DIGITALEUROPE

DIGITALEUROPE's Views on the Internet of Things

Brussels, 14 April 2016

Executive Summary

The Internet of Things requires an innovation friendly approach to policy. The pace of change is very high and many technologies and business models are still emerging.

There is a clear need for a permissive but accountable approach to new developments to allow innovation whilst maintaining appropriate safeguards to security and privacy.

In general, the EU's approach to IoT policy should be guided by the following principles:

1. Be pro-innovation and pro-competition
2. Recognise the global nature of digital and remain open to free trade
3. Take stock of existing, harmonised and horizontal legislation before focusing on vertical regulation
4. Adopt simple and flexible rules for businesses and consumers
5. Encourage industry led standards
6. Involve and consult regularly with all interested stakeholders

We encourage the European Commission to take stock and make use of existing legislation before rushing into developing new regulatory measures. New legislation should only be considered where necessary and kept to a minimum to maximise innovation. One of the key elements in all actions is speed, to keep pace with innovation and technological developments.

We also encourage the introduction of an Innovation Principle to all future legislation so that whenever a policy or regulatory decision is under consideration, the impact on innovation should be fully assessed. In particular, that means a strict assessment as to whether the proposal is the minimum intervention for the objective, that it is technology neutral, business model neutral, that objectives are clearly identified and progress against the objectives and impact monitored against the original impact assessment.

For more information please contact:
Damir Filipovic, Director – Digital Economy
+32 2 609 53 25 or damir.filipovic@digitaleurope.org

CONTENT:

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

INTRODUCTION

The Internet of Things links the physical and digital worlds

The billions of connected things around us are helping drive a new digital revolution. Nearly 5 billion connected things today, reaching 25 billion by 2020, open the doors to entire new ways of living, thinking and operating. This revolution is transforming every part of society, every sector in industry and the entire government apparatus. Interactions in the value chain of a business, interactions amongst citizens, interactions between the government and citizens and interactions between businesses and citizens are changing forever.

The Internet of Things (IoT) has arrived and Europe has the opportunity to lead the way.

The convergence of the physical and digital world is enabled through sensors, connected devices, networks and cloud based platforms. Throw big data analytics at it and suddenly you can extract transformational benefits out of all the insights collected from connected devices and sensors.

The potential is huge when you know that 90% of data created at the edge of the IoT is never captured, analysed or acted upon in real-time 60 percent of that data loses its value within milliseconds of being generated. All of this data is lost without ever turning it into insights or automated real-time decisions and actions. That is where the potential lies! It isn't just the ability of connecting devices, but now it has become the ability of feeding data into automated decision loops, or with more time using intelligent systems to consume the data, analyse it and generate actionable insights. We have moved from "What is happening?" to "Why did it happen? What could happen? What should happen?"

The convergence of various technology shifts is accelerating the IoT deployment:

1. The cost for low-power networking technologies allowing things to communicate has fallen dramatically, allowing virtually any aspect of our environment to be connected and to interact.
2. The number of connected devices is growing and this has resulted in an explosion of data about the environment around us.
3. Many of the IoT input/output functionalities can be organised in a wearable way, supporting people and their needs most closely
4. Cloud as a growth engine for business has offered agility and flexibility for businesses to respond to changing market conditions. New solutions can be deployed quickly and cost effectively.
5. New ways to engage the business and its customers through real-time information offering decision-making power in the palms of a hand.

IoT offers a transformative business opportunity in a way to:

1. Improve product development
2. Optimize asset productivity
3. Increase operational efficiency
4. Gain real-time responsiveness
5. Drive customer engagement and improve user experience
6. Unlock new revenues from existing products and services
7. Inspire new working practices or processes
8. Support more convenient and enjoyable ways of life
9. Change or create new business models or strategies

DIGITALEUROPE is presenting in this document policies that are of importance to help create the right legal framework to support the Internet of Things and potential use cases in the Internet of Things with actual real-world examples.

POLICY RECOMMENDATIONS

Connectivity

The Internet of Things is expected to be the next wave of the 'digital revolution'. One of the key prerequisites for the successful implementation of the variety of IoT applications and use scenarios is the availability of ubiquitous, reliable high-capacity networks which can support the heterogeneous and often 'always on' requirements of IoT driven IP traffic.

While the target of achieving 100% coverage of basic broadband (through land network - fixed and/mobile), Europe is not on track towards ubiquitous availability of high-speed, high-capacity connectivity. To merely achieve the existing 2020 broadband targets, the investment gap is 90-106bn euro1 and considering the connectivity requirements are likely to exceed the existing targets, the investment gap may be even larger.

According to a McKinsey study from 2012, building out FTTH to cover 50% of households and vector-based VDSL to cover the remaining 50% (enabling speeds above100mbps) will require investment of around €200-250bn and €50-70bn to bring LTE to 95% of the EU15 population.

Satellite coverage can play a role as complement, or back up or being beside land network (fixed and mobile).

A number of factors will determine which connectivity technology to choose from depending on the requirements of IoT services and devices:

- Data or speed rate (upload/download/symmetry)
- Motionless or mobile (range, coverage, location accuracy)
- Latency[2] (synchronous/asynchronous, remote data storage and computing resources)
- Redundancy (availability)
- Security (networks, identification, authentication, encryption, protection)
- For use by Consumers, in addition to the use by Enterprise, Privacy Protection
- Density (address space, dispersed or concentrated)
- Service level agreement (provisioning, management, monitoring, end-to-end QoS)

Both wireline and wireless technologies, including backhaul networks, are essential to connect IoT devices, depending on the use case scenarios.

1 The €90bn is from the Commission staff working document accompanying the Connected Europe Facility proposal from 2011. The €106bn is from the recent Boston Consulting Group study: https://etno.eu/datas/publications/studies/FINAL_BCG-Five-Priorities-Europes-Digital-Single-Market-Oct-2015.pdf

2 It has to be noted that telecommunications networks and their likely evolutions do not seem sufficient yet to cope with very stringent timing and reliability requirements for applications such as the full automation in driverless cars. Hence a specific IoT effort involving the automotive and transport ecosystem as well as the digital and electronics industries should be considered

In the future, 5G will be designed for use cases expanding from man to man to machine to machine requiring more from networks. It is expected to accommodate a wide range of IoT use cases with advanced requirements, especially in terms of latency, resilience, coverage, and bandwidth but also flexibility, low costs and low consumption of energy to fulfil vertical-specific requirements later described in this document. 5G will offer an expected peak data rate higher than 10 Gbit/s (compared to the 450 Mbit/s LTE can offer today), combined with virtually zero latency, i.e. less than 1 ms, meaning that the radio interface will not be the bottleneck even for the most challenging use cases. Flexible integration of existing access technologies such as LTE and Wi-Fi with new technologies creates a design that is future proof at least until 2030 by re-using legacy investment.

In order to achieve the best connectivity, key for the entire European industrial base, Europe needs to refresh its telecom regulatory environment to create healthy ecosystem enabling investments in best in class networks. The review of the telecommunications framework to incentivize investment is essential if Europe is to reap the benefits of IoT.

European policy makers should urgently focus on creating the right conditions that would boost investment in networks and prepare the ground for 5G. In addition, DIGITALEUROPE recommends harmonised spectrum and technology cohesion (avoiding technology fragmentation). Good example are efforts of the Commission and international agreements already signed on 5G cooperation and research.

Does IoT require IPv6 addressing?

IPv6 over IPv4 is a key enabler to IoT:

- The transition to IPv6 is on-going and unavoidable as infrastructure operators are implementing it.
- It offers a highly scalable address scheme to cope with the explosion of IoT devices.
- It solves the Network Address Translation (NAT) barrier due to the limits of the IPv4 address space.
- IPv6 provides for IoT devices to have multiple addresses and an even more distributed routing mechanism than the IPv4 Internet.
- IPv6 provides features that are useful both for the operation and the deployment of IoT (including multicast, anycast, mobility support, auto-configuration and address scope).

IPv6 is the universally agreed, preferred communications protocol for IoT for scalability, security by design and simplicity.

Spectrum

IoT infrastructure and devices are expected to be inter-connected wirelessly and whilst a number of existing air interface technologies may satisfy some requirements today (e.g. WiFi, Bluetooth, GPRS, etc.)3, these may not be suited to all applications that might require for example, longer reach, higher reliability, lower latency, better building penetration and so on.

DIGITALEUROPE expects the IoT and M2M market to grow tremendously and EU policy makers and national administrations are making recommendations on future policies to facilitate its growth in a coherent and harmonised way. Removing some of the barriers to appropriate spectrum access is one such recommendation.

DIGITALEUROPE recognises the work carried out by the RSPG assessing the common key requirements for M2M applications today which can include[4]:

- Often low power/low duty cycle (due to battery consumption constraints)
- Various radio access components are needed to address the demands of several sectors
- Several applications require frequencies below 1 GHz due to propagation characteristics (e.g. penetration through building walls)
- Usage of commercial networks (responding to various needs)
- Moderate requirements on robustness and latency
- Very high density in urban environments
- Low per-device cost solutions
- Often installed for a long period of time.

DIGITALEUROPE, in addition, recognizes other key requirements for IoT and M2M:

- Sometimes extended duty cycle
- Some applications would depend on the use of frequencies above 3GHz due to extended bandwidth demands
- Some applications would depend on highly reliable and robust circumstances
- Some applications would depend on very low latency.

Industry is aligning around widely harmonized standards by:

- Working to develop and advance 3GPP technologies for IoT, such as NB-IOT and LTE eMTC, allowing operators to substantially reuse existing network and device technologies
- Proactively supporting standardisation and spectrum regulatory activities for the IoT wideband SRDs
- In general, creating the necessary market conditions for industry growth and common standards to enable larger eco-systems, economies of scale, and affordable devices.

3 The usual effective working ranges for these technologies are: Bluetooth (10 – 15 m), WiFi (100 – 300 m), GPRS / WCDMA (1 – 100 km).
4 RSPG13-540 (rev2): RSPG Report on Strategic Sectoral Spectrum Needs

Defining 3GPP radio technology for the rapid, efficient deployment of IoT will be beneficial for:

- Meeting massive IoT requirements with complementary technologies: NB-IOT, LTE Release 13 MTC, and EC-GPRS that can be leveraged opportunistically based on availability, use case, and deployment scenarios
- Capitalizing on LTE availability to deploy NB-IOT in the guard band of LTE systems, or as a stand-alone carrier in, for example, GSM bands.

Accelerating in progress IoT wideband SRDs standardisation and spectrum regulatory activities will be beneficial for:

- Building/Home Automation complementing support to the global Smart Metering EU programme (according to EC mandate M441)
- Complementing cellular, especially for those massive non-nomadic use cases
- In general, delivering IoT solutions to the market in a timely manner.

European administrations in CEPT have been studying the IoT and M2M spectrum needs and offer a view that most M2M applications (e.g. Smart Metering, vending machines, home alarms, remote monitoring, etc.) existing today or foreseen can be carried over SRD, RLAN, PMR or MFCN (commercial cellular mobile broadband networks such as GSM, GPRS, WBCDM, and LTE).

Therefore, frequency bands can be made available for, but not limited to, M2M through licence exempt or licensed designation for mobile networks. Both administrations and stakeholders believe that the predicted growth of M2M applications will put pressure on the use of existing frequency bands, including bands for SRD, especially below 1GHz.

Consideration of the licence exempt approach has resulted in new entries in CEPT's ERC Recommendation 70-03 Annexes 1&2 for the frequency ranges 870-876 MHz/915-921MHz. IoT wideband SRD technologies such as 802.11ah, 802.15.4t etc. would benefit from EU harmonisation of these bands.

Consideration of the licensed approach leads to a suggestion that M2M can be effectively deployed in any harmonised mobile networks band, including 700MHz, 800MHz and 900MHz. One additional option would be the identification of the 2x3 MHz in the 700MHz band (733-736MHz and 788-791MHz) for M2M communications on national basis, as considered by the ECC Decision (15)01.

DIGITALEUROPE welcomes these studies and developments on the spectrum needs and the high level of interest in the IoT and M2M developments. DIGITALEUROPE wants to ensure that Europe remains at the forefront of the IoT and M2M developments and that as the market develops there may be reasons to re-appraise the spectrum situation to minimise fragmentation of the market and drive interoperability.

For mobile connectivity/nomadic (or semi-nomadic), DIGITALEUROPE recommends harmonised spectrum and technology cohesion (avoiding technology fragmentation) and in particular as resulting from the current work on M2M in the CEPT with regards to spectrum harmonisation and the usage of 3GPPP global standards, e.g. NB-IOT and LTE eMTC in Europe[5].

5 EC Decision on the use of the 700MHz band in Europe

Network Neutrality

An open Internet, innovation and investment in all parts of the Internet ecosystem are a prerequisite for a competitive and dynamic IoT sector in Europe and the source of a wide variety of rich and innovative content and services. DIGITALEUROPE supports competition-friendly policies that guard against discrimination and promote transparency whilst allowing for commercial arrangements that benefit consumers, businesses and public administrations alike.

Given projected requirements for IoT quality of service differentiation, net neutrality is a subject of particular relevance to the growth of IoT across the European Union. Machina Research estimates that the number of M2M devices requiring some form of differentiation of quality of service is likely to grow significantly over the next few years making up over 50% of all M2M devices by 2020. Those M2M devices requiring comprehensive or stringent Quality of Service (QoS) standards are estimated to increase from 1 billion to 3 billion units.[6]

The Telecom Single Market Regulation introduced measures on safeguarding open internet access that will apply from 30 April 2016. The Body of European Regulators of Electronic Communications (BEREC) has been charged under the Regulation with laying down guidelines for implementation of the net neutrality provisions by national regulatory authorities (NRAs) by September 2016.

It will be important to the success of the Internet of Things to interpret these rules and understand how they play out in the IoT ecosystem. Clarification by regulators will be necessary to allow IoT actors to obtain legal certainty as to how their networks and services will be interpreted in this context. Misinterpretation of the rules could lead IoT providers to avoid launching, or restricting, certain services to avoid the risk of falling foul of the Regulation.

While we do not believe that IoT services will be classified as internet access services (IAS), certain IoT services will fall under the 'definition' of specialised services, and hence will need to take care not to impact the quality or availability of IAS and to assess whether optimization is necessary to meet the quality level envisaged.[7]

Many more IoT services will fall entirely outside the scope of the Regulation as they do not relate to public provision of electronic communications. It is in particular important that the BEREC guidelines follow a technical interpretation of the provision that specialised services are services where optimisation is necessary to ensure an enhanced level of quality. For those IoT services which may fall under the Regulation as a specialised service they will need to have specific QoS parameters attached to them, e.g. for reliability.

As an Internet access service is inherently a best effort service, the need and end-user demand for specific QoS parameters render the optimisation of the service necessary. The guidelines should refrain from applying a further interpretation that specialised services should be limited to services that need to be optimised e.g. to deliver a public interest. This would firmly be against the intent in the Regulation, as clarified by the Commission's statement following the political agreement, and could foreclose innovation in and development of IoT services.

6 Source: Machina Research (2015), DNA of M2M, www.machinaresearch.com.
7 It is worth noting that in this circumstance, the statutory responsibility is on the service provider in question to meet the obligations. Other actors in the IoE ecosystem may need to design their elements of the solution with this in mind but are not directly responsible.

Platforms

Platforms provide a foundation for devices to connect and communicate from anywhere in the world and an environment for building and managing IoT solutions. They are the enablers of the internalization of Internet of Things solutions at high performance and cost-effective scale.

Platforms have been playing an increasingly central role in our lives and have proven to be beneficial for consumers, businesses and the economy, as they drive innovation, create new markets, and increase consumer choice whilst lowering costs and prices.

The Digital Single Market discussions on online platforms should not be confused with the platforms used for Internet of Things. The IoT Platforms should be pursued by industry and provide high degree of data security and data protection.

Data Protection

A significant proportion of the data in the IoT can be regarded as "personal data" which means it falls under the legal requirements of the 95/46/EC Data Protection Directive and the future General Data Protection Regulation (GDPR).

While the GDPR broadly maintains the definition of personal data as set out in the 95/46/EC Directive (any information relating to an identified or identifiable natural person), it expanded the definition by including identifiers such as location data or online identifiers. This expansion has resulted in a wide variety of data such as IP addresses, cookie identifiers and radio frequency identification tags (RFID) being classified as personal data.

There is some concern with the recently adopted GDPR that it will actually block or even prohibit certain IoT solutions. This is particularly true when applying the purpose limitation principle, which entails that personal data collected for a specific purpose can only be further processed for a purpose compatible with the purpose of collection. For any further processing, an entity must ascertain whether the processing for another purpose is compatible with the purpose of the data collection.

While the GDPR lists a number of elements to take into account for this assessment, which provide some flexibility, further processing will any case require notification of the data subject, which may be difficult to operationalize and overall it will be difficult to conduct further processing. This will have a direct impact on big data applications and IoT solutions.

Notification and consent are difficult concepts to apply in the IoT world. M2M devices, such as sensors and actuators, often do not have a user interface, so providing information and check-box options will not always be possible. Moreover, their pervasiveness in the environment could make decisions that are not somehow clustered and centralized irritating for the data subject. Would the data subject want to be pestered thousands of times as they walk down the street?

One solution to problems with notice and consent, and indeed further requirements such as fulfilling data subjects' rights, is for IoT providers to design their systems not to collect personal data. In some circumstances this is fairly straightforward. Sensors collecting soil acidity data on a farm are unlikely to be seen to be collecting personal data.

Others are more complex, such as when the existence of a device owned by an individual is registered but care is taken to ensure that there are no means to identify the individual, for example by avoiding the collection of identifiers or on other factors specific to a person. The ability to allow such anonymous processing to take place will be central to the success of the IoT. Policy makers and data protection authorities need to take a pragmatic approach in determining whether data is 'sufficiently' anonymous, rather than urging an ever more cautious approach that treats all data as if it is personal, 'just in case'.

Pseudonymisation of data will also play an important role. It should be noted, however, that relaxing the obligations on fulfilling data subject requests is only a fraction of the legal obligations that a service must meet in processing personal data and often not the most complex ones. As such, it can only be a partial solution.

IoT solutions should be developed with privacy in mind. This means the concept of "Privacy by Design" should be promoted and a standardized approach should be developed. Such an approach is proactive, not reactive, which means it will allow anticipating and preventing privacy-invasive events from occurring; it is important not to wait for privacy risks to materialise, privacy by design extends throughout the entire lifecycle of the data involved, from start to finish.

Data Ownership, Access and Re-Use

Very often you hear that data is the "new currency". The increasing use of data has initiated a debate on "data ownership". There is no straightforward answer, the B2C context is different from the B2B context, and a further breakdown will be necessary by use cases.

Access to, transfer and the use of data, is already covered by the existing legal framework, including data protection, competition, unfair commercial practices, contract and consumer protection law. To the extent that the processing (including access, transfer and use) relates to personal data, which is very broadly defined in Europe encompassing any data that has the ability to identify an individual. The rights of individuals are extensively regulated by the current and upcoming data protection rules. Rights of access and use between commercial parties processing both personal and non-personal data should be set by contractual relations between the various parties involved.

In the B2B context, the data accessed and used is usually defined through contracts between the different companies or organisations involved. Given the disparate entities potentially involved in the offering and differences in the nature and purposes behind the generation of certain types of data, we are not convinced that a uniform regulatory solution is preferable to existing contract negotiations. Not all of the actors involved in a 'system' will have equal claim to all types of data. Where additional analysis or combinations of data have been used to draw out new insights this is clearly added-value brought to the data by the processor in question. Even the customer who opts for a specific solution may not need access to all the data being generated. Some data may be business confidential, whereas in other cases they may decide they have limited interest in the data in question and may be willing to trade it against other advantages in contract negotiations. Without evidence that such negotiations are proving unworkable, we do not see a need for regulatory intervention.

In the B2C context it is assumed that the data subject should decide on the use and re-use of his/her data. Granting the right to a third party to access and re-use the data should be done through explicit consent or through a legal contract. However, there are instances where this could give rise to certain challenges. One must consider intelligent transport management which requires the collection of personal location data to map and predict traffic flow. Accuracy improves as more traffic data is connected.

To conclude, contractual relations and existing rules are sufficient. It is currently premature to conclude that new legislation is needed. The existing rules should be carefully assessed according to various use cases and soft regulation should be promoted.

Data Location

Data flows and data location restrictions represent a barrier for the development of IoT services. One example is mobility services across countries.

Given the importance of the global nature of the Internet based economy, restricting data flows and requiring local storage will strongly impact both international and domestic service providers and their customers. Data location requirements create barriers to market access, particularly impacting small and medium sized enterprises (SMEs), which are eager to attract customers not only domestically, but also in foreign markets. Data location requirements impede on the ability to operate in a global market without inherently improving security or privacy outcomes.

It is important to carefully balance the impact of the domestic policies with its potential impact on global trade, technological innovation and the benefits of information. In relation to the commercial sector, we believe that any location requirements should stem only from customer choice as opposed to regulation. Data location requirements disrupt the free flow of data and have an impact on both local and global industry, which rely on international data value chains, as well as on the GDP growth of the country adopting it.

Finally, data location policies prevent the emergence of a true Digital Single Market. The presumption should always be to allow data transfers within Europe, between Europe and the rest of the global digital economy. Minimal exceptions should only be allowed subject to stringent assessment, in full respect of the basic principles of necessity, proportionality, non-discrimination and subsidiarity – and in line with the exemptions of Art 14 of World Trade Organisation (WTO) General Agreement on Trade in Services.

Security

There are important security challenges in the IoT space, given that the number and range of new connections opens new vectors for attack, that operation technology and information technology are two different realms with different skill sets that are finding themselves converging and that multiple new vendors with limited experience in dealing with network and information security are inevitably entering the market. Nevertheless, from a legislative and policy standpoint, it is important to focus on the use case and risk, not the technology architecture.

The draft Network and Information Security (NIS) Directive is in the late stages of the policy-making process, likely to be adopted in before the summer. It includes the requirement to undertake technical and organisational measures to safeguard security, reporting of security incidents to the competent authority and oversight by such institution. The sectors covered by the NIS Directive are those generally deemed to be critical infrastructure: energy, transport, banking, finance, health and water supply.

Though not generally seen as critical in and of themselves, digital service providers will also be covered. The definition of network and information services will include IoT networks within these sectors. Targeting critical use cases has the advantage of avoiding unnecessary and costly regulation for services that do not require it and distract focus of competent authorities overseeing the services.

The advent of the IoT is also accelerating the need for cyber security in industrial control systems. The complexity of IoT will mean that cyber security must be designed into the components that make up the automation system.

The adoption of industrial security standards with certification will be essential to the advancement of IoT because it will ensure the security not just of individual assets but also of the larger systems and systems of systems. These certifications will play a role similar to those which occur in the realm of safety certifications. Adherence to the certification means that the elements of a system hold the key security building blocks. The elements are combined in a secure way by security certified teams and are operated as a secure system by security trained operators.

The key to security certification is consistency and applicability. As such, we do not see the need for additional regulation for IoT security above and beyond the existing framework.

Liability

Liability risks discussed in the framework of IoT are not new or specific to IoT. While such technologies create interdependencies between multiple product developers, service providers and users of the data, that is also true for other types of technology and services with complex supply and value chains. In this respect, the existing legal framework is fit to address liability issues in the field of IoT and we see no need for new liability rules for data driven services and connected products, especially not in the B2B area.

The Product Liability Directive (85/374/EC) imposes liability for damages caused by defective products on the producer. While its applicability to technologies that operate as often as not as a service than individual products might need clarification, this is not a new issue and should be addressable under the existing framework.

However, in specific situations using completely autonomous systems, adapted or dedicated liability rules could be required. We therefore suggest an in depth analysis of the existing rules to specific use cases so to determine if the existing legal framework is fit for purpose or if new rules or tools are required to address liability challenges.

The General Data Protection Regulation will also have an impact on the liability of IoT services and products as it relates to the processing of personal data. Moreover, aside statutory requirements, contractual liability provisions play an important role in resolving liability issues. Any policy initiative in this domain should remain risk-based, flexible and future-proof.

Research and Innovation

DIGITALEUROPE highly appreciates the IoT Large-Scale Pilots in the H2020 Work Programme 2016-2017 to ensure the take up of IoT in Europe and to enable the emergence of IoT ecosystems and urges the European Commission to include similar actions at an even larger scale in the Work Programme for 2018-2020.

Furthermore, DIGITALEUROPE welcomes the emergence of AIOTI (Alliance for Internet of Things Innovation) as an industry-driven stakeholder platform for IoT. The overall goal of the establishment of AIOTI is the creation of a dynamic European IoT ecosystem to unleash the potential of the IoT. It will assist the European Commission in the preparation of future IoT research as well as innovation and standardization policies. It is also going to play an essential role in the designing of IoT Large Scale Pilots in the remainder of H2020.

Digital Skills

The single largest obstacle to harnessing the power of digital technologies and its transformation potential is a shortage of skills, particularly digital technology experts, where the shortfall is currently estimated at just over 700,000. Digital skills are essential to ensure that both business and individuals can take full advantage of the Internet of Things and its potential for job creation.

The development of an Internet of Things solution requires the combination of several ICT skills. The companies that decide to embark into the IoT are looking for new types of skills, for instance in the areas of Digital Security, Business Networks, Big Data Analytics, Internet of Things, Mobile Technologies, Cloud Computing, Business Change Management, InMemory Database, Integrated Product Service, Smart Grid Technologies or Novel Interfaces. Other trends that will disrupt the economy will include 3D printing, advanced robotics, artificial intelligence or virtual reality. The specific skills in these areas include, among others, product and network security, data privacy and security expertise, data analytics, data scientists, big data engineering, data management, design skills (platform design, user interface) or app development.

We need to continue raising awareness of the importance of digital and digital jobs. We recommend that the European Commission launch a survey on specific skills requirements across Europe with a focus on digital technologies to make sure that supply meet demand, as the digital skills in demand are constantly evolving. Digital skills training programmes are also of utmost importance. Industry has been working closely with schools, universities, employment agencies and NGOs to set up innovative programmes to supply people with key skills necessary for the digital transformation.

Dedicated Massive Online Courses (MOOCs) on IoT developed by business and available publicly can be used by teachers at schools and employers. Member States should keep reforming curiculla and work with Industry to develop specific IT curiculla at all levels of school, which is already the case when it comes to the cooperation between business and Universities to establish IoT or Industry 4.0 curiculla.

International Dimension

The world is in the midst of a dramatic transformation from isolated systems to Internet-enabled devices that can network and communicate with each other and the cloud. The IoT is rapidly becoming reality, driven by the convergence of increasingly connected devices.

The IoT is pushing manufacturing and automation industries to new levels of service and process integration, driven by ICT technologies. The emergence of a sustainable IoT requires close collaboration between the various stakeholders in the ecosystem and seamless interoperability between their systems.

Trade agreements should recognize that voluntary, industry-led globally-relevant standards are a key enabler of ICT interoperability. These standards should also be given full consideration by any global or regional standards-setting fora focusing on the Internet of Things.

Wearables

Wearables refer to clothes we wear and objects we carry (such as bags, watches, glasses, jewellery…) which embed devices (cameras for visual recognition and recording, microphones for speech recognition and recording, screens for virtual reality) and sensors to extend their functionalities.

Some products already on the market are in the domains of:

- wearable cameras
- smart clothing
- smart glasses
- healthcare & wellness
- sports and activity trackers
- wearable 3D motion trackers and
- smartphone-compatible watches

Wearables allow to be more efficient, have better knowledge and consciousness of oneself, interact remotely, learn differently, experiment and play in virtual realities and imagined worlds, create new experiences, etc.

Smart Cities

A smart city is an intelligent ecosystem combining its people (inhabitants, elected representatives, administration, companies), infrastructures, operations and processes in the benefit of its citizens. All components of such an ecosystem aim at working in an interconnected and integrated fashion to utilise resources efficiently. In the context of increasing population density due to migration from rural areas and raising demography, smart cities are to meet the demands of their rapidly growing and urbanizing population. This effort spans from the renovation/modernization of existing cities to the construction of new municipalities and urbanization of rural centres that develop into cities.

Key areas for smart cities include built environment, economic development, energy, health and human services, payments, public safety and security, telecommunications, transportation, waste management, water and wastewater.

The smartness of the city will rely on the integration of data. Therefore, an open, integrated digital platform is needed. This platform includes:

1. capturing of data, static as well as real-time data, delivered by connected devices (personal of via infrastructure)
2. data identification and storage (cloud and/or local)
3. data analysis and integration
4. data visualisation and decision making tools

Integration of data means that data from different domains are linked in an intelligent way, in order to make smart decisions. E.g. Electrification of transport means data links between energy and mobility.

Smart Building/Home Automation

The "Internet of Things" (IoT) and in a broader sense Machine-to-Machine (M2M) communications has in Smart Building/Home Automation one of its major applications area such as:

- Heating, Ventilation and Air Conditioning (HVAC)
- Shutters, terrace awnings, blinds and curtains, electrical door locks, electrical windows, garage door and gate openers, lighting control etc.
- Security, fire and anti-intruding surveillance systems
- Home automation additional functions like automatic plant watering, pet feeding etc.
- Energy management & saving with/without connection to third party service management or utility provider (the latter would also interface to Smart Metering/Grid systems)

Smart mobility

Smart mobility has several applications:

- Provide feature functionalities (navigation, traffic management, stolen vehicle recovery, autonomous driving and parking…)
- Maintain and improve services
- Address vehicle safety concerns
- Diagnose and assist with technical issues
- Respond when the system senses the vehicle has been involved in an accident, and
- Fulfil requests for service by customers.

In the area of intelligent transport, it is to be noted that current industry efforts are resulting in speedy development in ETSI ITS as well as 3GPP level of DSRC/LTE V2V and V2X technologies (LTE Releases 13 and 14), paving the way for 5G.

Smart environment and energy (smart grids/water/circular economy)

IoT supported systems and devices have a high potential to enhance energy, water and resource efficiency. Smart grids can help manage energy demand on the grid and better manage peak demand, helping to reduce the pressure on energy infrastructure. IoT enabled devices can help us monitor water flow and quality more effectively, detect leaks more rapidly and support the management of drought and flood conditions.

Smart devices can also help to support the delivery of a circular economy by allowing manufacturers to better anticipate when products are likely to fail and are in need of repair, allowing for spare parts to be delivered ahead of failure or to initiate remote software repair, which in turn can support new resource efficient business models and drive innovation. Smart environment and energy have also high potential in areas where constrained resources and fragile environments make populations vulnerable. This could lead to the improvement of:

- Energy efficiency and improved grid management
- Water efficiency and improved flood/drought responsiveness. Clean water delivery (register and monitor data on water usage and flow rates, water quality, ensure secured and reliable delivery infrastructures).
- On and off-grid electricity (monitor and distribute electricity produced/captured/stored based on consumption monitoring, monitor remotely appliances and devices to reduce consumption especially at peak hours…)
- Manage natural resources
- More repair of products and reduced material consumption
- Reduced carbon emissions
- Enhanced sanitation and hygiene
- New business models and innovation

Smart manufacturing

Smart manufacturing allows flexible reaction to market changes and a more personalised and diversified product portfolio. Its objectives are:

- Make manufacturing more efficient across the complete product lifecycle,
- Reduce time-to-market, improve quality of products, and increase productivity through using advances in simulation, visualisation and analytics in digital design, rapid prototyping and manufacturing engineering,
- Make production more sustainable in terms of resources, materials and energy,
- Stimulate common manufacturing platforms and ecosystems, and
- Create “virtual” value chains independently from the geographical location of its actors while producing closer to where the goods are sold

Smart farming

The applications of IoT to farming are to:

- Optimise, protect and increase production,
- Mitigate risks (pollution, weather conditions, climate change),
- Protect natural resources (pollination, nature, plants, animals),
- Trace and label food produced,
- Improve storage and distribution of food, and
- Predict agricultural yields/shocks.

This can be done by having a better knowledge of the environment (weather monitoring) and animals (individual tracked), controlling irrigation, monitoring soil (moisture, pH levels, carbon, nitrogen, potassium, calcium, and magnesium), etc.

Healthcare and wellbeing

The IoT has the potential to improve health and wellbeing of humans and animals:

- Diagnose, monitor and manage (medical) conditions,
- Monitor vaccines, pharmaceutical drugs and therapies,
- Provide preventative care (monitor and track health data and physical activities to promote healthier lifestyles),
- support independent living,
- Track and contain diseases, and
- Predict outbreak spreads.

Retail

Smart Retail introduces ways to understand customer movement, interests, behaviours, intentions and their shopping profile and to offer more personalized services to offer relevant products at the right time, the right place for the right event (if meaningful). Augmented reality, interactive screens, intelligent lighting, “smart” surveys conducted on a mobile device can improve shopping experiences. Intelligent lighting could be used for fitting rooms changing lighting based on the garment you are trying on or when at a shop browsing through their catalogue the physical product you are interested in will be illuminated. By blending on-line and in-store services the customers can experience products in real and still have access to large categories and delivery services.

Smart Retail in addition to multi-channel retailing maximise sales opportunities and optimise the retail supply chain management.

Public safety

Public safety networks provide mission critical communication solutions for police, fire and rescue departments, emergency medical services, and other critical government services. These type of services have specific communication requirements; their network must be highly reliable and secure. This has fostered the development and deployment of specific public safety communication solutions – also called Radiocommunication for Public Protection and Disaster Relief (PPDR), typically in exclusively reserved spectrum.

The main challenge is to switch from traditional narrow band systems currently in place which serve well the need for voice communications to networks ready to complement existing voice services with mobile broadband connectivity to offer both, mission critical voice and data services.

Now is the time to prepare for this change and facilitate the modernization of national safety networks. The EU should play an active role in promoting a shift towards modern European LTE based public safety networks in a harmonised and coordinated manner.

LIST OF USED ABBREVIATIONS

3D	Three dimensions
3GPP	Third Generation Partnership Project
5G	Fifth generation of communications system
AIoT	Alliance for Internet of Things Innovation
B2B	Business to Business
B2C	Business to Consumer
BEREC	Body of European Regulators for Electronic Communications
CEPT	European Conference of Postal and Telecommunications Administrations
DSRC	Dedicated Short Range Communication
eMTC	enhanced Machine Type Communication
ERC	European Radiocommunication Committee (now ECC – European Communications Committee)
FTTH	Fibre to the Home communications network access technology
GDP	Gross Domestic Products
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
H2020	Horizon 2020 EU research and innovation programme
HVAC	Heating, Ventilation and Air Conditioning
IAC	Internet Access Services
ICT	Information and Communication Technologies
IoT	Internet of Things
IPv6	Internet Protocol version 6
ITS	Intelligent Transport Systems
LTE	Long Term Evolution, wireless technology
M2M	Machine to Machine
MFCN	Mobile/Fixed Communications Network
MOOC	Massive Open Online Courses
NAT	Network Address Translation
NB-IOT	Narrow-Band Internet of Things
NGO	Non-Governmental Organisation
NIS	Network and Information Security
PMR	Public Mobile Radio
PPDR	Public Protection and Disaster Relief
QoS	Quality of Service
RFID	Radio Frequency IDentification tags
RLAN	Radio Local Area Network
RSPG	Radio Spectrum Policy Group
SRD	Short Range Devices
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
WBCDM	Wide-Band CDMA technology
WiFi	Wireless Local Area Network
WTO	World Trade Organisation

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: FFTI
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK