UNVER, Mehmet Bilal; VANBERG, Ayşem Diker

Conference Paper

How interoperable and standardised should IoT market be: A policy discussion from an EU-centric point of view

27th European Regional Conference of the International Telecommunications Society (ITS): "The Evolution of the North-South Telecommunications Divide: The Role for Europe", Cambridge, United Kingdom, 7th-9th September, 2016

Provided in Cooperation with:

International Telecommunications Society (ITS)

How interoperable and standardised should IoT market be: A policy discussion from an EU-centric point of view

Dr Mehmet Bilal UNVER[*]
Dr Ayşem Diker VANBERG[**]

Abstract

Internet of Things (IoT) depicts a world of networked smart objects, including cars, refrigerators, health care services, wearable devices, etc. which mark a distinctive revolution in digital world. In order for this revolution to realise a certain level of interoperability and standardisation needs to take place. European Commission's previous efforts as to achieving IoT interoperability ended up some recommendations as to industrial solutions including industrial and innovation policies as well as monitoring exercises. Notwithstanding the milestones taken so far, more collaboration and solid analytical approach is needed for a future-proof and scalable solution. This paper revisits the IoT interoperability considering the previously taken measures including ex ante measures, i.e. data portability and ex post interventions, i.e. *Microsoft* decision. Depending on and benefiting from these progresses, the prospective standardisation and interoperability efforts are suggested to be comprehensive and detailed enough. Particularly it is suggested that future IoT standards and reference frameworks need to embody the standards applicable to data portability that are expected to be adopted in near future. It is also found that as IoT settings vary significantly a comprehensive approach would respond more appropriately to differing market situations. Last but not the least, in case industrial efforts fail to find appropriate and fitting solutions, determination of technical and legal interoperability in IoT context would rather rely on the European Commission as lack of interoperability would cause significant losses in consumer welfare and innovation capacity of the EU.

Keywords: Interoperability, Internet of Things, Standardisation, European Commission, Digital Single Market, Protocol Layering.

[*] PhD Candidate, Anglia Ruskin University Law School; *e-mail address:* mehmet.unver@pgr.anglia.ac.uk.

[**] Lecturer, Anglia Ruskin University, Anglia Law School, Cambridge/UK; *e-mail address:* aysem.dikervanberg@ anglia.ac.uk.

Introduction

Internet of Things (IoT) depicts a world of networked smart objects, including cars, refrigerators, health care services, wearable devices, etc. which are distinguished through RFID chips that communicate constantly and seamlessly with each other. IoT can generate an incredibly powerful breadth of data which can then be translated into a product cloud or networked system out of which all the users' needs and demands are sorted out, optimised and managed much more effectively. Even a hyper-connected world could be realised by means of scalable IoT, however this largely depends on prevalence of interoperable IoT infrastructures, devices and applications.

While the EU policy makers strive to ensure a certain level of interoperability among the IoT platforms and services under the initiative of Digital Single Market (DSM), lack of widely established business models as well as standardisation is a serious problem testament to an emerging market. It is well argued that an emerging market is ought to be kept free to thrive on its own path to yield out innovative solutions. Notwithstanding this fact, IoT is an immature yet steadily growing market that would result in a social revolution alongside an IP-based transformation. As realisation of this revolution is dependent on recognition of common sets of interface specifications and data representation methods, interoperability and standardisation seems to play a greater role in IoT context. As reported by the experts "interoperability" is necessary to create 40% of the potential value that can be generated by the IoT in various settings, and accordingly is of the potential to unlock the potential economic impact to be created through IoT clouds (Internet Society, 2015).

At this crossroad, interoperability largely turns into a problem of standardisation within the realm of connected products and devices, which already exceeded the global population and is expected to reach 50 billion by 2020, up from 25 billion in 2015 (KPMG, 2015). Subsequently this raises two crucial questions related to the IoT: First, whether the market itself capable to ensure interoperability through its own dynamics? Secondly, how far standardisation ensures interoperability and needs to be relied upon for this purpose? This paper, aiming to find proper answers to these questions, fleshes out the IoT industry looking into the growing business models, protocol layers, regulatory steps already taken, technical and legal underpinnings of IoT ecosystem including different levels of interoperability (i.e. data portability). Elaborating on the intended level of interoperability within the European

context, this paper focuses on the possible roadmaps for an ideal an appropriate regulatory landscape including standardisation.

Whilst standardisation could theoretically be linked to a centralised market and reduced product differentiation, now it is clearer than before that IoT industry marks distinct features warranting detailed standardisation and a comprehensive approach. For the European stakeholders and citizens to reap the potential benefits of connected devices and products, an ultimate way of flexible, future-proof, scalable and self-configuring IoT schemes need to be in place on the other hand. This presumably conflict of interests might create dilemmas unless cooperation and interaction between stakeholders is put into place. This paper, paying attention to the already taken steps towards IoT interoperability tries to give clarity as to the EU level discussion on to what extent IoT platforms and services need to be interoperable.

In this discussion, ex ante measures responded, i.e. data portability and ex post interventions applied such as *Microsoft* case are exemplified and analysed for their relevance to IoT. Also standardisation efforts to date are examined with their implications towards intended level of interoperability and standardisation. Ultimately, it is suggested that previous experiences and distance covered should be taken into consideration in prospective standardisation efforts and data serialisation works. In this regard, it is emphasized that would-be standards applicable to data portability need to be translated into more comprehensive interoperability/standardisation frameworks within the context of IoT. It is also found that as IoT settings vary significantly a comprehensive approach would respond more appropriately to differing market situations. Last but not the least, in case of failure of industrial efforts it is suggested that Commission would be able to enforce standards that are defined and implemented so as to create flexible, self-configuring and future-proof roadmaps for a hyper-connected world of IoT across EU.

Internet of Things: Conceptual Framework

Internet of Things (IoT) is defined as "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (ITU-T, 2012). This term denotes a trend where a large number of embedded devices employ communication services offered by the Internet protocols. Many of these devices, often called "smart objects", are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in environment (Internet Society, 2015).

IoT enables a very broad range of applications – from more efficient agriculture, manufacturing, logistics, counterfeit detection, monitoring of people, stock, vehicles, equipment and infrastructure, to improved healthcare, retailing traffic management, product development and hydrocarbon exploration (Brown, 2015). It also enables new business models such as car and truck rental clubs, whose members can book and use vehicles parked around their neighbourhood almost on-demand; or "pay-as-you-drive" insurance based on precise driving patterns, behaviour and risk (Brown, 2015).

IoT is successor of Machine-to-Machine (M2M) applications which send and receive information through cellular systems with particular examples from infrastructural networks, e.g. energy meters, wind turbines. M2M devices use standard mobile subscriber identity modules (SIMs) for identification and authentication (GSR, 2015), and enable device owners to track temperature changes, energy consumption, traffic intensity, etc.

IoT depicts a world of networked smart objects, including cars, refrigerators, watches, health care devices, etc., which are distinguished through data sensors (e.g., RFID chips) that communicate constantly and seamlessly with each other. This concept denotes a trend whereby a large number of embedded processors and sensors employ communications services offered by the IP. Such devices, often called "smart objects", are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment (Internet Society, 2015). For instance, a digital blood glucose meter measures a patient's glucose level and warns him or her about the trends in glucose levels requiring attention, like the case when a thermostat gives some information about the daily weather and optimizes the interior air according to this. Both glucose meter and thermostat, including the data sensors to give the necessary signals to their users, could also send the relevant data to their producers/vendors insofar as they are connected through IP. Also these smart objects could be configured to send small amount of data to and receive from other objects surrounded by themselves through low frequency spectrum bands.[1]

With regard to the case of glucose metering, cloud-based health management systems could be given as an example as being implemented in Microsoft's HealthVault monitoring system or in iOS or Android medical apps. In Microsoft's case, HealthVault helps to link geographically distant individuals and machines as patients use at-home monitoring devices to

[1] For instance, a thermostat might be designed to stop working when a nearby window to which it is connected is opened. In this situation, the thermostat receives a signal from the window immediately after its opening with the help of the embedded sensors.

measure glucose levels or heart rates, then upload their data on the specific cloud (Becker, 2012). This data is then immediately made available to the patients' healthcare providers at the Cleveland Clinic, which allows them to follow patients' progress remotely as well as to later draw on more comprehensive and accurate data when meeting with the patients in person (Becker, 2012).[2]

In conjunction with the given examples, connectivity in the IoT context could be said to serve a dual purpose: First it allows information to be exchanged between the product and its operating environment, its maker, its users and other products and systems; second, connectivity enables some functions of the product to exist outside the physical device, in what is known as the *product cloud* (Porter and Heppelmann, 2014). Connectivity in the IoT context takes three forms, which can be present together (Porter and Heppelmann, 2014):

- One-to-one: An individual product connects to the user, the manufacturer, or another product through a port or other interface -for example, when a car is hooked up to diagnostic machine.
- One-to-many: A central system is continuously or intermittently connected to many products simultaneously. For example, many Tesla automobiles are connected to a single manufacturer system that monitors performance and accomplishes remote service and upgrades.
- Many-to-many: Multiple products connect to many other types of products and often also to external data sources. An array of types of farm equipment are connected to one another, and to geolocation data, to coordinate and optimise the farm system. For example, automated tillers inject nitrogen fertiliser at precise depths and intervals, and seeders follow, placing corn seeds directly in the fertilised soil.

As could be seen above, IoT systems and applications require a coherency within the complexity of proliferation, incorporating seamless connectivity combined with smooth control of embedded sensors through IP networks linked to central hubs. In this vein, information sharing and data management constitute other constituents of a successful IoT scheme. With regard to this latter issue, data gathering about the state of the things and use these data to feed services at the infrastructure layer would enable IoT systems and

[2] This cloud computing technology, referred to by some in the health technology and participatory medicine arena as a "data utility layer" allows patients and physicians to combine data from multiple sources that might otherwise be incompatible into a single source that can be accessed from any location via any Internet-connected device (Becker, 2012).

applications to bring out the intended efficiency and functionality (Uckelman, Harrison and Michahelles, 2011).

Technical underpinnings of IoT and protocol layering

Though not being fully standardised, the IoT networks reveal IP-based systems and applications connected to each other. The functionalities delivered by the IP-based networking lead to far-reaching outcomes with the help of embedded sensors, processors, software, etc. These developments were seen primitively in machine-to-machine (M2M) solutions designed to remotely monitor meters on the electrical grids, healthcare devices, cars, etc. Many of these early M2M solutions, however, were based on closed purpose-built networks and proprietary or industry-specific standards rather than on IP-based networks and Internet standards (Internet Society, 2015). Going beyond mobile connectivity, the IoT brings about a radical innovation by the virtue of advanced systems and networks incorporating microprocessors, data connectivity, information gathering and analysis. Signifying a revolution after introduction of *computer* and that of the *Internet* (Internet Society, 2015), IoT has unravelled the functionality of the IP for transmitting, converting and analysing the data gathered from the smart and connected products.

Different levels of IoT connectivity depict a multi-layered IP-based ecosystem, hosting a number of protocols, having interlinks between smart objects, user and the service provider, which sometimes extends to other service/application providers. Just like the Internet's functionality, in the IoT ecosystem are existing five layers (application, transport, network, data link, physical) governed by the relevant protocols. Each layer protocol fulfils the necessary task(s) for the layer above itself. Similarly with the Internet architecture, all layers (except the physical layer) are performing their services by using services provided by the layer below and performing actions within the layer (Oen, 2015).

For instance, for a user to be given information about the thermostat in his or her house, a user interface is necessary to be embedded in his or her smart phone (or an equivalent device) connected to the Internet. This interface, being visible to the end user (even remotely), also functions as the highest layer of the IoT ecosystem called "application layer". User interfaces enable the end-user to visualize and deploy a specific set of commands or modes of interaction with the IoT device that can potentially be replicated into another (different) application (Zingales, 2015). Underlying functionalities below the application layer are fulfilled by other layers in an order and (logical) understanding. Within this structure, IP has

proven to be scalable, supporting a range of applications, devices and underlying technologies, which is important for the innovations such as IoT (Oen, 2015).

While 4 layers (IEEE based) or 7 layers (OSI based) are acknowledged for the Internet from the beginning, these established layers are not directly translated to the IoT context. For example three main (simplified) layers are defined by the AIOTI, namely *network* layer, *IoT* layer and *application* layer incorporating sub-categories/layers.[3] Likewise, some other taxonomies expand the layers applicable to IoT. They, rather than trying to fit all of the IoT protocols on top of existing architecture models like OSI Model, classify the protocols into differentiated versions (e.g. 8 layers) to provide some level of organization.[4] There are also (mostly open source software) multi-layer frameworks built up for IoT, including those adopted by Alljoyn, IoTivity, IEEE P2413, Thread, IPSO Application Framework (PDF), OMA LightweightM2M v1.0, LightweightM2M, Weave, Telehash. The illustration below provides another good summary of the performance benefit that the relevant protocols bring to the IoT.[5]

[3] According to AIOTI's reference architecture application layer contains the communications and interface methods used in process-to-process communications, whereas IoT layer is grouped into 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. 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) (https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti).

[4] See http://www.postscapes.com/internet-of-things-protocols/.

[5] https://www.micrium.com/iot/internet-protocols/.

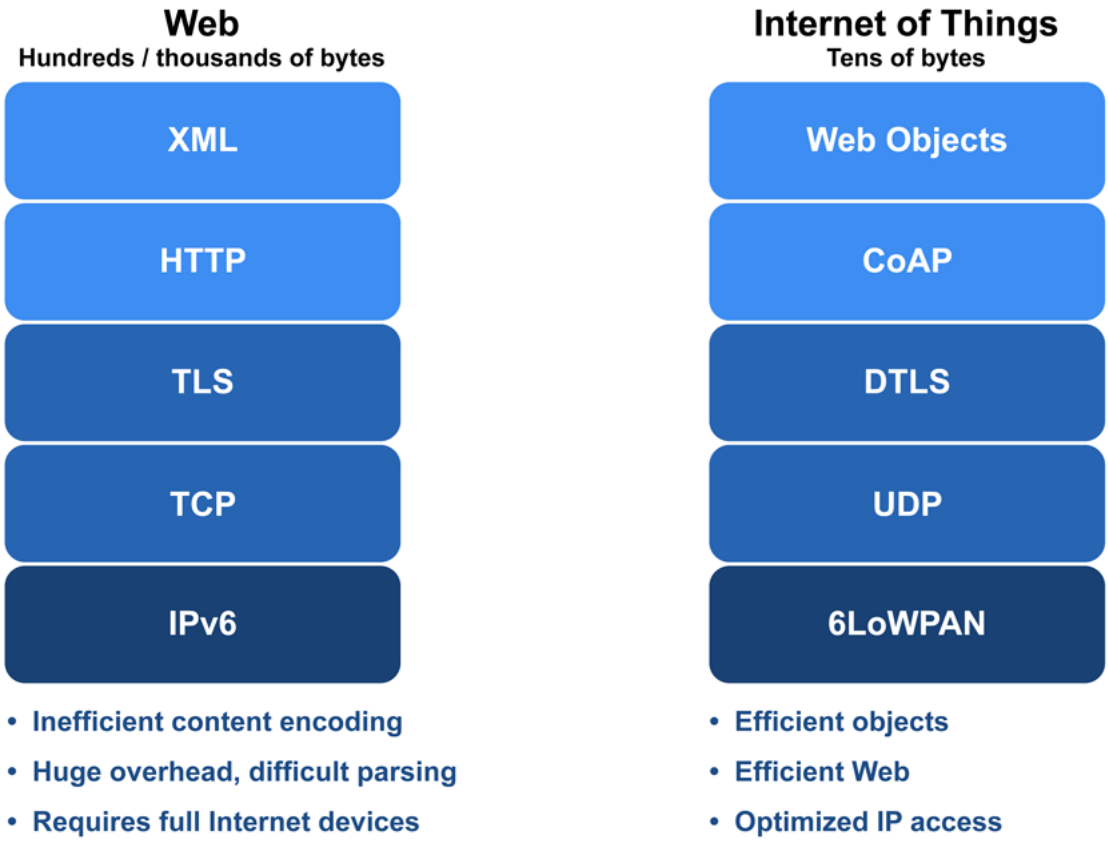

Fig-1: Comparison of Web and IoT protocol stacks

Regulatory implications in general

IoT is largely seen as a revolution rather than an evolution (e.g. from M2M) as it involves the use of IP as well as product clouds thereby targeting and embracing a wide-ranging spectrum of networks, devices and interfaces. This fact brings out some consequences. First of all, as IoT technically builds upon IP-based systems it creates a fora for revisiting *protocol layering* as described above. Secondly, IoT bears a set of political choices with regard to keeping the governing interfaces open or closed in conjunction with the goals determined as to innovation and interoperability.

IoT's revolutionary face comes with multi-dimensional functioning and technical capabilities out of combination of IP connectivity and embedded sensors. While the latter is also echoed with the M2M, the former is much more unique to IoT. Some of IoT devices may require a SIM while most of the IoT devices do not, being open to various connectivity means and technologies. Lack of standardisation for IoT also marks a big difference comparing to M2M. Both at the level of connectivity and applications, IoT requires standardisation to yield out global effects and scale economies. Notwithstanding, IoT would unleash significant

innovations and distinct developmental path as there is no pre-defined (standardized) underlying infrastructure or technology for the industrial solutions. On the other hand, the proprietary solutions developed by many IoT alliances (e.g., IETF, OneM2M) often appear incompatible with each other, and this is considered able to create switching barriers commonly referred to as lock-in problem (BEREC, 2016). These facts arouse some debates regarding how to deal with IoT in terms of regulatory treatment as detailed below.

IoT, being software-enabled, alike many OTTs,[6] converges to electronic communications in terms of the resulted benefits as well as the transmission used. IoT user (e.g., manufacturer, energy provider) becomes dependent on a connectivity service provider (or an IoT who would be in the position to offer both the IoT platform and broadband connection) for products and services, providing end-users (e.g., car owners, electricity customers) the ultimate IoT based services, devices, etc.

At this juncture, IoT service providers resemble OTT players as both involve similarities as to enabling communication and data exchange among the parties with no need to construct an electronic communications network enabling broadband connections. While this means relatively less investment and sunk costs, capex needed for IoT would increase enormously when shifting from individual level to community or society level.[7] Also IoT involves not simply VoIP type applications running over the broadband connections but also a real added value in provision of monitoring, efficiency increases, etc. reaching out big data tools and management. In fact, IoT promises an infrastructural and presumably industrial innovation rather than just a software-enabled progress. Thus, IoT systems entail a large set of networking technologies, devices and applications that allow implementers to benefit a wide-ranging opportunities, marking a stark difference from OTT type applications. Given this, IoT systems pave a new ground for the users and their (business and entertainment) needs, making them integrated with an extensive breadth of opportunities, e.g., from online monitoring to data management.

[6] OTT refers to "video, voice and other services provided over the Internet rather than solely over the provider's own managed network" (OECD, 2013).

[7] At the macro level, two of the areas of greatest IoT development and investment are *smart cities* – where infrastructure and building systems will improve the efficiency and sustainability of a whole range of urban activities – *smart power and water grids*. Closer to the individual, "connected vehicles" with hundreds of separate sensors will be safer, more reliable and able to participate in sophisticated congestion management systems. And population health and wellbeing – a challenge to governments around the world as populations grow older, with a corresponding increase in age-related chronic conditions – could be significantly enhanced with IoT-based systems used by individuals, carers, primary care doctors and hospitals (GSR, 2015).

Notwithstanding, IoT and OTTs meet each other at "net neutrality" as they both consume bandwidth. Main concern about the OTTs stem from the fact that these players are considered to create a threat in the sense that they are targeting telcos' customers just through relying on their networks with no upfront cost except for those incurred for the necessary digital inputs (e.g., search algorithms).[8] This tension, surfacing around for a decade known as 'net neutrality' has a borderline with IoT applications as these might potentially create similar implications by placing significant demand on telcos' networks. Thus it is argued that net neutrality regulations that cover business ICT services may restrict the ability of businesses to offer a range of ICT products that rely on a differentiated quality of service (KPMG, 2015).[9] Thus it is suggested that open internet rules must be applied flexibly enough to ensure a real-time, differentiated approach for applications like autonomous vehicles (KPMG, 2015).

Net neutrality represents just an area that IoT will seemingly have a touch with regulations in place. In fact, there are lots of areas, where IoT oriented regulatory treatment would be necessary, including spectrum, numbering, IP addressing, standardisation and roaming.[10] According to BEREC, in view of the Digital Single Market (DSM) review, in general, no special treatment of IoT services and/or M2M communication is necessary, except for roaming, switching (lock-in issue) and number portability (BEREC, 2016). In this regard, applicability of permanent roaming for IoT connected devices, more flexible switching solutions (i.e. assignment of MNC[11], OTA[12] provisioning), relaxation of numbering assignment are suggested by BEREC as being seen appropriate for regulatory intervention (BEREC, 2016). Except for these, the European authority does not consider that there is a further need for regulatory involvement.

At this juncture, it is clear that IoT systems and applications embrace a diverse range of regulatory and non-regulatory issues which go hand-in-hand, also creating a hurdle for future elaborations. As many issues of IoT are undergoing experimental processes, pre-emptive and precautionary policy interventions should not be responded at the first instance. From this

[8] OTTs arouse a widespread concern for revenues of telcos as applications like WhatsApp threaten the SMS revenues of mobile operators and Voice over Internet Protocol (VoIP) services like Skype or Viber threaten their voice revenues (Feasey, 2015).
[9] According to KPMG (2015), customer needs for prioritised network access will apply to ICT applications for emergency services, connected cars and smart energy meters. For instance, the use of videoconferencing for remote telemedicine consultations has the potential to reduce healthcare costs and improve patient outcomes. However, the viability of the service will be in large part dependent on the ability of service providers to guarantee network access at a certain level of quality.
[10] See GSR, 2015; Brown, 2016.
[11] Mobile network codes.
[12] Over-the-air.

point of view, the public should not turn a blind eye to the challenges raised by these new developments, because "the internet of things is not only a technological revolution but also social revolution" (Thierer, 2014).

IoT based policy initiatives in EU

As existing telecommunications laws and regulations were designed mainly with a view to deal with the voice and subsequently Internet access services, IoT is not embodied by the legacy rules. On the other hand, evolution of IoT is hard to be evaluated independent of the existing regulatory environment which might need to be revisited in accordance with the emerging requirements as mentioned above. In the way just described, in 2012 the European Commission has conducted a public consultation, aiming to seek answers to whether or to what extent IoT platform and services need to be regulated.

IoT Expert Group identified areas to develop policies including data protection and security, user identification and privacy, architectures, ethics, standards and governance, ending up three regulatory approaches identified as follows:

- "No change" with respect to the current regulatory system, implying that the EU should not intervene in the IoT market, allowing the market to evolve on its own.
- "Soft law" to provide guidance by using non-legislative measures, including monitoring of IoT development, supporting research and innovation in areas with high socio-economic impact, and the participation in standardisation bodies as well as active support to industry.
- "Hard law" to enforce regulatory measures by legislation, addressing the relevant concerns raised in the context of IoT including data privacy and security, whereas the extent of regulatory measures is considered to vary depending on the industrial sector (SMART, 2013)

This consultation exercise found a diversity of views on whether IoT-specific regulation is necessary or not. Industry respondents emphasized that state intervention would be unwise in this still immature sector, considering general rules as sufficient. Privacy advocacy groups and academics responded that IoT-specific regulation is needed to build public confidence, as well as to ensure a competitive market (European Commission 2013). Meanwhile, an FTC staff report suggested that IoT-specific legislation would be premature. It instead encouraged self-regulatory programs for IoT industry sectors to improve privacy and security practices,

while also reiterating the FTC's previous call for "strong, flexible and technology-neutral federal legislation" to strengthen its ability to enforce wider data security standards and require consumer notification following a security breach and for broad-based privacy legislation (Brown, 2015).

European Commission encourages industrial efforts within the context of IoT, giving weight to soft law instruments under the promulgated objectives of interoperable, standardised and competitive marketplace.[13] The Commission specified more concretely the scope of these measures, ranging from innovation, industrial policies to monitoring exercises. Along the same lines, in March 2015, the European Commission launched the Alliance for Internet of Things Innovation (AIOTI), which is an open stakeholder platform encompassing all actors who have a stake in the IoT value chain. AIOTI's workgroup (WG3) focused on standardisation recommends the use of standard-based solutions for the deployment of IoT in future projects. The complexity and interdependence of IoT standards is illustrated by the interoperability "plugtests" that are performed by the ETSI for key IETF protocols for the IoT developed on IEEE technologies.

Soon after in May 2015 Commission proposed in the Digital Single Market (DSM) Strategy to launch an integrated standardisation plan to identify and define key priorities for standardisation with a focus on the technologies and domains that are deemed to be critical to the DSM.[14] A public consultation to gather views on priorities for standards closed in January 2016 and results are expected to be published soon. European standards in a number of areas including IoT could be expected to be promoted so as to increase the opportunities to deliver interoperable products and services to a global audience using economies of scale for the different elements (sensors, chips, platforms, etc.) across the supply chain.

To sum up, in parallel to the procedures used in the global arena such as under ETSI, ITU, etc., efforts of dynamic groups who represent the industry have so far and for the predictable future seems to given the defining role to develop most effective solutions for future world of IoT in EU.

Interoperability in field of IoT

[13] https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation.

[14] In this context, the objective is defined as avoiding fragmentation between national initiatives in Europe, allowing cross-fertilisation between different application domains, and making sure that the regulatory framework supports seamless up-take across borders. In due course the European Commission also looked for inputs on standards in the IoT and related areas such as 5G communications, Cloud computing, Intelligent Transport Systems (ITS), Smart Cities and efficient energy use.

As acknowledged by BEREC (2016), IoT industry is currently driven more by proprietary standards than by open standards. Proprietary systems, whilst drawing the innovation paths based on governing interfaces, essential patents, etc., have also the potential of hindering "interoperability" within the IoT ecosystem that grows on the basis of protocol layers. Interoperability, reflecting the "ability of a system or a product to work with other systems or products without special effort [on the part of the customers and competitors]" (IEEE, 2016) has broader impacts and implications for IoT systems and networks.

From *political point of view*, interoperability represents one of the pillars emphasized by the Commission in different policy documents. Commission highlights the importance of leading developments in field of IoT, drawing attention to the key priorities for standardisation, cross-fertilisation between different application domains. Having a concern about fragmentation of the European market, Commission identifies lack of interoperability as one of the major three challenges against the IoT development (European Commission, 2016). With respect to interoperability policy design, a model of play-and-plug systems based on scalable and seamless up-take across borders is aimed by the policy makers in EU.

From *regulatory point of view*, interoperability also emerges as a concern for the market players as well as the regulators. This mainly stems from the "network effects" that could turn IoT-based capital and brand loyalty into a threat for competitors through customer lock-in. For products with network effects (the purchase of a product increases its value to existing purchasers), greater sales volumes can increase the likelihood of consumers being locked into existing suppliers – especially if the supplier uses non-standard interfaces and sells complementary services (Brown, 2015). This point is also highlighted by BEREC (2016) even though it is acknowledged that adoption of proprietary standards might have a positive effect for the investments and R&D. On the other hand, it should be noted that EU Commission is so sensitive in building up interoperable, scalable and open access industrial solutions, which could be seen in establishment of AIOTI for this purpose.

Achieving interoperability has always been a competition policy tool for the EU authorities, by means of whether ex ante or ex post measures followed so far. Commission's intervention in *Microsoft*[15] case demonstrates this fact. *Microsoft* case originated from Sun's (currently Oracle's) complaint that Microsoft had been leveraging its dominant position in client PC

[15] See Commission Decision of 24.03.2004 relating to a proceeding under Article 82 of the EC Treaty, Case COMP/C-3/37.792 Microsoft ("Commission's *Microsoft* decision").

Operating System (OS) market to work group server OS market by refusing to supply the interface information (a set of full specifications ensuring interoperability between Windows OS servers and non-Microsoft work group servers). Commission reached to the finding that Microsoft's refusal constituted an abuse of dominance and imposed a fine of 479 million Euros for infringement of Article 102 (ex-82).

In *Microsoft* case, Commission required Microsoft to disclose interface information (specifications) that would allow non-Microsoft work group servers to interoperate with Windows PCs and servers. In so doing, Commission considered that none of other alternative tools was substitutable with the interoperability information in order to compete viably in the market.[16] Commission's fears surrounded the ubiquity of Windows client PCs and harmful effects of an extended market power via the "network effects" by hindered interoperability. In justifying mandated disclosure, Commission seems to have regarded the proprietary specifications embedded into the Microsoft servers as *de facto standards*, being unsatisfied with either open software standards or decompilation right that can be exploited within the meaning of Directive 2009/24/EC (Software Directive).[17]

Interoperability concerns stretch from basic software interfaces to operating system extensions allowing further applications to run on the same platform. To achieve interoperability, firms must have access to and be able to use the precise information that defines the boundaries between ICT systems, that is, the interfaces between them (Samuelson, 2009). While this central tenet is unchanged for the ICT industries, unlocking interoperability information is not clear-cut or simple in each case. For the multi-layered IoT structure, open and accessible APIs are necessary for the third parties to achieve interoperability in case underlying protocols and the data formats are not disclosed with this purpose.[18]

As a matter of fact, IoT interoperability is an issue which directly relates to emergence of the IoT market like the computer industry in late 1980s or early 1990s. In the same way that

[16] Commission in its comparative analysis referred to three categories of technical tools (the use of open industry standards supported in Windows; the distribution of client-side software on the client PC; and the reverse-engineering of Microsoft's products) which Microsoft alleged could substitute the interoperability information that Sun demanded, and concluded that none of them is a viable solution for companies willing to compete with Microsoft on the market for work group server operating systems (Commission's *Microsoft* decision, paras. 667-691).

[17] See Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, Art. 6, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF.

[18] From another perspective (focused on application layer), if a single data format is to be chosen for this purpose it should be a binary format that is fast to process and transfer (Oen, 2015).

monolithic business information systems of the past have evolved into highly networked systems that use the internet extensively, open-loop RFID applications in networked environments represent a challenge that various stakeholders from the industry are facing and partly solving (Uckelmann, Harrison & Michahelles, 2011). What's more, in IoT applications B2B applications have a significant stake in development and this requires more standardised and interoperable solutions. Indeed real economic benefits come with B2B applications.[19] Last but not the least, IoT can benefit from the latest developments and functionalities commonly referred to as Web 2.0 through provision of new intuitive user-centred and individually configurable and self-adapting smart products and services for the benefit of businesses and society (Uckelmann, Harrison & Michahelles, 2011).[20] John Deere and AGCO, for example, are beginning to connect not only farm machinery but irrigation systems and soil and nutrient sources with information on weather, crop prices and commodity futures to optimise overall farm performance (Porter and Heppelmann, 2014). This industrial trend (of connected but coherent parts) requires more flexible and integrated solutions allowing every product company to decide how to incorporate smart, connected capabilities into its products.

Achieving IoT interoperability

The required level of interoperability in IoT context might differ from one case to another. A multi-dimensional and layered interoperability in all terms and conditions represents a necessity for a successfully working IoT. This has particular relevance for the governance of the IoT where the magnitude of the consumer value will depend not only on the connection between objects (i.e., infrastructural interoperability) but also on their ability to read each other's data structures and concepts (semantic and syntactical interoperability), the possibility for consumers to export those data to yet other technological platforms (data portability), as well as the ability to transfer and render useful data across systems without incurring legal liability for accessing and processing those data (legal interoperability) (Zingales, 2015). Considering that all kinds of interoperability have a legal aspect and implication, emergence of three main levels of interoperability emerge for the IoT context:

[19] According to McKinsey report, B2B applications can create more value than pure consumer applications. While consumer applications such as fitness monitors and self-driving cars attract the most attention and can create significant value, it is estimated that B2B uses can generate nearly 70% of potential value enabled by IoT (McKinsey, 2015).

[20] In this context, the competitive boundaries of industry widen to encompass a set of related products that together meet a broader underlying need. The function of one product is optimised with other related products. For example, integrating smart, connected farm equipment such as tractors, tilters and planters can enable better overall equipment performance (- Porter, E. M. and Heppelmann, 2014).

- Technical interoperability
- Semantic and syntactical interoperability
- Data portability

Among these semantic (and syntactical) interoperability complements to technical interoperability, whereas data portability refers to both but in a rather limited fashion. In terms of terminology, technical interoperability covers infrastructure and software level interoperability, and is thus preferred to either infrastructural or software-based interoperability. Technical interoperability requires that objects be able to speak and be heard, whereas semantic interoperability requires that they speak the same language.[21] Having both kinds of interoperability may also require that objects be able to carry out commands and transmit data (Kominers, 2012). Data portability, on the other hand, seeks to enhance the power of individuals by ensuring that they have a copy of their electronic personal data and become able to transmit those data from one data holder to another. This provides greater freedom of choice for individuals when selecting service providers; enables them to switch providers; and leads to increased competition between service providers (Bapat, 2016).

While an interoperability is intended to be achieved for IoT platform and services, there should be no barrier for both technical and semantic interoperability. In other words, there should be solutions enabling mapping between different protocols where data representation and semantics are the two aspects that need to be agreed upon for an interoperable IoT (Oen, 2015).[22] Thus, interoperability can be achieved by the acknowledgement and implementation of data representation and semantics based on globally adopted protocols. Fro

[21] Not every object will need to both speak and listen. Some objects will be transmitters; they will only need to be able to speak. For example, an RFID tag embedded in a can of beans will probably not have much reason to listen to other cans of beans on the shelves. Other objects, receivers, will only need to listen. Picture a black box device monitoring a factory. It would only need to listen for signals from other devices and record them; it would not necessarily need to talk back.

[22] The following description puts forward a clear-cut explanation as to this taxonomy:

> "[I]n order for message exchange to work, the two devices that want to communicate need to agree both on the semantics and on the mechanics of the message exchange. The mechanics are documented in a Web Services Description (WSD), which is a machine-processable specification of the web service's interface, written in WSDL. This WSD defines the message formats, data types, transport protocols, and transport serialization formats that should be used between the communicating devices. It can also contain information on expected message exchange patterns. While the service description represents a contract that concerns the mechanics of interacting with a particular service, the semantics represents a contract governing the meaning and purpose of that interaction. The dividing line between these two is not necessarily definite. As more semantically rich languages are used to describe the mechanics of the interaction, more of the essential information may migrate from the informal semantics to the service description. As this transformation occurs, more of the work required to achieve successful interaction can be automated."

These two components are also enablers of data portability, which is needed for an IoT consumer to transmit his data from one provider to another. On the other hand, data portability is set out as a peculiar right within the context of General Data Protection Regulation numbered 2016/679, which mainly aims at data protection by rendering more sovereignty to consumers. While enshrined to ensure data protection, the "right to data portability" adopted by the GDPR enables more than this, with far-reaching implications regarding competition law and policy. As this right is directly related to interoperability, a prospective policy design on IoT interoperability should consider this given right.

Data portability

On 6 May 2015, the European Commission has adopted the DSM Strategy to create easy access and exercise of online activities under fair competition conditions and to give a high level of data protection to both individuals and businesses[23]. One of the initiatives for the DSM Strategy for the Europe is the General Data Protection Regulation (GDPR) including the "right to data portability". Hence the right to data portability is introduced by the European Commission in 2012 and then adopted by the European Parliament and Council in due course ending up the below provision (Article 20) in May 2016:

"*1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.*

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."

[23] European Commission, 2015.

According to the final text the right to data portability has two key elements: the right of the data subject to obtain a copy of personal data his/her data from the data controller and the right to transfer one's data from one data controller to another data controller. The given text limits the scope of the right to data portability to a great extent by adding that the controller would only transfer the data to another controller, where such a transfer is "technically feasible". The details of those electronic formats and the practicalities of how such transfers would take place need to be further clarified by the Commission in the implementing acts. Aiming to grant more protection and control to the data subjects over the data provided by them to and processed by the data controllers, this provision addresses the issue of data portability particularly from the perspective of the individual user.

Arguably, what is technically feasible for a data controller might not be technically feasible for another data controller. The scope of application of the right to data portability depends on the interpretation of this very term and without clarity as to what is meant by technically feasible, the scope of data portability is likely to be limited. Introduction of an industrial solution based on open source software or a de facto standard, which is reasonably (or none) priced could dismiss such concerns. However, against the seeming reluctance of the EU authorities to introduce such a standard gives a leeway for the market players and their conflicts of interests. Albeit with some concerns as to the technical feasibility, mandatory data portability would ultimately have the stakeholders meet and find an industry-wide interoperability standard. In case stakeholders (i.e. SSOs) could not find an appropriate solution this duty will possibly rely on the European Commission though there is no such an explicit statement in the GDPR.

The given right to data portability under GDPR undoubtedly cover IoT systems as long as any personal data is controlled throughout such systems after an automatic processing process.[24] However data portability itself is a limited a right when compared with ultimate aim of enabling interoperability between the IoT platforms and services. Data portability is ensured when exporting relevant data from central databases is ensured mutually between the stakeholders. Although a standard way would be needed so as to ensure extracting data from IoT systems, this would not create open and accessible platforms by itself. Achievement of interoperability incorporates a higher requirement (of technical and semantic interoperability

[24] As a matter of fact, this right is given to all to enable them to receive the personal data concerning him or her (i.e. personal data granted to the relevant companies with a given consent), and transmit those data to another controller in seamless way. IoT companies' transactions in many ways match this scope of the GDPR and are covered under the Article 20 of this Regulation.

based on common protocols) so that IoT devices and applications can exchange information and be replaced by each other, allowing a full-fledged consumer switching. Products, services and applications in this scenario could be able to communicate over various network layers, regardless of manufacturer or operating system. On the other hand, data portability just takes place at the level of central processing systems for a particular purpose of data exporting across different platforms.

Having a direct impact on the economic benefits and added values to be derived from IoT systems, interoperable devices and applications would unlock the real potential of IoT market. Enabling a hyper-connected industrial world, fully interoperable IoT systems would be able to create spill-over effects on further innovations and economic developments. In any way, ensuring data portability requires a certain level of interoperability being achieved among the market players (Wahyuningtyas, 2015) as IoT platforms need to understand and co-operate with each other for this purpose. Taking a further step towards full interoperability, whilst eliminating consumer lock-in and potential anti-competitive conducts, would create centralised products and dull incentives to innovate unless pre-emptive safeguards are taken.

Standardisation

Interoperability in the IoT industry is largely echoed with the standards, similarly with, even further than many other industries (e.g., health care, manufacturing and automotive). Although even in a case where two firms agree on a format or specification a standard could be mentioned theoretically, standardisation is a multi-party, cooperative and continuous (dynamic) process in an ideal manifestation. Standardisation truly takes place insofar as the stakeholders are involved in a learning, sharing and production process whereby every participant's IPRs are disclosed under fair, reasonable and non-discriminatory (FRAND) terms to create an interoperable, accessible and reasonably (or non) priced technology or product.

However, while companies might be aware of these factors and in principle willing to participate in standard-setting activities by disclosing and openly licensing their entire range of intellectual property, the tools deployed in the context of standard-setting organizations to promote that behaviour are currently limited, as they are generally focused on a small set of IP rights, or on a limited notion of interoperability (Zingales, 2015). Notwithstanding, IoT market is already witnessing a proliferation of consortia for cross-industry cooperation, some of which with the specific objective of setting standards. This is not unlike the case of cloud

computing, which has been recently defined by the European Commission as a 'jungle of standards' generating confusion for their proliferation and the lack of certainty as to which standards provide adequate levels of interoperability and security (Zingales, 2015).

Regarding the interoperability initiatives pursued by the relevant organisations (e.g. alliances, consortia and standard setting organisations) the following list gives detailed information about their founders, main focus and purposes.

Organisation	Date and type	Premium members	Main Focus	Scope and progress
Open Interconnect Consortium (OIC)	2014 Cross-industry consortium	Broadcom, Samsung, Cisco, Intel, Mediatek, Samsung, and General Electric	Open source products for device-to-device, device-to-infrastructure and device-to-cloud communication.	Developing standard specifications for interoperability across connected devices, to create a cross device/cross technology framework for secure device discovery and connectivity.
AllSeen Aliance	2013 Cross-industry consortium	LG, Sharp, Panasonic, Philips, Sony, HTC, Hayer, Arçelik, Quero, Silicon Image, Electrolux and Sears.	Peer-to-peer and open source software with the aim of facilitating discovery and communication both for hardware and software products.	Developing an open source codebase including device discovery to exchange information and configurations, user notifications, a common control panel, etc.
IoT-A	2015 SSO	EU initiative Alcatel Lucent, FhG IML, Hitachi, IBM, NEC, NXP,	Preparation of architectural reference model and a definition of an initial set of	Provision of a common structure and guidelines for dealing with core aspects of developing, using and

		SAP, Siemens, a number of universities.	key building blocks.	analysing IoT systems.
Industrial Internet Consortium (IIC)	2014 Cross-industry consortium	Intel, Cisco, IBM, General Electric and AT&T	Focusing on enterprise IoT to identify core standards and requirements for future works (but not to set standards)	Creation of reference architectures, establishing a range of innovation "test beds"
Hypercat Consortium (HC)	2014 Cross-industry consortium	One-stop shop of best practice IoT implementation through the sharing of knowledge of processes and applications		Providing and open source common protocol, a catalogue format and an API to interact with the catalogue. Recently joined IIC to integrate the work of the two bodies in solving interoperability challenges.
Thread Group	2014 Cross-industry consortium	ARM Holdings, Samsung and Nest Labs	Mesh networking protocol for low power devices around homes, using an IPv6 address (with a protocol called Low power Wireless Personal Area Networks or	Developing solutions for all industries as being exclusively focused on networking. Deployment of higher layer specifications like AllSeen and OIC.

			6LoWPAN).	
IEEE P2413	2014 Cross-industry consortium		Defining an architectural framework for IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, identification of commonalities between different IoT domains and blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy and safety.	Building on the IoT reference architectures being developed in other organisations such as ISO/IEC JTC 1 Special Working Group 5 (Internet of Things) and Working Group 7 (Sensor Networks), oneM2M, ITU-T, IETF and W3C.
OneM2M	2008 Standardisation	Founded by the cooperation of different standard organisations	Creation of distributed software layer for interworking of different machines (M2M). The objective is to standardise interfaces so that they are	

			applicable to the entire ecosystem.	
ISA 100	2005 Standardisation		Establishment of standards and related information defining procedures for implementing wireless systems in the automation and control environment with a focus on the field level.	
Apache Thrift	2007 Data serialisation framework	Facebook (founder) Part of Apache Incubator in 2008	Making reliable, high performance communication and data serialisation across languages as efficient and seamless as possible.	Code generation that is used to define and create services for several programming languages in a simple and approachable way.
Google Protocol Buffer	Data serialisation framework	Google	Definition of data structure and use generated source code to read and write the structured data to and a variety of data streams and using a variety of	Developing binary data format that is compact and enables updating the data structure while still being compatible with deployed programs using old format.

			languages.	

As could be seen above, each of the consortia has different function and target in the long run. In short IoT consortia, alliances and SSOs address different challenges pursuing different methods, including through different policies regarding intellectual property rights (IPRs) (Zingales, 2015).

Ideal manifestation of interoperability in the IoT context

Interoperability has an existential meaning for the emergent IoT services as described above. IoT has a full-fledged meaning and functionality with the multi-layered interoperability, which would have different repercussions in different cases and market structures. For instance, in *Microsoft*, interoperability was an issue relating to disclosure of interfaces governing Windows architecture, being related to the operating system that was considered as de facto standard at the time. The specifications unravelling interoperability between Windows and non-Windows software was the subject-matter of the dispute that has been solved by means of Commission's ex post intervention.

When coming to the IoT interoperability, there are lots of sub markets, i.e. from home automation to smart cars. Providers in these relevant markets are manufacturers who could be deemed as IoT users, whereas the IoT service itself is being offered by the software companies who could be qualified as IoT service providers (BEREC, 2016). While the IoT service providers mostly come out of either software or hardware vendors like IBM, Intel, Alcatel Lucent, Cisco, IoT users have a big diversity according to the industry in question, i.e., Tesla (smart cars), Philips (lightbulbs), Medtronic (glucose meters).

Most of the IoT users, namely manufacturers and producers see a market advantage to creating a proprietary ecosystem of compatible IT products, sometimes called "walled gardens", which limit interoperability to only those devices and components within the brand product life (Internet Society, 2015). While this might result in customers' being locked into a particular device ecosystem and increase the switching costs for customers, for a premature market like IoT, these considerations would not be directly considered as a threat for the market competition. By contrast, innovation and entrepreneurship would be deemed as being fertilised on this ground. Hereby the crucial question arises as to whether IoT-based products

constitute a separate market or be included within the existing product market. In other words, does “competition for the market” or “competition in the market” take place in this context?

Answering this question relates to the product differentiation. For instance wrist bands or tech shirts would create separate markets for the potential customers who would prefer such products towards particular aims, i.e. following up the calories burned or the distance covered, movement intensity, heart rate. On the other hand, some other IoT products such as smart TVs target competing with the conventional products (i.e. LCD TVs) that are manufactured through quite the same methods yet with less advanced features (e.g. no user interaction on internet). On the other hand, these IoT products bring out innovative features and sometimes radical changes to business models as well as daily lives of the people. In simplest forms this could either be seen in some vegetables being ordered from the grocery through the RFID tags embedded into the house baskets or in the glucose meters used to calculate the level of glucose in people’s bloods. However more tangible values like efficiency gains and reduced costs in production cycles could arise out of IoT based innovations particularly in B2B forms. Even emergence of new business models could be affiliated to IoT. The manufacturer, through access to product data and the ability to anticipate, reduce, and repair failures, has an unprecedented ability to affect product performance and optimise services (Porter and Heppelmann, 2014). This opens up a spectrum of new business models for capturing value, from a version of the traditional ownership model where the customer benefits from the new service efficiencies to the product-as-a-service model in which the manufacturer retains ownership and takes full responsibility for the costs of product operation and service in return for an ongoing charge (Porter and Heppelmann, 2014).

From this juncture point of view, we would rather make a distinction according to whether the IoT-based products constitute separate markets or not. This might be compelling in terms of the interoperability discourse. If the smart and connected (IoT) products make a result of market creation, relevant platform and services would be under a relatively more scrutiny in terms of influences on the potential competition. In a separate IoT-based market both mergers and antitrust decisions would be made according to the features of relevant products, namely as to whether they constitute a dominance in the relevant market. While this could be generalised for all kinds of IoT products, other products that just *compete in the market* would use IoT-based features to make a product differentiation and attract more consumer via smart meters, IP connectivity, real-time data flows, etc.

In case of *competition for the market*, interoperability would have a more determinant role in business models. In such situations, lack of interoperability would result in a more fragmented and heterogeneous market structure, having more influential and sometimes irrevocable results. In these markets where closed systems are prevalent, customers purchase the entire smart, connected product systems from a single manufacturer (Harvard, 2014). Entry into those markets, where access is given to chosen parties and interfaces are retained in walled gardens, would be far more difficult as value chains of the production cycles are inaccessible to outsiders.[25]

An open system, by contrast, enables the end customer to assemble the parts of the solution – both the products involved and the platform that ties the system together from different companies (Harvard, 2014). Here, the interfaces enabling access to each part of the system are open or standardised, allowing outside players to create new applications (Porter and Heppelmann, 2014).[26] Closed systems create competitive advantage by allowing a company to control and optimise the design of all parts of the system relative to one another.[27] The company maintains control over technology and data as well as the direction of development of the product and the product cloud. Producers of system components are restricted from accessing a closed system or are required to license the right to integrate their products into it. A closed approach may result in one manufacturer's system becoming the de facto industry standard, enabling this company to capture the maximum value (Porter and Heppelmann, 2014).

A de facto standard prevailing in the industry reminds *Microsoft* case where the intervention was based on the reasoning of same characteristic features of the Windows operating system. A similarly designed intervention could only be possible after a maturity has taken place in IoT markets. In other words, for an IoT brand or an underlying technology to become de facto standard, the relevant product should have penetrated into the market with a scale economy arising from network effects. Not only such an entrenched market power but also new

[25] The operating data that GE gathers from its aircraft engines, for example, is available only to the airlines operating the engines (Porter and Heppelmann, 2014).
[26] When Philips Lighting introduced the hue smart, connected lightbulb, for example, it included a basic smartphone application that allowed users to control the colour and intensity of individual bulbs (Harvard, 2014).
[27] If either Philips Healthcare or GE Healthcare were the dominant manufacturer of medical imaging equipment, for example, it could drive a closed approach in which it could sell medical imaging management systems that included only its own or partners' equipment to hospitals. Philips also published the APIs which led independent software developers to quickly release dozens of applications that extended the utility of hue bulbs, boosting sales (Harvard, 2014).

entrants' opportunities being constrained by the IoT product in question would cause some problems in effect.

In the particular method Commission conducted its scrutiny concerning Microsoft's denying disclosure of its interfaces, Microsoft's refusal is found as *limit[ing] the prospect for such competitors to successfully market their innovation and […] discouraging them from developing new products*[28]and therefore *limit[ing] technical development to the prejudice of consumers*.[29] In fact, Commission's analytical approach that emanates with establishing eliminatory risks on competitive structure and focuses on their indirect effects towards future innovations as well as on restriction of consumer choices reveals a threshold for intervention. This threshold could be considered as a rather low one comparing to those set out in the precedents of the Court of Justice (i.e., *Magill, IMS Health* where prevention of a new product is sought for antitrust conviction).[30] Notably, *Microsoft* formulation overriding the former case-law seems to have been thought for network-based software industries where indirect network effects pose not only entry barriers but also difficulties for finding evidence for establishing abuse(s).

Within its scrutiny which attributes a crucial role to 'industry-wide incentives to innovate', Commission adopted a new *incentives balancing test* for proving lack of objective justification (on part of the refusing dominant firm). According to the Commission, "a detailed examination of the scope of the disclosure at stake leads to the conclusion that, on balance, *the possible negative impact of an order to supply on Microsoft's incentives to innovate is outweighed by its positive impact on the level of innovation of the whole industry (including Microsoft)*. As such, the need to protect Microsoft's incentives to innovate cannot constitute an objective justification so as to offset the exceptional circumstances identified".[31]

From this point of view, two main results arise out of the Commission's attitude. First of all, lack of interoperability lays out a ground for a relatively easier intervention and less lenient

[28] Commission's *Microsoft* decision, para. 694.

[29] Commission's *Microsoft* decision, paras. 693-701.

[30] Commission seems to be satisfied in case disclosure of interoperability information that were formerly refused by Microsoft would bring out advanced features to be attached to the existing products of competitors:

> "[I]f Microsoft's competitors had access to the interoperability information that Microsoft refuses to supply, they could use the disclosures to make the *advanced features* of their own products available in the framework of the web of interoperability relationships that underpin the Windows domain architecture" (Commission's *Microsoft* decision, para. 695).

[31] Commission's *Microsoft* decision, para. 783.

approach when compared with lack of access to or interconnection with a leading network like in *Oscar Bronner*[32] case where a newspaper distribution network is denied of access. Second, the Commission signals that in case the industry does not find itself a path of follow-on innovation establishment of a de facto standard in the marketplace suffices to intervene to the market where there is no or insufficient interoperability. This second issue relates to and is justified with the introduction of *new balancing test* via which the Commission builds up a semi ex ante formula that would reflect on regulatory policies.

Given the Commission's priorities under the Digital Single Market initiative, the intended levels of efficiency, enhanced business opportunities and increased consumer welfare also support the view of more interoperable, connected and coherent EU market. In this vein, interoperability needs require a certain level of standardisation for the market players to have a cross compatibility between devices, infrastructures and clouds and customise their products accordingly. A significant number of alliances, SSOs and consortia pay effort to create IoT standards, reference frameworks and database codes. Commission's efforts as to standardisation through AIOTI is noteworthy here.[33] However whether and to what extent these efforts will be successful bringing out a dynamic and competitive IoT environment remains to be seen as many of said ventures have different aims in effect.

Data portability, on the other hand, denotes another legal and technical means to ensure interoperability. The right to data portability introduced by the GDPR, whilst envisaging a limited right for the end-users, could be considered as a leverage to facilitate interoperability as well as market access, customer switching across players and consumer sovereignty. This

---

[32] Case C-7/97 *Oscar Bronner GmBH & Co KG v Mediaprint* [1998] ECR I- 7791 ('*Oscar Bronner* judgment'). In the seminal case of *Oscar Bronner*, the Court of Justice clarified its position as regards a new competitor's access to an essential facility. Oscar Bronner was the publisher of a small daily newspaper, which accounted for 3.6 per cent of the Austrian daily newspaper market and was enjoying steady growth in new subscriptions and advertisement revenues. On the other hand, Mediaprint was the publisher of two newspapers which together enjoyed 46.8 per cent market share in the Austrian daily newspaper market. Bronner sought access to Mediaprint's established delivery scheme. When Mediaprint refused this, Bronner filed a complaint before Austrian courts seeking an order requiring it to grant access to Mediaprint's delivery scheme for a reasonable payment. The national court referred preliminary questions to the CJU. The CJU held that provided that Mediaprint was found to have a dominant position in the nationwide delivery schemes market, its refusal could amount to an abuse if it satisfied the following criteria cumulatively :

i) First, refusal was likely to eliminate all competition in the daily newspaper market;

ii) Second, the service must be indispensable for carrying on the entrant's business, in that there is no actual or potential substitutes for such delivery;

iii) Third, the refusal must not be objectively justified. (*Oscar Bronner* judgment, para. 41*)*

[33] AIOTI ecosystem is designed to build on the work of the IoT Research Cluster (IERC) and spill over innovation across industries and business sectors of IoT transforming ideas into solutions and business models. The Alliance will also assist the European Commission in the preparation of future IoT research as well as innovation and standardisation policies (See https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti).

right granted for end-users would create an environment whereby customers could easily switch from one IoT service provider to another, and prevent network effects from being an entry barrier in the end. From this point of view, the right to data portability would offer a demand-side effect over the potential anti-competitive threats to an extent.[34] While this effect could be uncertain or limited for saturated/mature markets like social networking, advent of far more opportunities (i.e. creation of a pro-competitive and dynamic market) would take place in the emerging IoT markets.

For consumers to reap from these opportunities a certain standardisation is also needed in the context of data portability. As detailed above, this is a requirement as IoT market players need to send relevant information pertaining to their subscribers (to enable customer switching), and for this purpose a set of interoperability interfaces owned by IoT service providers are needed to be opened to their competitors. In this context, the governing interfaces of IoT platforms would ensure IoT companies to have an "export-import module" through which, portability of personal data across different IoT platforms is ensured. Such a standard (ensuring data portability) relates to internal management processing and results in an overhaul in such processing systems. In fact, this standard could not be thought and designed independently from other software interfaces of the same company. Thus, if a long-term approach is to be followed for interoperability policy design, then a macro standardisation would rather be preferred incorporating data portability interfaces.

Commission's policy suggestions promulgated at the end of 2012 public consultation might be considered target-based for a comprehensive standardisation scheme as it covers long-term soft law measures including innovation and industrial policy tools as well as monitoring exercises. These measures would go a long way towards promoting comprehensive standardisation, providing a minimum baseline upon which companies could expand their cooperation into further collaboration based on patent pools-like mechanisms (Zingales, 2015). It would be ideal and effective when cooperation between stakeholders brings out macro standards as incompatibility would emerge between the small-scale standards should standardisation of each constituent part of IoT systems take place separately.

In accomplishing afore-mentioned objectives, not only soft law measures but also a detailed reference framework is needed as implied above. In doing so, a requirement arises as to

[34] This new right would increase manoeuvrability and transition capabilities of customers offsetting the demand-side scale economies associated with network effects (See Yoo, 2012).

investigating how to integrate data portability interfaces into the IoT ecosystem in an effective and forward-looking manner. Such an integration would rather ensure flexibility, self-configurability and integrity between the constituent parts of the IoT hardware and software. *Microsoft* could be exemplified as both server-to-server and server-to-client interoperability was the subject-matter of the Commission's decision as to disclosure of interface specifications. On this ground, a more comprehensive interoperability scheme would rather be pursued in similar settings including IoT based environments. In this regard, interoperability necessary to ensure data portability needs to be examined in the sense that to what extent the standards applicable in that context could be harmonised with the broader view of IoT standardisation schemes.

Ultimately saying, promotion of large-scale standards would increase the opportunities to deliver interoperable products and services to a global audience using direct and indirect network effects for the different elements (sensors, chips, platforms, etc.) across the supply chain. For these supply chains to be effective and cross-fertilised, flexible, self-configurable and fully (backward-forward) compatible architectures need to be designed based on multi-layered interoperability. In the end, a more determinant role might rely on Commission through its standardisation power (i.e. in case of failed attempts in the industry) going beyond ensuring dialogue and interaction between stakeholders as expected under AIOTI.

Conclusion

The combination of IP connectivity, prevalence of sensors embedded into the devices and sophisticated data analysis techniques nearly for a decade enable IoT applications become a reality in home interiors, public spaces, various industries, etc. For these implementations to turn into a hyper-connected world and bring out long-term and effective results in real economic terms, interoperability emerges as an inevitable need to take place in IoT markets. To emphasize, accessing real-time information through ICT means in a plug-and-play mode as suggested by the EU's IoT paradigm calls for open, scalable, secure and standardised infrastructures.

Hence IoT standardisation emerges as a key issue for IoT interoperability, making a distinction from other ICT systems that depend on a particularised form of software and hardware interoperability. *Microsoft* could be exemplified as this case was related to interface information regarding access to Windows architecture to enable non Windows servers to compatibly work with Windows servers and clients. However in IoT context, a multi-layered

interoperability including technical and semantic understanding based on common protocols need to be predefined for ensuring the intended level of device-to-device, device-to-infrastructure and device-to-software interoperability. It should be noted that as IoT settings vary significantly a comprehensive approach would respond more appropriately to differing market situations.

All IoT-based requirements would then be expected to be reflected on the standardisation efforts based on a flexible system architecture. Ideally, open, accessible and future-proof IoT platforms would promise the intended level of interoperability. In such an environment, the underlying systems and technologies would be adaptable to various industries, rendering ability to map different protocols and hardware-software combinations. For such a prospect to realise, EU policy makers should go beyond enabling data portability, and integrate this measure with further technical and legal steps. Thus, preparation of detailed reference frameworks as well as promotion of large-scale standards represent the requirements in the near future for a hyper-connected world of IoT. Last but not the least, in case the industry stakeholders fail to arrive comprehensive and effective solutions, the European Commission would be in the position to intervene in view of previous experiences including *Microsoft* case.

REFERENCES

- Bapat, A., 2013. The new right to data portability, 13(3), *P & DP*, pp. 2-7. [online] Available at: <http://www.pdpjournals.com/images/stories/back_issues/privacy-data-protection-16-6.pdf> [Accessed 1 September 2016].
- Becker, M. W., 2012. Interoperability Case Study: Cloud Computing, Research Publication No.2012-11, The Berkman Center for Internet & Society at Harvard University. [online] Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046987> [Accessed 1 September 2016].
- BEREC, 2016, Report Enabling the Internet of Things, BoR (16) 39. [online] Available at: <http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things> [Accessed 1 September 2016].
- Brown, I., 2016. Things to Regulate, *InterMEDIA*, January 2016, 43(4), pp. 39-44.
- Brown, I. 2015. GSR15 discussion paper, Regulations and the Internet of Thing (IoT), [online] Available at: <http://www.itu.int/en/ITU-D/Conferences/GSR/Pages/GSR2015/GSR15-discussion-paper.aspx> [Accessed 1 September 2016].
- European Commission, 2016, Staff Working Document; Advancing the Internet of Things in Europe. [online] Available at: <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe> [Accessed 1 September 2016].
- European Commission, 2015, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions COM(2015) 192, [online] Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN> [Accessed 1 September 2016].
- European Commission, 2013, Conclusions of the Internet of Things public consultation [online] Available at: <https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation> [Accessed 1 September 2016].

- European Commission, 2004. Commission Decision of 24.03.2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft) (Commission's *Microsoft* decision). [online] Available at: <http://ec.europa.eu/competition/antitrust/cases/dec_docs/37792/37792_4177_1.pdf> [Accessed 1 September 2016].
- Feasey, R., Confusion, denial and anger: The response of the telecommunications industry to the challenge of the Internet, *Telecommunications Policy*, 39, 2015, p. 444-449.
- Gasser, U., 2015. Interoperability in the digital ecosystem, [online] Available at: <http://www.itu.int/en/ITU-D/Conferences/GSR/Pages/GSR2015/GSR15-discussion-paper.aspx> [Accessed 1 September 2016].
- Internet Society, 2015. Rose, K., Eldridge, S. & Chapin, L., (eds.) The Internet of Things: An Overview, [online] Available at: <http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf> [Accessed 1 September 2016].
- ITU, 2012. Overview of Internet of Things, [online] Available at: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060> [Accessed 1 September 2016].
- Kominers, P., 2012. Research Publication No. 2012-10 April 2012, Interoperability Case Study Internet of Things (IoT), Berkman Center for Internet and Society at Harvard University.
- KMPG, 2015, Securing the benefits of industry digitisation, A Report for Vodafone, [online] Available at: <https://www.vodafone.com/content/dam/vodafone-images/public-policy/policy-papers-and-news/Vodafone-Industry-Digitalisation-Report-051115.pdf> [Accessed 1 September 2016].
- OECD, 2013. Communications Outlook 2013, OECD Publishing, 2013, [online] Available at: <http://www.oecd-ilibrary.org/science-and-technology/oecd-communications-outlook-2013_comms_outlook-2013-en> [Accessed 1 September 2016].
- Oen, H. M., 2015. Interoperability at the Application Layer in the Internet of Things (MSc Thesis), Norwegian University of Science and Technology.
- Porter, E. M. and Heppelmann, J. E., 2014. How Smart, Connected Products Are Transforming Competition, *Harvard Business Review*, pp. 65-88. [online] Available at: <https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition> [Accessed 1 September 2016].

- Schindler, H. R., Cave, J., Robinson, N., Horvath, V., Hackett, P., Gunashekar, S. Botterman, M., Forge, S. and Graux H., Europe's policy options for a dynamic and trustworthy development of the Internet of Things), SMART 2012/0053, http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR356/RAND_RR356.pdf.
- The Institute of Electrical and Electronics Engineers (IEEE), 2016, Standards Glossary. [online] Available at: <https://www.ieee.org/education_careers/education/standards/standards_glossary.html> [Accessed 1 September 2016].
- Thierer, A. D., 2014. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation, *Richmond Journal of Law & Technology*, 21(2), pp. 1-118.
- Uckelman, Harrison and Michahelles, 2011. In: (eds.) D. Uckelman et al ed. 2011, *Architecting the Internet of Things*, DOI 10.1007/978-3-642-19157-2_1, Springer-Verlag Berlin Heidelberg.
- Yoo, C. S., 2012, When Antitrust Met Facebook, *George Mason Law Review*, 19(5), pp. 1147-1162.
- Wahyuningtyas, S. Y., 2015. Interoperability for data portability between social networking sites (SNS): the interplay between EC software copyright and competition law, *Queen Mary Journal of Intellectual Property*, 5(1) pp. 46-67.
- Zingales, N., 2015. Of Coffee Pods, Videogames, and Missed Interoperability: Reflections for EU Governance of the Internet of Things, *TILEC Discussion Paper* (DP 2015-026). [online] Available at: <http://ssrn.com/abstract=2707570> [Accessed 1 September 2016].