-to-day activities in the city and to longer-term development planning. Examples of such parameters are information about public transport (real-time location, utilization), traffic intensity, environmental data (air quality), occupancy of parking spaces, noise, monitoring of waste bins, energy consumption in public buildings, etc.

Smart Cities have emerged as a key customer group for FIWARE. Attracted by its open nature and multi-vendor approach, cities are interested in making FIWARE part of their operating systems. The recent announcement by Telefónica, Orange, and Atos[97] focusses on building and supporting standards for smart cities based on FIWARE's open specifications. The network of "Open & Agile Smart Cities"[98] connected in February 2016 89 cities around the globe.

6. Automated Driving/Smart Mobility

Examples of opportunities and added value that the IoT and digital technologies can bring to the transport sector include connected and automated driving; hybrid-electric, silent and reconfigurable aircraft; personal air vehicles; smart vessels; smart logistics, new forms of mobility and business models; next generation air traffic management; reduction of noise and CO2 emissions in aviation; and the Behavioural Digital Aircraft[99] concept. The concept of Connected Vehicles (vehicles connected to other vehicles and/or to the infrastructure, potentially being semi-autonomous and autonomous) is the next step for future smart transportation and mobility applications.

Connected and automated vehicles have a significant market potential, not only for European vehicle manufacturers and suppliers, but also for the European ICT industry, mobility service providers and SMEs. The combination of advanced connectivity systems and automated vehicles could disrupt the entire road transportation ecosystem. Connected and automated vehicles can enable the breakthrough of new "mobility-on-demand" services and innovative digital services in areas such as entertainment, commerce, vehicle management, etc. New mobile ecosystems are then based on trust, security and convenience to mobile/contactless services and transportation applications in order to ensure the security, mobility and convenience of consumer-centric transactions and services.

---

97 https://www.fiware.org/news/telefonica-orange-engineering-and-atos-join-forces-to-push-common-standards-for-smart-cities-based-on-the-fiware-platform/

98 http://oascities.org/

99 Following the work undertaken by the CRESCENDO Project funded under the EU's 7th Framework Programme for Research

Notably, connected systems in transportation may attract particular attention from car manufacturers, policy-makers, ICT companies, service providers, users, and investors. IoT technologies can be deployed to connect automobiles to outside systems and road infrastructure. In doing so, automobiles can relay and share traffic data, speed data, offer safety and communication channels for driver-vehicle or inter-vehicle interactions. This way, IoT technologies create a connected and automated vehicle with strongly reduced driving load, and even driverless cars, as part of a seamlessly integrated transportation system. This can contribute to several transport policy objectives regarding safety, efficiency of traffic flows, infrastructure capacity and energy efficiency.

In the global context of road transport, connectivity will be a critical enabler supporting new business opportunities favoured by EU and Member States' policies on transport and future mobility services. The IoT will contribute to the collection of additional data, besides data already collected by vehicles and traffic management centres. Big data analytics taking advantage of connected road users will increase the understanding of complex traffic situations and flows, leading to e.g. more optimised responses to emergencies, to prediction of road-user behaviour and route planning. This data, exchanged on the road and on the Internet, will be useful in the development of new services for vehicle users, as well as new means of transport management.

IoT furthermore enhances the opportunities for individualisation and personalisation of not only transport solutions but also configuration of messages, human-machine interfaces, driver training etc. Wearables are being introduced as a means of monitoring road user health, and holds potential for contributing to increased road safety. IoT will therefore enable new forms of mobility with increased access and accessibility for persons and goods as well as opening for new business models. Extended opportunities will include other modes of transports, such as automated vessels and integrated logistics.

Although in principle, automated driving is possible without a sophisticated communication infrastructure[100], implementing it requires connectivity, like e.g. navigation positioning and high-resolution digital maps. In fact, fully automated driving based only on on-board control systems without any support from wireless communication systems is until now not trialled and tested. In all likelihood, IoT/connectivity and autonomy must be combined, exploiting both the evolutions in network connectivity and low latency and the capabilities of local vehicle control and autonomy. In addition, connected and automated driving can benefit from local transport services. These allow vehicles to adapt in real time, e.g. to the traffic situation, to road conditions (e.g. rain, ice, damage etc.) and to unexpected events (like an accident).

7. Smart Farming

Smart Farming is understood to encompass the application of data gathering (edge intelligence), data processing, data analysis and automation technologies, that jointly orchestrated allow for improved operation and management (analytics) of a farm with

[100] Recently, there have been several demonstrations based only on on-board sensor systems (e.g., Audi 550-mile piloted drive from Silicon Valley to Las Vegas in 2014 -Audi AG, October 2014).

respect to (near real time) standard operations and re-use of these (animal-plant-soil) data in improved chain transparency (food safety) and chain optimization (smart data). In this sense, smart farming is strongly related, but not limited, to the concept of Precision Agriculture and Precision Livestock Farming. IoT and smart farming applications will set new trends in ICT and agriculture, such as solutions adapted to small- and medium size farms, improvement of farm management systems, development of new agri-food business models and enhancement of "transparent farming" approval among European consumers and markets. IoT and smart farming applications hold many promises for a more sustainable, productive and competitive EU farm sector.

The agri-food supply chain is very complex: there are many different players involved and dynamics in the industry are constantly changing. There are also differences in the food supply chain (depending on the types of products and the locations in which they are produced) and a high degree of volatility (mainly linked to the changing climate, political actions and social changes). Moreover, consumers now want to know more and more about the content and safety of their food, where and how it is produced and what the environmental and social impacts are.

Promoting a broader uptake of smart farming technologies at EU level is key to ensuring a Digital Singe Market for the IoT applied to agriculture. The final report of the Precision Farming Focus Group, set up under the EIP-AGRI[101], provides recommendations for future research activities and potential EIP Operational Groups that could contribute to mainstream smart farming technologies in Europe.

8. Circular Economy

Fully customised and collaborative business models hold large potential for achieving a circular economy where people can shape products and services according to their needs and where manufacturing becomes more flexible and more human-centric.

Recent studies[102] have highlighted how the interplay between circular economy and digital enablers, such as IoT, provides a fertile ground for innovation and value creation.

The Circular Economy to be effectively and efficiently implemented requires a systemic approach to eco-innovation and the adoption of new business models for sustainable production and consumption patterns. In this systemic change perspective, it is crucial to redesign the whole value and supply chains, from devices and applications, to production processes, from logistics to retails. IoT can become the facilitator of this transition that can contribute to reindustrialise Europe, through a customised production that would take place closer to the end-user by setting up a complex ecosystem of on-demand services and temporary use of assets based on exchanges via online platforms[103].

9. Earth and Ocean Observation Systems and Future Blue Economy

[101] http://ec.europa.eu/eip/agriculture/
[102] Intelligent Assets: Unlocking the Circular Economy Potential, Ellen MacArthur Foundation 2016
[103] Upgrading the Single Market: more opportunities for people and business (COM(2015) 550 final)

Horizon 2020 includes initiatives to improve both earth observation systems to monitor agricultural production and ocean observation systems for navigation and collecting, transmitting, storing and analysing data. Furthermore, the Blue Growth focus area addresses infrastructure in the Arctic and Mediterranean, monitoring of marine resources, and maximising the use of the oceans' potential. The promises of IoT technologies can spur developments in many value chains of the future blue economy and their synergetic interactions.

Seafood traceability has a strong potential for sustainable fisheries, especially in the context of global fight against unsustainable, illegal, unreported and unregulated fishing. It will therefore help address the increasing need for food security and safety for the EU and the growing world population, in balance with healthy marine ecosystems. Moreover, seafood traceability could lead to the optimisation of seafood waste in a circular blue economy.

Interconnection through communication networks across private, public and industrial spaces, and reporting about the status of the surrounding environment could help generating and capturing synergies between off-shore industries or seabed infrastructures while addressing environmental concerns in the largely unknown global ocean. Long term efforts to provide seamless access to marine data are paying off with new products and services emerging on the blue economy.