AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

AIOTI Digitisation of Industry Policy Recommendations

November 2016

Table of Contents

Executive Summary

The goal of the Alliance for Internet of Things Innovation (AIOTI) is the creation of a dynamic European IoT ecosystem to unleash the potential of IoT. AIOTI Working Group 4 ('WG4') is the AIOTI policy working group. The scope of WG4's work is to identify existing or potential barriers that prevent the take-up of the IoT in the context of the Digital Single Market, and to make policy recommendations on topics relevant to the creation of a Digital Single Market for IoT.

The AIOTI firmly believes that the Internet of Things (IoT) has an important role to play in furthering the Digitisation of Industry, in the interests of end-users, which is an important part of the European Commission's Digital Single Market strategy.

In this document, the AIOTI reviews and makes a number of recommendations relevant to a number of Digitisation of Industry policy measures that are particular relevant to IoT[1], namely the creation of an IoT Trust Label, IoT numbering and addressing, the 'free flow of IoT Data' and IoT liability. Wherever possible, the AIOTI includes evidence from vertical industry sectors in order to inform further discussion on these topics.

The AIOTI recommendations are as follows:

- In relation to **IoT numbering and addressing** we recommend incorporation of ITU supranational numbers within the EU regulatory framework for electronic communications. We also make a recommendation to expedite roll-out of IPv6 for IoT.

- In relation to the emerging idea of an **IoT Trust label**, we assess a number of options and outline a potential industry led IoT Trust Charter for IoT.

- In relation to the **free flow of IoT data**, we strongly support legislative measures to remove any barriers to the free geographic movement of data across the EU. In relation to data ownership, we are in favour of relying on existing horizontal law and regulation to address any issues that arise in this emerging area.

- In respect of **IoT liability**, we set out an updated analysis of the potential concerns in this area, and recommend a 'wait and see' approach on this topic, with key industry and government stakeholders maintaining an open policy dialogue.

This policy document follows up the AIOTI's previous policy document of October 2015[2], in which the AIOTI made a number of policy recommendations in relation to Privacy, Security, Liability and Net Neutrality.

[1] In particular, see the measures outlined in the Staff Working Document: Advancing the Internet of Things in Europe accompanying the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market COM(2016) 180, available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15276

[2] See http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11815

1 - Introduction

1.1 IoT is already starting to have a significant positive impact on the European economy. With the correct policy approach, it can truly transform how enterprises large and small function and do business, to the benefit of European businesses and consumers alike.

1.2 In order for these benefits to be realised, stakeholders must also ensure that any concerns associated with IoT are addressed. IoT enabled objects may have the capability to communicate, store data, process data, exchange data, make decisions and execute such decisions. Although the exact functionality of the IoT enabled object will vary depending on the circumstances of each use-case, this type of capability may raise a number of policy considerations in the fields of privacy, security and liability.

1.3 In this document the AIOTI has considered what may, initially, seem like a disparate set of topics. However, they are all connected by three key themes.

- The first theme is that of **trust**. It is vital that IoT develops in a way that is ensures trust. Those involved in the IoT ecosystem have every incentive to ensure this is the case. This topic was much discussed within the AIOTI and the importance of creating a trusted environment for IoT features in all of topics considered by AIOTI WG4 in this document. The AIOTI's proposals should represent a pragmatic approach in this area. We welcome the views of civil society representatives on the considerations that have been set out in this document.

- The second theme is **technological neutrality**. The market context set out in this document, which particularly informs the AIOTI's recommendations on numbering and addressing, demonstrates the variety of technological means that are being used to deploy IoT devices. In the IoT environment, it is important that policy does not unduly favour, or disadvantage, one technological option over the other, and the AIOTI's recommendations on this topic should be seen in this context. Over time, these technologies are likely to coalesce. Standards will obviously have an important role to play here, as exemplified by the work of the AIOTI standardisation group (AIOTI Working Group 3).

- The third theme is the importance of, wherever possible, a **horizontal approach to law and regulation**. This, after all, is one of the key themes underpinning the AIOTI's activity, recognising that IoT represents a true convergence between technology (in whatever form) and industry. The AIOTI Policy Group has endeavoured to focus on topics which have an impact across the IoT supply chain. We may not always think that new horizontal regulation would be warranted, and our analysis of potential regulatory intervention in the area of IoT data ownership is an example of that. However, policymakers should still strive for a horizontal approach wherever possible, and measures to facilitate free flow of IoT data across the EU is a great example of where such a policy approach would be welcomed. AIOTI WG4 also advocates a focus on enforcement of existing horizontal law and regulation, as opposed to introducing new regulation specifically with IoT in mind, as our analysis of the situation in respect of IoT liability demonstrates.

1.4 The policy dialogue in this area will undoubtedly continue. This is something the AIOTI welcomes. We hope that the views set out in this document will help to inform the debate.

2 – Numbering and Addressing for IoT

Purpose of this section

2.1 This document sets out different technical numbering and addressing options relevant to IoT, in order to inform the ongoing policy discussion on this topic. WG4 considers it important to have a high level summary of these different technical options as, to date, much of the policy debate in this area has been focused on the use of telephone numbers for IoT applications.

2.2 While the document discusses communication specific identifiers it doesn't address identifiers in general and their use for the identification of the Things in IoT. Policy discussion around this topic should also take into account wider technical considerations (see 2.5 below).

2.3 A key issue that has been raised in relation to the use of telephone numbers for IoT applications is what happens when telephone numbers allocated to a telecoms provider in one Member State are then used by an IoT customer in second Member State. This consideration has informed discussion of a potential European IoT numbering scheme and also proposals in the new European Electronic Communications Code regarding use of telephone numbers for IoT, which highlight the importance of a technologically neutral approach in this area.[3]

2.4 The key theme underpinning this section is that any policy must be cognizant of these different technology options and should not unduly favour, or disadvantage, one technology over another.

2.5 It should be noted that the AIOTI Standardisation Working Group (WG3) is carrying out further work in the area of IoT Numbering, Addressing and Identifiers for Things which will become part of the AIOTI WG03 High Level architecture. That activity is outside the scope of this paper but is central to the ongoing work of the AIOTI in this area.

Contents

2.6 This section is set out in the following parts:

- terms used in this section;
- four different technical numbering and addressing options for IoT, as well as their existing administration;
- policy issues related to IoT numbering and addressing for IoT, and
- policy recommendations to support continued IoT take-up across the EU.

[3] For example, see blog post of Roberto Viola, Director General of DG Connect at https://ec.europa.eu/digital-single-market/en/blog/machine-machine-connectivity-digital-single-market, report of the Body of European Regulators of Electronic Communications (BEREC) at http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things and the European Commission's review of the regulatory framework for Electronic Communications at https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code

TERMS USED IN THIS SECTION

2.7 The following terms are used in this document:

- **Numbering -** this refers to the International Telecommunications Union's (ITU-T) numbering and addressing systems which underpin international telecommunication. An example of the way that ITU-T has shaped the telecommunication networks of today is the numbering Recommendation ITU-T E.164. This recommendation provides the structure and functionality for telephone numbers.[4] A number of IoT devices still use E.164 numbers, although the end-user (where there is one) will not be aware of this number so it serves a very different purpose to a 'traditional' telephone number.

- **Addressing** - addresses are bound to a specific network technology and location in a network. An example of an address is an Internet Protocol address (IP address) which is a numerical label assigned to each device (e.g., computer) participating in a network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

- **Identifiers** - A label (numeric, alphanumeric, or other) that is used within a specific context to uniquely identify an entity.

2.8 It should be noted that the numbering systems referred to in this section function as network or device interface addresses, their primary role is to ensure that data traffic is delivers to a specific device interface or routed towards other networks. While these numeric or symbolic addresses sometimes can be helpful in ex-post attribution of actions, data flows or messages, they are not identifiers and WG4 strongly advises against using them for identification or authentication.

2.9 Address and number assignment is a function of the particular communication technology and network layer. A network layer protocol like IP uses addresses that reflect the network topology in order to provide distributed routing. Assignment can be static or dynamic (i.e. DHCP) within the address range of the IP service provider. Phone numbers are assigned by the communication service provider and IEEE identifiers are usually assigned by the manufacturer of the communication interface. Changes in network configuration, nomadic use, change of service provider, change of communication interfaces and technologies or parts replacements could all trigger a change of the address, making it unsuitable for use as an identifier by any other layer than the network or transport layer that assigns and manages them.

[4] For more information on the ITU's role in this area please see https://www.itu.int/en/ITU-T/studygroups/2013-2016/02/Documents/Numbering%20naming%20and%20addressing%20leaflet.pdf

DIFFERENT NUMBERING AND ADDRESSING OPTIONS FOR IoT

(A) IP addresses

Administration of IP addresses[5]

2.10 All networks located in the EU fall within the RIPE NCC service region and can apply to the RIPE NCC for IP addresses. RIPE NCC is an independent, not-for-profit membership organisation that supports the infrastructure of the Internet through technical coordination in their service region. RIPE NCC's most prominent activity is to act as the Regional Internet Registry (RIR) providing global Internet resources and related services (IPv4, IPv6 and AS Number resources) to members in its service region.

2.11 The Internet Assigned Numbers Authority (IANA) operates the global registry for IPv6 and IPv4 addresses according to policies adopted by the communities of the RIRs through an open, inclusive and bottom-up policy development process. IANA distributes blocks of IPv6 and IPv4 addresses to the five RIRs and consequently delegates to RIRs the authority to further distribute more specific IP address blocks according to policies developed by each RIR community.

2.12 RIRs operate in large, geopolitical regions that are continental in scope. Currently, there are five RIRs:

- ▪ AFRINIC Serving Africa Founded in 2005
- APNIC Serving the Asia Pacific region Founded in 1993
- ARIN Serving North America Founded in 1997
- LACNIC Serving South America and the Caribbean Founded in 2001
- RIPE NCC Serving Europe, Central Asia and the Middle East Founded in 1992

2.13 The duties of an RIR include the distribution of IP address blocks to legal entities according to policies set by each RIR community through an open, inclusive and bottom-up policy development process. The RIRs also registers information about the distributed IP addresses and their associated legal entities in publicly available databases they maintain for this purpose. The RIRs and their communities work closely together to develop consistent policies and promote best current practice for the Internet.

IP case study - Internet (IPv6 based): e.g. Home Automation

2.14 In the case study, the following considerations apply – as shown Figure 1 below:

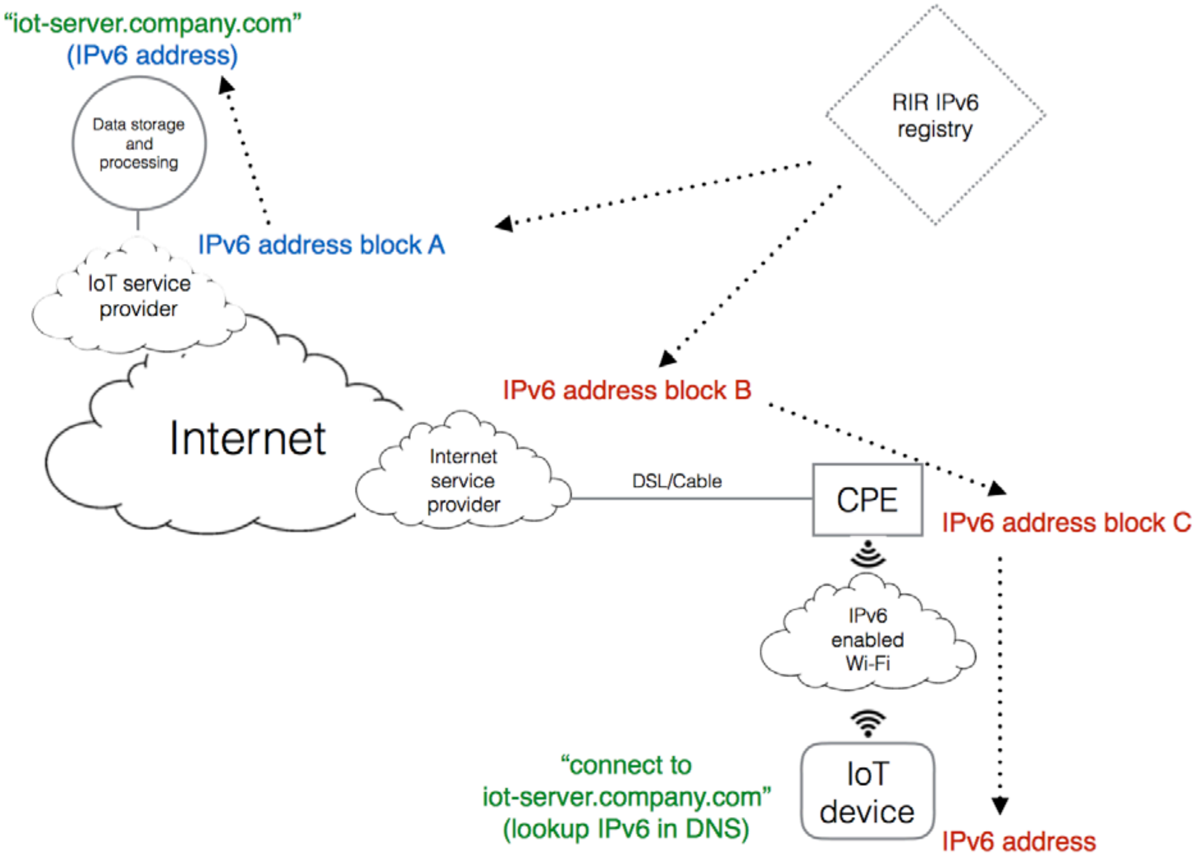
- Customer gets a Wi-Fi enabled device, which uses a IEEE address at Ethernet layer
- Connects it to his home network
- Customer Premises Equipment received an IPv6 range from the Internet service provider who provides the connection and has an RIR membership
- Somewhere on the Internet the IoT company has a connection their Internet provider,

[5] As part of its Visual Networking Index (VNI) for 2015 to 2020, Cisco has projected that globally, 48.2 percent of all fixed and mobile networked devices and connections will be IPv6-capable by 2020—up from 23.3 percent in 2015.Therefore IP addresses will represent the significant majority of IoT connections. Cisco also forecasts that globally, 34 percent of total Internet traffic will be IPv6 driven by 2020 and that IPv6 traffic will grow 16-fold from 2015 to 2020, a CAGR of 74 percent. Cisco has observed that advancements in the IoT are continuing to drive IP traffic and tangible growth in the market

who has his own IPv6 address range (also an RIR member)

- The device is programmed to connect to a symbolic name which is mapped to an IPv6 address using the DNS
- Change of service provider will cause an address change, DNS mapping will compensate for that as long as the domain name is not changed.

Figure 1 – IP address home automation case study



(B) Telephone numbers[6]

Administration of telephone numbers

2.15 The ITU is the body responsible for assigning and managing E.212 resources (i.e. the allocation of Mobile Country Codes or Mobile Network Codes). The ITU also assigns 'supranational' E.212 and E.164 numbering resources for the provision of IoT applications across borders. A number of mobile operators use E.212 shared resource 901-XX, with E.164 shared resource +882-XX for cellular IoT applications.[7]

2.16 In the telecommunications sector, numbering resources are traditionally assigned and managed at national level by the relevant National Regulatory Authority (NRA). A

[6] Machina Research considers that by 2025 there will be 27 billion IoT connections, of which 2.2 billion will be supported by cellular networks. Therefore telephone numbers remain relevant for IoT connections that operate in licensed bands.

[7] For more information please see ITU-T Recommendation E.190: (1997) Amd.1 (11/2009

number of NRAs in Europe and also in other international jurisdictions have considered whether or not to introduce specific E.164 number ranges for IoT services in their respective countries. Some NRAs have introduced such a range[8], while others have not.[9]

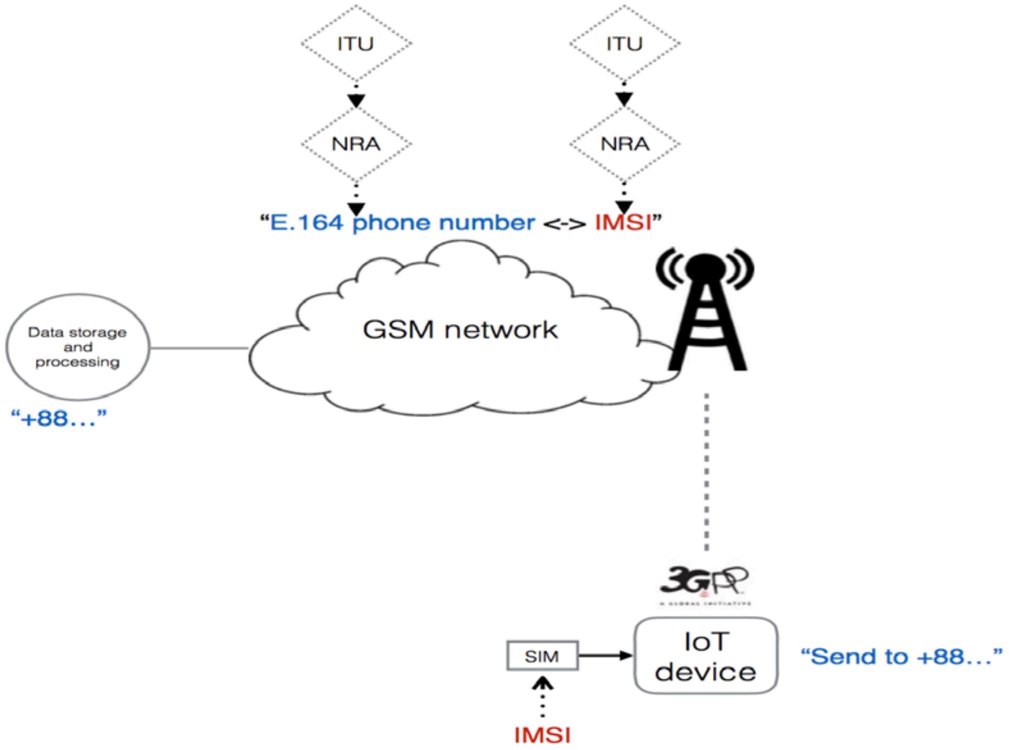
2.17 BEREC (the Body of European Regulators for Electronic Communications) has stated that the use of existing numbering resources - the extraterritorial use of numbers and the use of ITU numbers - seems to be a reasonable approach for IoT.[10]

Case study - Cellular native (E.164 based): e.g. Connected Car

2.18 In this case study, the following considerations apply, as shown in Figure 2 below.

- Customer gets a GSM enabled device
- A SIM card is inserted with an IMSI of the operator
- The IMSI internally is mapped to an E.164 number which the operator also holds (via the ITU or the national regulator)
- Device can be programmed to send data to an E.164 number which addresses a server connected to the GSM network

Figure 2 – telephone number connected car case study



(C) IEEE Extended Unique identifiers

[8] For example Belgium, Netherlands, Singapore
[9] For example Ireland, the UK
[10] See section 2.2.1 of the BEREC Feb 2016 Statement of the Internet of Things

Administration

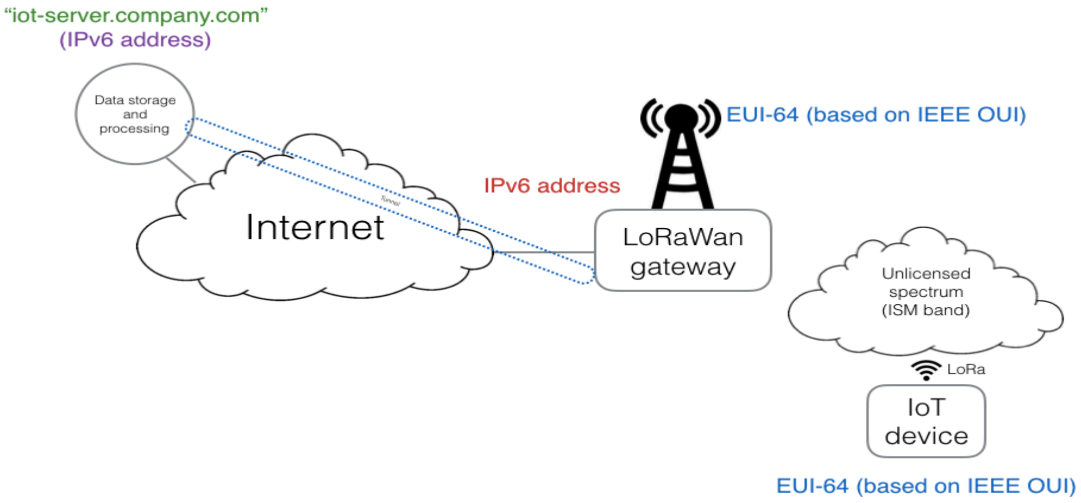
2.19 64 or 48 bit IEEE Extended Unique Identifiers (EUI-64/48) consist of an Organizationally Unique Identifier (OUI) which can be 24, 28 or 36 bit and a unique number for the remaining bits. EUIs can be used for various purposes. In this context we consider their use as addresses in communication networks (mainly at the link layer) based on IEEE standards like 802.3, 802.11, 802.15.4 and other technologies like Bluetooth, LoRaWan and Sigfox. The IEEE Standards Association operates a registration authority at which organisations can apply for an Organizationally Unique Identifier (OUI). A unique number shall be assigned by the organization that owns the OUI for the remaining part of the EUI.[11]

Case study - LoRaWAN using IEEE identifiers e.g. Smart Parking

2.20 In this case study, the following considerations apply, as shown in Figure 3 below.

- The LoRa enabled IoT device has an IEEE derived identifier, this defines both the individual unit as well as the specific application
    - The LoRaWAN gateway is connected to the Internet as any other regular device
    - The LoRaWAN gateway, receiving the signal knows, based on the first part of the IEEE identifier where to send the data
    - The processing facility is connected to the Internet as any other service would be
- The gateway sends the data across the Internet using the pre-configured destination (DNS name) of the designated processing facility
- Essentially the functions as a VPN tunnel, where the Internet just forms a transport layer for the LoRa based IoT data packet.

Figure 3 – IEEE identifier smart parking case study


"iot-server.company.com"
(IPv6 address)
Data storage and processing
Internet
Tunnel
IPv6 address
EUI-64 (based on IEEE OUI)
LoRaWan gateway
Unlicensed spectrum (ISM band)
LoRa
IoT device
EUI-64 (based on IEEE OUI)

[11] https://standards.ieee.org/develop/regauth/tut/eui.pdf

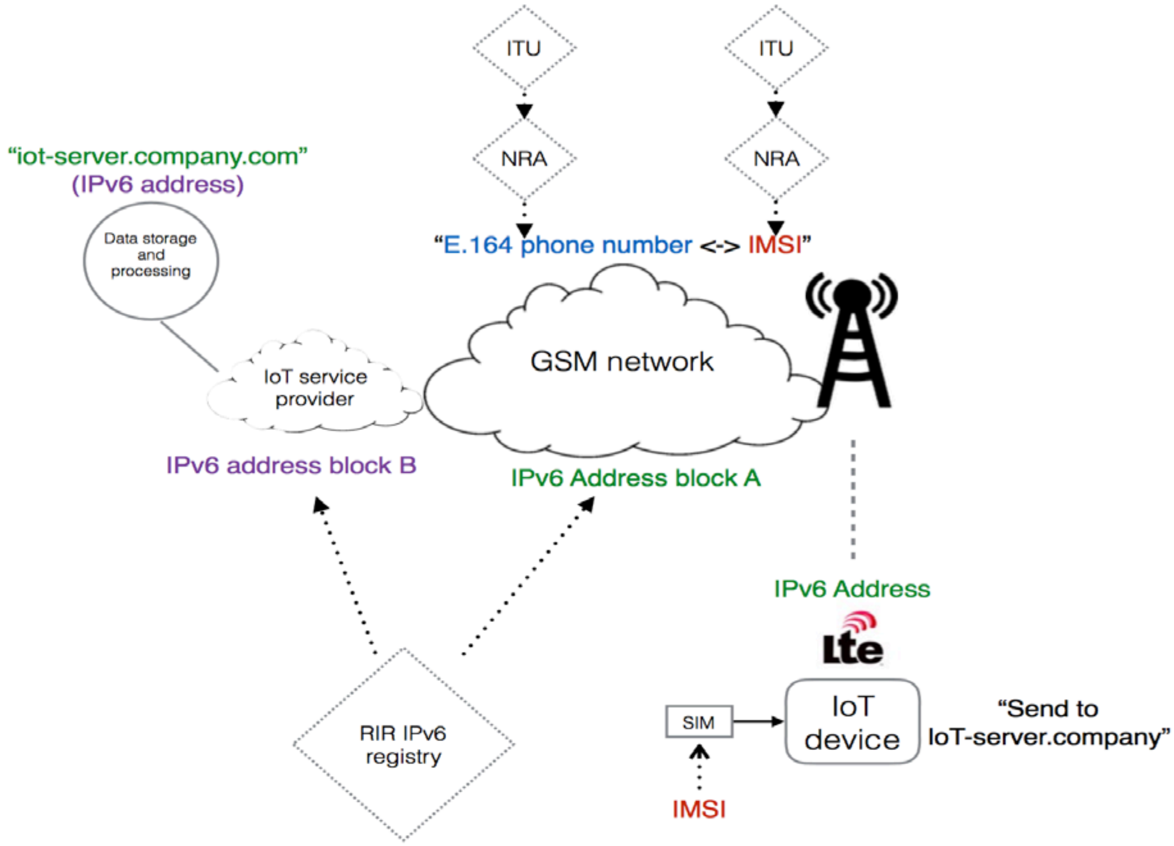
(D) ***Hybrid (IPv6 over cellular):***

2.21 In a modern network environment systems can also complement and overlap each other. In this case study, the following considerations apply, as shown in Figure 4 below.

Case study - Industrial Automation

- Customer gets a GSM enabled device
- A SIM card is inserted with an IMSI of the operator
- Upon connection the GSM network uses the IMSI to identify and authenticate after which it assigns an IPv6 address from their own IPv6 range (RIR member)
- The GSM network is connected (part of) the Internet
- The IoT service provider can be reached transporting data across the Internet using IPv6 addresses
- Device can connect to IoT service
- IoT services as well as devices can move around networks (changing IPv6 addresses or even IMSI)
- DNS maps between symbolic identifier and IPv6
- In this example the actual addressing for data communication is done using IPv6 addresses. The IMSI is only used for identification and authentication of the mobile network ‘subscriber’ (albeit that the end-user of the IMSI will be a machine).

Figure 4 – IPv6 over cellular industrial automation case study



ASSESSMENT OF POLICY ISSUES RELATED TO IoT NUMBERING AND ADDRESSING

2.22 In assessing actual or potential problems related to IoT numbering and addressing, WG4 has identified the following topics. Each of these will be assessed and this will inform WG4's view on its policy recommendations in this area, including the potential role of a European/International numbering scheme for IoT.

- Numbering/Addressing barriers to free-flow of IoT devices across the EU
- Exhaustion of numbering resources
- Pace of migration from IPv4 to IPv6
- Security implications in choosing a specific numbering and addressing technology
- Number Portability/Switching

Numbering/Addressing barriers to free-flow of IoT devices across the EU

2.23 This concern is more likely to apply to IoT applications that use E.212 or E.164 numbers, as these numbering resources are typically regulated at national level, as opposed to IP addresses, which are by definition 'international' in nature and not affiliated with a specific geographic region (or perceived to be subject to the jurisdiction of national regulatory authorities for telecommunications).

2.24 The concern here is that IoT devices may not travel freely within the EU due to, for example, regulatory measures in a Member State which may restrict the use of, supranational or non-domestic numbering resources for IoT applications. This is a particular concern given many IoT applications are inherently cross-border in nature.

2.25 BNetzA, the German NRA, has recently adopted measures to explicitly allow the extraterritorial use of foreign IMSIs in Germany and vice versa for German IMSIs abroad for M2M services. Such a policy approach is welcome. However, not all NRAs in the EU have adopted such a policy stance.[12]

2.26 Therefore WG4 considers that measures at EU level to clarify or facilitate the free-flow of IoT devices using E.212 or E.164 resources across the EU would be welcomed.

Exhaustion of numbering resources

2.27 An often raised concern is that numbering resources may be unduly depleted or even exhausted due to the very fast growth of IoT.

2.28 In relation to E.164 number resources, the Body of European Regulators for Electronic Communications (BEREC) has recently stated that "*the alleged scarcity of E.164 numbers does not seem to be a barrier or a problem to be solved to foster the development of IoT*" and that "*the issue of possible scarcity of E.164 numbering resources should be analysed and solved by NRAs at national level, e.g. introducing a new numbering range for IoT services or increasing the mobile number resources*"[13].

[12] This concern has now been addressed by the German national regulatory authority for telecommunications Bundesnetzagentur (BNetzA) – see http://www.twobirds.com/en/news/articles/2016/germany/june/german-telecommunications-regulator-enacts-new-rules-to-facilitate-m2m-communication

[13] http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

Therefore the exhaustion of E.164 number resources does not seem to be a founded concern.

2.29 With regard to IP addressing, one of the drivers in the move to IPv6 was to ensure a sufficient quantity of IP addresses and it is generally accepted that there are sufficient IPv6 addresses available compared to IPv4. BEREC has also stated that "*the IPv4 addressing structure provides an insufficient number of publicly routable addresses to provide a distinct address to every Internet device or service (however, many connected devices may be located behind one IPv4 address), in particular in view of the expected growth of the market*". BEREC has concluded therefore that "*migration to IPv6 appears to be advisable to enable the accessibility of connected devices from the public network*".

2.30 Given the expected shift towards Internet based addressing and identifier systems, which include IPv6, as well as the availability of dedicated numbering systems, there currently appears little risk that exhaustion of any of the numbering or addressing resources would present a problem.

2.31 For EUI-64/48 identifiers no exhaustion is expected in the foreseeable future.

Pace of migration from IPv4 to IPv6

2.32 The need to facilitate migration of internet applications to IPv6 has already been recognised by policymakers across the globe.[14]

2.33 The EU has previously focused in this area through the IoT6, a 3 years FP7 European research project on the future Internet of Things. This project aimed at exploring the potential of IPv6 and related standards (6LoWPAN, CORE, COAP, etc.) to overcome fragmentation of the Internet of Things. This work concluded in 2014, stating that "*IPv6 will be (and actually it is already) a key enabler for the future Internet of Things*" and that "*Adoption is just a matter of time*".

2.34 However, despite some market projections, recently BEREC has sounded a rather more cautious note on IPv6 adoption, stating that "*it is expected that IPv4 and IPv6 will exist alongside for quite some time although use of IPv6 has seen substantial growth over the last few years*"[15].

2.35 Given the time that has elapsed since the IoT6 activity concluded, it may be helpful to assess current roll-out of IPv6 deployment for IoT across the EU and whether further policy activity can be undertaken in this area to facilitate the deployment of IPv6.

2.36 Even though there will be a use of IPv4 addresses on the Internet, to ensure the IoT reaches it maximum potential, it is ever more important to ensure new networks, applications or devices are capable of and prefer the use of IPv6 over IPv4, a resource that only has a very limited availability for new market entrants.

Security

[14] See for example, https://www.google.com/intl/en/ipv6/statistics.html and the activities of http://www.ipv6forum.com/

[15] http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

2.37 In a recent report[16] by ICANN's Security and Stability Advisory Committee (SSAC) it is noted that the continued use of IPv4 in combination with address sharing which is a common method to mitigate the address space depletion harms security of the Internet and applications that use it (such as the IoT). Amongst the issues high-lighted is also the inability for Law Enforcement Authorities and digital forensics functions to correctly identify a user based on the IPv4 address. The report concludes that both device manufacturers and network operators should accelerate plans to deploy IPv6.

2.38 The primary role of the SIM card is twofold as follows:

- *Identity*: the SIM card contains a unique reference number that identifies the SIM card and therefore the subscription that accompanies that SIM card. The mobile network can recognise the reference number and ensure that associated costs incurred are allocated correctly.
- *Authentication*: in order to ensure that the identity is valid, the mobile network uses a security mechanism to allow access to the network. This is achieved by the network issuing a challenge (similar to a security question) that only that particular SIM card can answer from the information it has stored in its memory. Once validated, access to the network is granted.[17]

2.39 Given the ICANN SSAC report highlighted above, concerns about security risks stemming from the depletion of the IPv4 address pool provide further evidence of the need to expedite migration to IPv6.

Number Portability/Switching

2.40 Another consideration that flows from the use of numbering resources in the telecommunications regulatory framework is the ability to port the number as part of a switch from one connectivity provider to another.

2.41 In relation to E.212/E.164 resources, the question of number portability in an IoT context has recently been considered by BEREC which has stated that "*the number portability obligation might not be appropriate in case the E.164 number of the connected device is not known by the IoT user (and/or by the IoT end-user), which usually happens when the device is not designed to send or receive any voice calls or SMS*".[18]

2.42 The ability to switch providers (where requested by the customer) in a cellular IoT context without the need to switch SIM cards has been driven by the GSMA's remote provisioning activity, which has resulted in a single, de-facto standard mechanism for the remote provisioning and management of IoT connections, allowing the "over the air" provisioning of an initial operator subscription, and the subsequent change of subscription from one operator to another.[19] It should be noted that there is however no 'one size fits all' approach to provider switching given the multiplicity of different IoT use-cases and demand-side considerations. Irrespective, given the availability of the OTA model where required, neither number portability nor provider switching appear to be barriers to the use of IoT devices in cellular networks.

[16] https://www.icann.org/en/system/files/files/sac-079-en.pdf

[17] See https://www.gsmaintelligence.com/research/?file=81d866ecda8b80aa4642e06b877ec265&download

[18] http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

[19] http://www.gsma.com/connectedliving/embedded-sim/

2.43 As IP addresses identify a network location, the need for individual number portability is not an issue. A device or user who migrates to another network, will automatically receive an address from the new network's range appropriate to the new attachment point, where the old address becomes available for re-use in the old network. The Internet's public Domain Name System (DNS) is used to provide a mapping between the more permanent symbolic identifiers (such as hostnames) to the current IP address of the network location for a particular service, device or user.

2.44 Within the Internet technical community there is broad consensus that the use of IP address literals in applications, protocols and uniform resource locators (URLs) should be avoided at all cost, replacing these with fully qualified domain names that can be looked up using the DNS.[20]

AIOTI WG4 NUMBERING AND ADDRESSING POLICY RECOMMENDATIONS

2.45 After consideration of the actual or potential issues set out above, AIOTI WG4 has not identified a clear driver that would point towards the need for a new European or International numbering scheme for IoT. In line with the European Commission's view on sustaining an open market in which different technologies co-exist to form a single IoT eco-system, WG4 considers that it is unlikely that development of a single numbering system to support such a broad landscape would be feasible, neither on technical grounds nor on economic arguments of providing consumers and market players with a choice. In general it has to be taken into account that IoT and the use of IoT devices is not limited to national and regional boundaries. Any approach must have an international focus.

2.46 Not all of the devices and applications in the IoT landscape will use 3GPP or IETF technology. As such, AIOTI WG4 would advocate using "the right tool for the right job" and address the different numbering schemes and their feasibility in light of technical options available as well as the specific dynamics of both the connectivity market as well as specific requirements (technical requirements, public policy objectives etc).

2.47 AIOTI WG4 would however highlight the need for an expedited deployment of the IPv6 protocol in the Internet's networks, services and applications, as the IPv4 address space is no longer capable to sustain the growth of the Internet, let alone provide addresses for the vast amount of IoT devices that are expected to connect. Continued use of IPv4 will harm the Internet's model of 'permissionless innovation' and inhibits to fully enjoy the benefits of economic and societal advantages that the IoT is expected to bring.

2.48 WG4 would also highlight that it is important to ensure there are no undue regulatory barriers in existing national regulatory frameworks that could restrict use of Supranational E.212 or E.164 numbering resources, as these resources have an important role to play in ensuring the free flow of IoT devices across the EU.

2.49 In light of this, AIOTI WG4 makes the following policy recommendations:

- The European Commission should open up a new policy workstream designed to further promote and facilitate the take-up of IPv6 for IoT applications, building on the work that has previously been undertaken by IoT6.eu;

[20] https://msdn.microsoft.com/en-us/library/windows/desktop/ms740586(v=vs.85).aspx and https://tools.ietf.org/html/rfc3235 paragraph 3.1.3

- The European Commission should seek to either amend the existing telecommunications regulatory framework (in the context of the Telecommunications Framework Review) or issue a Communication to ensure there are no undue regulatory barriers to use of Supranational ITU E.212 or E.164 resources for IoT applications across the EU, and

- The European Commission and/or BEREC should develop guidelines on how to ensure that any IoT policy initiatives (for example related to use of Over the Air provisioning for cellular M2M services) are adopted consistent with the principle of technological neutrality, as envisaged by the new Electronic Communications Code[21], taking into account the different technical options for numbering and addressing as set out in this section.

[21] See for example Recital 226 and Article 87(6) of the proposed Electronic Communications Code.

3 – IoT Trust Label

Introduction

3.1 The European Commission has identified trust in IoT as a key factor in determining the speed of take up of IoT devices and services. The Commission Staff Working Paper of 19 April 2016 points to several key factors in building this trust. These include:

- Ensuring security and privacy, including providing sufficient computing capacity, secure setup and configuration, and trustworthy identification and authentication of users and devices 'in a distributed environment'
- Compliance with data protection rules regarding profiling
- Anonymization of both user and protocol metadata
- Secure and functional safe infrastructure.

3.2 The problem in the Commission's mind is how to help build this trust. It is suggested that a Trust Label, like the energy labelling scheme in the EU, might help, particularly as far as consumers are concerned. The Commission interestingly also suggest that industry led initiatives could be important.

Is there a Real Problem?

3.3 It is difficult to get an idea of the level of trust in IoT. But there are some studies which suggest that the Commission is right to be concerned.

(i) MEF

3.4 In a report published in 2016, the global mobile trade body, Mobile Ecosystem Forum surveyed over 5000 mobile users and found that:

- 60% of mobile users are worried about a world of connected devices;
- Privacy (62%) and security (54%) are seen as the biggest threats worldwide;
- Home security raises the most concern among connected devices and applications.

(ii) Accenture

3.5 A recent Accenture report claimed that 54% of digital consumers are cautious about the information they share due to lack of confidence in the online security that protects their personal data. It said that 'digital trust is at a deficit. The majority of consumers remain cautious about sharing their personal information online and, when they do, they trust established brands more than other companies. The time is now to close the gap in consumer confidence and gain their digital trust. It is simply a prerequisite for those wanting to leverage the IoT business.'

3.6 For Accenture, digital trust depends on: security, privacy, benefit/value and accountability. Customers may be willing to make benefit versus risk decisions in exchange for some perceived value and it is important that companies enable consumers to make informed decisions in a suitably transparent way. Businesses must remain accountable for any lapses in protecting consumers' digital information.

(iii) Symantec

3.7 In 2015 Symantec published a report on IoT security, and their analysis of 50 smart home devices currently available. Their conclusion reads: 'none of the devices enforced strong passwords, used mutual authentication, or protected accounts against brute-force attacks. Almost two out of ten of the mobile apps used to control the tested IoT devices did not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. The tested IoT technology also contained many common vulnerabilities. All of the potential weaknesses that could afflict IoT systems, such as authentication and traffic encryption, are already well known to the security industry, but despite this, known mitigation techniques are often neglected on these devices. IoT vendors need to do a better job on security before their devices become ubiquitous in every home, leaving millions of people at risk of cyberattacks.'[22]

3.8 Additional studies by Symantec also highlighted that personal information privacy and security definitely top European consumers' expectations when selecting suppliers of connected devices and digital services[23]. Such expectations however remain crucially underserved in areas such as self-tracking wearable devices and apps (e.g. personal sport and health monitors), with, among others, less than half of the reviewed apps having a privacy policy, many of them presenting serious risk of unintentional data leakage to multiple Internet domains, and most of them featuring weak user data segregation and poor individual session management[24].

(iv) OWASP

3.9 The Open Web Application Security Project's (OWASP) List of Top Ten Internet of Things Vulnerabilities sums up most of the concerns and attack vectors surrounding this category of devices:

- Insecure web interface
- Insufficient authentication/authorization
- Insecure network services
- Lack of transport encryption
- Privacy concerns
- Insecure cloud interface
- Insecure mobile interface
- Insufficient security configurability
- Insecure software/firmware
- Poor physical security

Is anyone looking at this?

A number of organisations are looking at this.

(i) The Online Trust Alliance (OTA)

[22] Note that the Federal Trade Commission has already taken enforcement action in this area, for example see https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

[23] Symantec State of Privacy in Europe 2015 (https://www.symantec.com/en/uk/about/news/resources/press_kits/detail.jsp?pkid=state-of-privacy)

[24] Symantec Security Response White Paper: How Safe Is Your Quantified Self? (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf)

3.10 OTA aims to provide guidance to manufacturers and developers to help reduce attack surface and vulnerabilities, and adopt responsible privacy and data stewardship practices. It also aims to drive the adoption of security, privacy & sustainability best practices; embracing "privacy and security by design", as a model for the development of voluntary, yet enforceable code of conduct.

(ii) OWASP (Open Web Application Security Project)

3.11 The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies. It has recently published its principles for IoT security: https://www.owasp.org/index.php/Principles_of_IoT_Security

(iii) The IoT Security Foundation (IoTSF)

3.12 IoTSF is a non-profit member organisation established to raise the quality of security across IoT, and has announced the formation of a number of working groups as it promotes the concept of the ***Supply Chain of Trust***.

(iv) ETSI

3.13 ETSI has had one workshop (16 June 2016) looking at some of the technical issues around IoT Security in the context of a possible IoT Trust Label.

What is the US doing?

3.14 The US Commerce Department recently held a wide-ranging consultation IoT, the results of which are awaited. There is growing Congressional interest in the issue, but no proposal (yet) for specific IoT regulation, and the Federal Trade Commission (FTC) regards IoT specific legislation as premature. The FTC has had a long interest enforcing US laws on data protection and privacy. It has identified some best practices for IoT companies, which include:

- the need to implement 'reasonable' security (including software updates, security reviews, vulnerability testing etc)
- Data Minimization (and where possible data de-identification)
- Notice and Choice: providing consumers with information and choices about certain types of data usage, especially those which could not have been assumed to be expected or consistent with the context of the original interaction.
- Careful use of data analytics. For example just because big data finds a correlation between different data, it does not mean the correlation is meaningful or ethically acceptable.

IoT Security

3.15 There is general agreement that security in an IoT world will need to be risk based. One solution is unlikely to fit all IoT applications. It is clear that security of some sort is not an option: all devices must consider the need for security in the design stages.

3.16 The question is what approach should be adopted? There seem to be three broad options:

(i) Wait and see;
(ii) Design an IoT labelling system as for energy labelling(i.e. certification scheme)[25]
(iii) Draw up some criteria for best practice in IoT security with a view to that becoming a standard of excellence.

Option One: Wait and See?

3.17 There is a case that the EU is already taking action in this area, and that therefore we should not start any new initiatives at present:

- The newly adopted EU GDPR aims to be applied horizontally, and thus will be fully relevant to the IOT space, in addition to consumer and contract laws.
- The EC is currently undertaking the review of the ePrivacy Directive, with the same goal in mind, e.g. adapt it to technology evolution and bring it in line with the GDPR.
- Compliance with NIS Directive. Risk management and breach notification should follow the NIS directive.

All the different initiatives already started must be harmonized: M 460, M 436, M487, M490, M530. Existing standards (ISO/IEC, CEN/CENELEC, ETSI) must be reused or referred when applicable. Common basic standards must be identified, regularly updated and communicated/disseminated. Existing international standards not yet included in European framework must be included via Vienna/Dresden agreement when relevant and justified.

3.18 Given this activity, there is a risk that additional principles or labels could overlap and sometimes be in conflict with legislation. It is important to have a stable legislative environment before proceeding with additional principles.

3.19 Some would argue that if individual players want to use additional assurance codes of conducts and such tools as a differentiation factor, this should be purely voluntary.

3.20 However, consumer confidence is key to accelerating pubic adoption of IoT. So it would be important for industry to demonstrate that it is addressing any specific IoT concerns.

Option Two: A Trust Label

3.21 The Commission’s energy label is a system for classifying the energy consumption of electrical products. It grades products according to defined criteria.

3.22 The arguments in favour are based on the opinion that leaving freedom to manufacturers to decide whether to incorporate security mechanisms or not in their products/devices, or how to build SW, has been shown to be ineffective.

3.23 In sectors where sensitive information (such as classified information) or critical processes are managed, security certification is a clear way to gain an objective (and verifiable) level of assurance in the underlying technology.

[25] For an example of an industry self-certification scheme for IoT, see the GSMA’s announcement of 13 September 2016 regarding the launch of IoT security self-assessment scheme at http://www.gsma.com/newsroom/blog/gsma-launches-self-assessment-security-scheme-iot-devices/. This is intended to give confidence to users that IoT services are secure, as well as enhance the reputation of service providers as trusted business partners

3.24 Some suggest that a standardized classification of security levels based on independent evaluation and certification schemes could be the baseline of an IoT security labelling, providing:

- scalable security to meet different security requirements

- a clear visibility of the security achieved by a product.

3.25 Going beyond the existing criteria (such as the Common Criteria Standards, published as ISO/IEC 15408 & 18045), it is possible to imagine 'new' criteria being agreed which would not undermine the manufacturer's flexibility and creativity. One can state Security and Privacy criteria from a functional perspective without imposing any architectural or technical specificities. And the level of assurance required can be adjusted depending on the criticality of the product. An example of this is the Common Criteria Protection Profiles for ICT products.

3.26 The problem is that IoT Security, unlike energy consumption, is not easily measured. There is a gap between the basic function for IoT security and the application requirements. In an IoT world a grading system may not be appropriate. IoT Security is created out of a variety of different elements: (a) the security of the device itself, (b) its use of encryption, (c) the handling of data once it leaves the devices (and goes to e.g. a server), (d) whether those who receive the information only do with it what consumers are comfortable with, (e) the ability of the system to be easily upgraded etc.

3.27 IoT will involve a mix of hardware, third party apps, platforms, cloud services etc. What would the label actually certify? Plus of course there would be assessment and verification issues: who would provide independent assessment and verification, and how would they do this? Given the complex interrelationships outlined above, it would be very difficult to provide any independent assessment of a product's performance in such a complex area.

3.28 In addition, the notions of Trust and Privacy in IoT are context specific and there are (probably) innumerable (and as yet unimagined) applications. Data transactions and relationships will be increasingly complex and dynamic. Any 'classical' approach - accreditation to or self-certification against set criteria/standards - will not be capable of giving the levels of meaningful assurance consumers will expect. Schema developed must be capable of addressing that complexity and dynamism (there are already notions of dynamic consent starting to appear and some good work has been done on assurance of complex critical infrastructure).

Option Three: a Trust Charter

3.29 A voluntary 'living' charter of generic best practice might be an effective way to address the identified concerns, while maintaining sufficient flexibility to adapt to an evolving IoT environment.

Such a Charter could do two things:

(i) Support compliance with the EU GDPR, NIS Directive and the use of Privacy-by-Design and Security-by-Design concepts.

(ii) Identify security issues for the IoT sector to consider such as outdated or flawed software, etc;

(iii) Outline best practices in resolving common issues.

3.30 This could build on the work started at ETSI in June 2016. It could cover provisioning and connectivity (authentication, integrity, access control, resource allocation), hardware and software security and maintenance (encompassing the spectrum from firmware to applications; vulnerability patches, software updates, security upgrades). As operational needs and practical requirements will differ in various contexts, this should come as a selection of recommended practices for everyone to implement as appropriate to their use cases rather than a prescriptive agenda.

3.31 This could be built into some kind of voluntary IoT Trust Charter and companies could declare their adherence to the best practices identified in the Charter.

An outline of a proposed IoT Trust Charter?

3.32 An outline of what we might include in an IoT Trust Charter in each of these areas is suggested below. It should be noted that further work will need to be done to consider how different practical approaches may be required depending on whether the IoT use-case is either B2C or B2B and in relation to the identification of different classes of 'sensitive data' for the purposes of data management.

(i) Data Security

- Promote end-to-end security by design in all products and services.
- Take measures to help ensure protection of data in storage and in transmission from attack or any other undue access, disclosure, loss or alteration (i.e. confidentiality, integrity, availability and authenticity)
- Promote that over the life cycle of any products and services there is regular updating of security measures, including to address emerging threats.

(ii) Data Management

- Promote transparency about what data is collected (including passive collection in smart spaces and smart cities) and do so in a way which is clear and simple for the user.
- Implement privacy enhancing techniques such as data segmentation, segregation, aggregation, pseudonymisation, tokenisation and anonymization to the extent possible.

(iii) Interoperability

- Promote products and services which help deliver flexibility and openness in service provision.
- Maintain as much as possible interoperability and openness over the life cycle of products and services
- Enable data portability through the adoption of appropriate industry standards.

3.33 Each of these sections could be underpinned by a 'technical annex'. As suggested above, in some cases the annex would point to existing initiatives. In the case of security it could use the work done under ETSI auspices.

Verification

3.34 If we proceed in this way, we would produce an industry led Charter. The issue of verification always arises in such cases. As a start we could simply provide for some sort of peer review: i.e. the body which drafted the Code would raise any questions they had about implementation with particular companies. This would be a light touch verification. If it proved inadequate we could think of other ways of providing verification.

Conclusion

3.35 The AIOTI WG4 considers that it could explore a way to reassure end-users about IoT Security and Privacy in a way which

(i) is fairly straightforward to implement so that we can start early in the hope of stimulating the market ahead of competitor geographies;

(ii) does not impose a disproportionate burden on companies;

(iii) takes advantage of the tools already available (standards, GDPR etc)

(iv) is flexible enough to cope with the evolving and dynamic nature of the IoT market place.

This suggests that the AIOTI could start by working on a form of Trust Charter, outlining what issues it should cover to build trust in IoT.

4 – Free Flow of IoT data

Introduction

4.1 IoT infrastructures, platforms, devices, applications and services have this in common: they all involve, and most of them are entirely based on and geared towards the generation, collection, transmission and processing of digital data over electronic communications networks, chiefly the Internet. Therefore any legal and operational obstacle to the movement of such digital data constitutes a potential challenge for the IoT. Some of the most crucial topics for discussion here ought to be what is commonly referred to as the geographic free flow of data and "data ownership".

4.2 The quotation marks are deliberately used here for the following reason: Throughout this paper, the concept of "data ownership" will relate to the lawful ability of an entity to hold, access, process, derive value from, and dispose of any given piece of data. However, in the strictly legal sense of the term, "ownership" may not always be a proper terminology, as some categories of data, as explained below, can technically not be subject to a proprietary right such as ownership. Having said that, for ease and convenience, and unless otherwise specified, the term "ownership" in this paper will always be meant as referring to the lawful ability described above, whatever its foundation in law and its proper legal terminology may be.

4.3 The Commission has begun work to cement the development of the Digital Single Market and tackle some of the data related challenges. The DSM strategy published in May 2015 and the more recent Communication on Digitising European Industry both espouse the benefits of data in driving innovation in products and services and new business models. The proposed Free Flow of Data Initiative which both documents allude to, aims to address issues such as data location, ownership, interoperability, portability and data usage. In this section, AIOTI WG4 endeavours to landscape these themes in the context of IoT and tries to give recommendations where possible on certain steps the Commission may take with regard to the development of regulations, best practices etc.

4.4 It is important to bear in mind that free flow and ownership are not two distinct topics, but two closely related and interlinked factors of the practical use of data: They both determine the accessibility of data, across borders on the one hand (free flow: where is the data?), and across organisations on the other (ownership: who can access the data?). These questions will now be considered.

Geographic free flow of data across the EU

4.5 The geographic Free Flow of Data Initiative will be essential to the success of the Digital Single Market strategy and is welcomed by many in the technology sector and other sectors. Data is a key enabler of the digital ecosystem and clearly provides benefits to governments, businesses and citizens. However, enhancing the free flow of data may require policy and even legislative measures to force Member States to remove unnecessary and unjustified restrictions to cross-border transfers at least within the EU Single Market. While such policies and regulatory initiatives may be delicate to articulate politically, from the economic standpoint, a large number of industry sectors in Europe such as banking and finance, energy, health, transport and retail, would greatly benefit from the easier cross-border use of digital data and could provide better and more competitive services to EU citizens as a result. In that sense, tearing down barriers to data flows would fit very well with the growth, jobs, innovation and competitiveness agenda of the Union. Getting there however will require addressing the challenges set out below.

(i) Data localisation

4.6 Any (national) legislative steps or policies that restrict where data can flow or reside may impede the further development of the digital economy and business innovation. IoT applications in particular could greatly suffer from restrictions on data flows, since constraints on cross-border mobility and transferability of data will unavoidably curtail large scale adoption and lead to counter-productive fragmentation of the market for IoT infrastructures, platforms, devices as well as applications and related services. Moreover, since IoT devices typically use the Internet Protocol to communicate, expecting IoT devices not to transfer data across borders would pretty much amount to expecting them not to communicate at all, which would defeat their very purpose and benefit.

4.7 Furthermore, strict data localisation mandates could seriously obstruct the security, resilience and business continuity of several large organisations using, offering or operating IoT solutions, many of which rely on international, and often even global information systems to conduct business. This applies among others to those businesses who serve other regions of the world from their European basis.

4.8 Also, these localisation mandates can be confusing as they differ per Member State and can have a negative impact on European and national competition as they may restrict the possibility of the provision of IoT products and services directly as well as indirectly as *inter alia*, not every IoT vendor has the ability to establish data centres in each Member State as may be required by some Member States.

4.9 It should also be borne in mind that contrary to political claims that are often heard in policy debates, data localisation does not solve any particular country's perceived privacy, cybersecurity, national security or surveillance-related challenges, because the physical location of data in itself constitutes no effective or even measurable protection from undue access, cyberattacks or other interference. Quite to the contrary, it makes the data easier to locate and target. Not to mention that data constrained into a particular territory or domain may not necessarily benefit from the protection of the state of the art security technologies and expertise available elsewhere.

4.10 At the same time, governments' political fear of "losing sovereignty over data" needs to be overcome, and in an environment where data is intrinsically mobile, this will require improving cross-border cooperation mechanisms especially in the law enforcement space. It should be well understood that the absence of practicable solutions to this challenge will assuredly hinder and delay the adoption of IoT and erode trust in new technologies in general.

4.11 Today, while the Commission appears strongly supportive of the removal or prevention of unjustified data localisation requirements, some Member States are taking or considering steps to put restrictions on where organisations can store and process data. In limited circumstances, for example on justified grounds of public safety and national security, there may be good reasons why countries implement such data restriction policies. However public safety and national security should not be used as catch-all excuses to extend restrictions across the board. In the vast majority of contexts, such approaches should be avoided.

4.12 **In light of this, AIOTI WG4 recommends that:**

- The Commission should use legislative tools to prevent unjustified data location requirements.
- In addition, the Commission should continue monitoring such developments, to conduct consultations with Member States in an effort to prevent the erection of unnecessary barriers to geographic data flows across the EU, to establish benchmarks and devise guidance on best practices and to promote a harmonised approach across Member States to uphold the Single Market principles and to ensure legal certainty for citizens and businesses.

(i) Interoperability and data portability

Interoperability

4.13 Interoperability is important to enable the complementary use and smooth functioning of diverse infrastructures, platforms, devices, applications and services in a given digital environment. Substantial work has already been done particularly in the areas of IoT Semantic Interoperability[26] and Technical Interoperability[27].

4.14 However, experience shows that top-down imposed interoperability requirements which make direct or covert technology choices (e.g. mandates for specific formats or design solutions, or requirements for specific models such as open source versus proprietary software) do not work well in practice because they curtail technological progress, reduce the incentive for innovation and sometimes even lock in security vulnerabilities that cannot be overcome without circumventing or abandoning the mandated technology.

4.15 Therefore it is advisable that flexibility with regard to interoperability should be preserved. In addition, it may have a negative impact on competition, as such requirements may prescribe (technical) conditions that may e.g. be costly for smaller IoT vendors or simply too burdensome in relation to the type of product or services and therefore may make such service or product unnecessarily expensive.

4.16 It is well understood that policy makers are keen to promote choice, competitiveness and innovation, in order to guard against market failure. However, there is no evidence that the nascent IoT sector is evolving towards such a failure, quite to the contrary. There is strong and fierce competition where vendors of different profiles, locations and specialties develop partnerships and co-operations at multiple levels, which is of a nature to foster interoperability. There is no evidence suggesting that developments in the IoT ecosystem are restricting data interoperability.

4.17 On the contrary, programmes are in existence that are driving the development of data interoperability in IoT. For example, HyperCat, a consortium of tech companies in the UK, are establishing programmes of work aimed at enabling devices to discover the

[26] AOITI WG03 IoT Semantic Interoperability Paper, http://www.aioti.org/resources/

[27] ETSI White Paper No. 3, Achieving Technical Interoperability – the ETSI Approach, http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf

data of other connected devices One project is the development of a BSI standard (PAS 212, Automatic resource discovery for the Internet of Things – Specification) which will support the exchange of data to enable IoT devices to interoperate. Therefore, until the market matures and the best of breed technological paradigms and their interoperability standards and practices emerge and consolidate, enough room should be left to the organic growth and self-regulation of the market.

4.18 For now, there is an ongoing debate whether or not there is a material gap to fill in terms of "what should be interoperable". IoT adoption being perceived as slower than desired is probably not a singular problem of interoperability. It has probably everything to do with the early reluctance, caution and practical difficulty characteristic of every shift to new technological paradigms. The same happened with the move to cloud computing over the last 10 years, or with the adoption of Internet-based communications in the decade before that.

4.19 **In light of this, AIOTI WG4 recommends that:**

- The current state and future outlooks of interoperability in the IoT domain do not warrant any regulatory intervention at this stage.

Data Portability

4.20 As for data portability, it is not an area that is unique to the IoT domain, and several legislative provisions and proposals exist which already address the matter. For instance the portability of personal data is already foreseen and regulated in the GDPR, and the portability of consumer-generated and consumer-contributed digital content is currently under discussion by the European Institutions, as well as the portability of lawfully acquired digital content protected by intellectual property rights such as copyright. These legal instruments are technology neutral and will apply within the IoT space as well as without. From the standpoint of the IoT community, the key consideration should be for vendors to embed into IoT systems and devices the ability to comply with existing regulatory requirements for portability.

4.21 Beyond those aspects, other areas that are not regulated in this way but where interoperability and, on that basis, data portability could become a relevant consideration may of course emerge as IoT use cases diversify and multiply and innovation and competition intensify. However, neither the needs of the demand side, nor the capabilities on offer on the supply side of the market have sufficiently crystallised just yet for anyone to credibly foretell where issues will arise.

4.22 For now, innovation and market forces should be left to drive the evolution of portability standards and mechanisms, bearing in mind that competing vendors will always have an inherent business interest to attract users from their competitors and will therefore of their own initiative propose often very creative mechanisms to facilitate portability for the user. Countless examples exist already in the cloud space where portability materialises in vendors offering tools and capabilities to "pull" user data from a competing provider into their own infrastructure.

4.23 Furthermore, international activities are also underway to support such market mechanisms. For instance, the International Organisation for Standardisation (ISO) is also working on international standardisation regarding data portability in the cloud computing domain (ISO 19086, which is currently in draft phase). It is recommended to assess those developments and where appropriate explore and develop best practices with regard to a minimum level of data portability.

4.24 With regard such a minimum level of data portability, of course it must be stressed once again that a one-size-fits-all approach to portability may not be desirable, since needs may be sector-specific and purpose-specific depending on the IoT application considered. Quite obviously, the portability requirements for switching electricity providers in a smart grid environment will have very little in common with those for switching consumer accounts across two or more health monitoring platforms. Just as importantly, forcing the portability of the smart-grid data into the health platform or vice-versa would be perfectly irrelevant and pointless. Similarly, portability needs will be very different depending on whether what is being "ported" is user data from one individual account to another, aggregated system data from one service provider to another, company-wide data from one platform to another, or big data from one infrastructure into another.

4.25 **In light of this, AIOTI WG4 recommends that:**

- Innovation and market forces should be left to drive the evolution of IoT portability standards and mechanisms.

"Data Ownership"

4.26 As mentioned in the introduction to this section, the term "data ownership" may not always be truly accurate as some data are not susceptible of ownership in the legal sense of the term. This is the case for personal data for example, but also for other types of data. Personal data typically belong solely and exclusively to the individual it relates to, irrespective of who else may have access to or knowledge of the information contained in the data.[28] The concept of 'ownership' works quite well for tangible matters but not so much regarding digital data.

4.27 Nevertheless, (certain) data can be and is protected by other means such as other proprietary rights, contractual rights, legislation and regulation. Therefore, in the subsequent sections of this paper, when the term "data ownership" is used, it should be understood as meaning, as appropriate, data control, proprietary or similar rights on data, and rights of access of re-use of data.

4.28 The access to, transfer and the re-use of data, is already covered to a great extent by several elements of the existing legal framework, including data protection, competition, unfair commercial practices, contract and consumer protection law, as well as intellectual property laws, including the database directive and the new trade secrets directive.

4.29 That being said, the IoT may create new challenges in relation to many of these topics. An important amount of these challenges are caused by the fact that, by means of IoT, the frequency by which data travels from one 'thing' to another through different infrastructures and several layers of (supply) chains, with or without human influence, has significantly augmented. Some of these challenges and the way in which they are addressed will be further considered below.

a. Proprietary Or Similar Rights On Data

[28] Exceptions may include unique identifiers such as National Insurance numbers, or numbers on Passports, Driver's Licence, etc. These all belong to the government entity that issued them, although they refer to an individual.

4.30 As mentioned already, although data may not be capable of being “owned”, they may nevertheless be subject to control. The extent to which such data is controllable or in another way protected firstly depends on the type of data.

4.31 Certain data may for an example be subject to intellectual property rights or similar entitlements (copyright, patents, industrial designs, trade secrets, business intelligence just to name a few).

4.32 Often though, various types of data are intermeshed so that a data asset comprises components of different natures subject to various regimes. E.g. a given file stored in an IoT device may well contain simultaneously personal data and copyrightable content, and also constitute a trade secret. Or legitimately acquired business intelligence belonging to one particular operator may very well be entirely built on personal data which the operator has never truly “owned” as such.

4.33 Because this is a highly complex, often confusing and still very poorly understood area which should be the subject of advanced legal studies in its own right, it is assuredly not a topic that the IoT community can address and settle on its own or for its own purposes. The answers to the questions raised by such complexities ought to be entirely technology neutral and business agnostic, since they will be relevant in the IoT context as in any other. Moreover, given the disparate entities potentially involved in the offering and differences in the nature and purposes behind the generation of certain types of data it is unlikely that a uniform regulatory solution can satisfactorily replace or substitute existing legislation and contract negotiations. In any case, the Commission is welcomed to conduct independently funded open and in-depth studies and consultations on these matters with relevant experts and stakeholders, among which IoT players will certainly be an important constituency to involve.

4.34 Having said that, a couple of considerations can already be formulated for the IoT community to reflect upon and to bear in mind. And whereas it is well understood that the Commission’s intention with the Free Flow of Data Initiative is to cover information strictly outside the realm of personal data, the considerations that follow with respect to personal data are nevertheless worth including here and bearing in mind at all times. Indeed, as said, it will often be difficult to dissociate, segregate or even distinguish personal and non-personal data in various IoT instances. Therefore the free flow discussion, even if relating to non-personal data, must still take into consideration any restrictions applicable to the flow of personal data, as such restrictions may also impact the flow of any other data which, for whatever reason, may not in a given context be dissociated from the personal data it is intermeshed with.

4.35 As it is not always clear from the outset what the actual (possible) use of an IoT infrastructure, platform, device, application or service (the ‘thing’ in IoT) is, could be or will be(come), and personal data may be collected and processed at some point, such IoT infrastructure, platform, device, application or service must be designed with individuals’ privacy in mind throughout the whole engineering process (Data Protection-by-Design) as well as embed the strictest privacy settings (Data Protection-by-default). These will in particular have to ensure that the collection, processing, disclosure, transfer and disposal of any personal data in the IoT system demonstrably happens in line with the requirements of the GDPR, for example the essential principles of:

- **lawfulness, fairness and transparency** (be relevant and appropriate to the legal basis for processing, e.g. consent, contractual necessity, legal compliance, legitimate interest)

- **purpose limitation** (state the purpose upfront and only use the data to that end)
- **data minimisation** (only collect and use so much data as indispensable)
- **accuracy** (be able to update, maintain, sanitise data as appropriate)
- **storage limitation** (be able to securely dispose of data at end of life)
- **integrity and confidentiality** (secure the data against undue access, loss or other compromise)

4.36 The use of privacy enhancing techniques such as segmentation, segregation, aggregation, pseudonymisation, tokenisation and anonymization by IoT developers should be encouraged across the board. There are a number of very strong legal incentives for those practices, both explicitly laid out and implicitly suggested by the GDPR. On the one hand, the less identifiable the information becomes, the less it is likely to involve a privacy risk to the individual, and therefore the less stringent the requirements on its processing become, especially in light of article 11 and recital 26 of the GDPR. On the other hand, as of the moment that the data is no longer identifiable, even indirectly, it loses its “personal” nature, and as of that moment it can become the proprietary business intelligence of whoever generated that anonymous data.

4.37 Last but not least, for data that is susceptible of some form of proprietary rights, IoT infrastructures, platforms, devices, applications and services should be so architected and designed as to enable the practical enforcement of such proprietary rights, for instance by including appropriate access control and digital right management features or capabilities.

b. Data Access And Re-Use Of Data

4.38 With regard to the topics of data access and re-use, a clear distinction should be made between personal data and other data.

i. Personal Data

4.39 As far as personal data is concerned, rights of access and use of the data are not in the hands of IoT players, they are narrowly regulated by data protection legislation. The two key considerations to bear in mind in that regard are the lawfulness of processing and the principle of purpose limitation.

4.40 As regards, the lawfulness of processing, the collection and processing of any personal data can only take place on one of the legal bases afforded by the law. IoT vendors should ensure that their products and services are so designed as to enable the demonstrable compliance with the specific conditions applicable to each of the available legal bases, depending on the one that will be relied upon in a given case. Notably (and not including here the legal bases of vital interest subject to very specific conditions and public interest subject to additional national or European legislation), each of the following bases may be relied upon in a given situation:

- Where personal data is processed on the basis of **consent**, the user facing IoT interface must be such as to provide the data subject with all required information to enable an informed choice, it should include a feature that prompts and records the consent expressed by the data subject bearing in mind the following rules: The burden of proof is on the controller; the consent needs to be explicit if the data processed falls in a special category; and consent must be withdrawable as easily as it is given. As the case may be, some form of age verification mechanism should also be included so as to enable compliance with the provisions relating to the consent of children online.

- Where personal data is processed in the **performance of a contract**, the user-facing IoT service must be so architected and designed as to clearly identify the scope of data indispensable to perform the contract between the vendor and the data subject, and to segregate that data so that it can only be used for that purpose. The use of the same data for other purposes, whether during or after the contractual relationship would need to rely on another legal basis.

- Where personal data is processed on the basis of a **legal obligation**, the data that is handled by the IoT instance must be scoped as narrowly as possible to meet the data minimisation requirement by only collecting and processing so much data as strictly necessary and proportionate to meet the legal compliance requirement in hand.

- Where personal data is processed on the basis of the **legitimate interest** of the controller or of a third party (e.g. to ensure the security and resilience of an IoT system), the purpose of the processing must still be clearly identified and made known, the principles of necessity and proportionality should also be fully respected and documented in particular as concerns the scope and volume of personal data collected and processed, and a proper balance of interests needs to be established and justified to determine that the legitimate interest pursued is not overridden by the privacy rights and interests of data subjects. In operational terms, this legal basis will be essential for countless IoT use cases including in non-consumer facing settings where the processing of personal data is merely incidental but nevertheless unavoidable, and where the purpose pursued is neither aimed at, nor even directly relevant to the data subjects. Such could be the case for example of smart transportation systems where the geolocation data of every individual vehicle may need to be processed for the purpose of operating the entire network, without however providing any service directly to any data subject. For the “balance of interests” test to be successfully met, it will be crucial that such IoT systems be architected and designed with all necessary and desirable privacy enhancing techniques so as to minimise the risk of privacy intrusions while still enabling the routine collection and processing of personal data.

4.41 As regards the principle of **purpose limitation**, this will be the key concept for IoT vendors[29] to bear in mind when thinking of the further processing (or “re-use”) of personal data. As long as data is being used for the original purpose stated when the first legal basis for processing was selected, the question of “re-use” essentially boils down to the appropriate management of data stewardship in the IoT value chain, contractually assigning the proper responsibilities and liabilities to each controller, joint controller, data processor, data sub-processor and other potential recipients of the data. Where the issue becomes more delicate is where a piece of personal data collected for one purpose is meant to be reused for a different purpose. This is not impossible but requires strict conditions to be met. The processing must be based on one of the available legal bases: if acquiring renewed informed consent of the data subject to the

[29] The term IoT vendor is used to define product, service and infrastructure providers in the IoT ecosystem. This document uses the terms IoT ‘service provider’, ‘supplier’ and ‘vendor’ interchangeably.

new purpose is not practicable, processing on the basis of legitimate interest remains possible, provided that (1) the new purpose is not incompatible with the original purpose of collection, (2) information is made available on the new processing and its purpose, (3) and it is re-established that the new legitimate interest pursued is not, in its given context, overridden by the privacy rights and interests of the data subject. For IoT vendors, such secondary re-use of personal data collected initially for a different purpose could be a very important business lever, but the ease or difficulty of doing it will to a large extent depend on how the GDPR rules on the notions of anonymous data and of processing not allowing identification (article 11, recital 26) are interpreted and implemented, especially in light of the outcome of the discussions about the grey zone of "derived data" mentioned in the previous section.

4.42 Turning now to the question of the "re-use" by an IoT service provider of personal data collected by another IoT provider, the same conditions will apply, with, in addition, the obligation for the source organisation to inform data subjects of the fact that the data is disclosed to the recipient, the obligation for the recipient to also inform data subjects of the source of the data and of the purpose of the processing, as well as the obligation for the recipient to offer data subjects a right and a practical means to object to the processing of their data. In other words, privacy law does not forbid the re-use of personal data from one IoT vendor by another IoT vendor, but it does set precise and detailed requirements on how this may be possible, ultimately preserving the data subject's ability to control the subsequent use of their personal data.

ii. Non-personal data

4.43 Moving on to non-personal data which, unlike personal data, may be subject to proprietary rights, there is no specificity that should make the re-use (e.g. licensing) of proprietary information by third parties any different in the IoT space as it is elsewhere. If the data generated in an IoT environment qualifies as "open public sector data" under applicable European or national provisions, the access to and use of such data should be permitted under the conditions defined by such rules. If on the other hand the data constitutes intellectual property, business intelligence or any other form of proprietary information of the IoT vendor(s) involved, statutory provisions and contractual arrangements applicable to such information should prevail in the IoT space as they prevail elsewhere. Part of the business incentive for the development of IoT applications is the ability to generate valuable information which gives competitive edge, commercial advantage or other forms of benefit to whoever invests in the generation of such data. Forcing the mandatory disclosure, free re-use or other surrendering of data thus generated would severely damage the attractiveness of IoT, question the sustainability of investments, jeopardise access to venture capital, deter innovation and ultimately defeat the massive benefits in terms of growth and jobs that the European Single Market should expect from the take-up of IoT.

4.44 **In light of this, AIOTI WG4 considers that**:

- Acknowledging the GDPR, policy makers and legislators should remain as neutral and as agnostic on this matter as possible, and leave it to market operators to decide which business models (open data, proprietary data, combination of both) best suit their needs. There is no objective value judgement that can be made for or against any particular approach, value generation can happen in a number of ways and innovation and entrepreneurship should not be unnecessarily interfered with or curtailed.

5 – IoT Liability

Introduction

Background

5.1 This section furthers the discussion around product safety and liability in the context of the IoT product landscape, taking into account the European Commission's Staff Working Document "*Advancing the Internet of Things in Europe*"[30] Section 2.6, *Safety and Liability.*

Revisiting some key questions in the context of IoT product safety and liability

5.2 The Staff Working Document cites a number of questions in relation to the interdependency that accompanies the sophisticated networks of products, services, users and providers that characterise the IoT space. There are important questions to be addressed in the context of IoT products and services,[31] including:

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

5.3 The answers to these and other key questions will become clearer as the full potential of the IoT starts to unfold. Crucially, this will enable legislatures and policy makers to have a much clearer understanding of the types of novel issues presented by IoT products and services in practice. This will, in the long term, contribute to identifying to what extent a legislative and/or regulatory response is required. In the short term, it's still very early days for the IoT – and it's important to take care to ensure that a premature response does not defeat the very beneficial purposes of the technology to the general community that response is trying to address.

Overview: The proper approach to the consideration of product safety and liability issues, and any consequential legislative or regulatory response

5.4 By way of overview, WG4 considers that:

- the questions cited above – and all questions around safety, liability, and the IoT – should not be looked at in isolation from the other potential issues relating to the IoT, such as privacy, security, and consumer rights in general;
- product safety and liability issues – especially regarding IoT products and services – cross borders; as much as possible, a coordinated global approach needs to be explored in order to avoid stifling innovation by creating an uncertain, inefficient and/or unworkable global legislative and regulatory context;
- in light of the above, any response – which might include the development of guidelines and other clarifications *aside* from binding law and regulation – should

[30] 19 April 2016

[31] p.21 AIOTI Working Group 4: Policy - Report dated 15 October 2015

be approached cautiously in the absence of clear evidence from directly affected stakeholders; and

- regulatory intervention and legislative reform should happen only: after thorough and broad stakeholder consultation; ideally once the technology's full potential is better known; in light of relevant consultations that are happening in other countries; and with regard to developments and discussion in other legal contexts (such as data protection, cyber security, etc).

5.5 Many of the "novel" safety issues widely considered to date and associated with the development of IoT technology can be reduced to expressions of the need for manufacturers to build adequate security into connected products, or to design products so that they "fail safe" in the event an unexpected event occurs and compromises the product's proper performance. These concepts may be more complex for IoT products, and the issues may arise more frequently as products become increasingly complicated and inter-connected, but they are not new concepts. Further, these are concepts which are accommodated surprisingly well within existing safety and liability regimes.

5.6 There is a significant analogy to be drawn with the development of the internet. The internet now permeates almost every facet of life (including the home, workplace, communications, transportation, business, leisure, and healthcare). This would not have been possible without the carefully balanced approached to the legislative and regulatory framework applicable to the internet adopted by government and policy-makers from an early stage, globally. A similar approach should now be adopted with respect to the IoT and associated products and services.

Product safety and liability: The analysis points to a "wait and see" approach, leading to incremental change and – potentially – clarification rather than legislative overhaul

5.7 Some commentators have suggested that the legislators and policy-makers should clarify product safety and liability issues in the context of the IoT by considering now, with a view to working towards amending in the not-too-distant future, the current legislative and/or regulatory landscape.

5.8 Legal certainty on both product safety and liability is an important objective. However, it's also important for IoT innovation and its potential to be given the legislative and regulatory "space" at the outset to flourish, so that it can bring fundamentally important benefits to consumers and industry alike.

- The legislative and regulatory "space" referred to above does *not* mean that there is (or should be) no relevant law or regulation regarding safety and liability applicable to IoT. The fundamental question is: to what extent are existing regimes sufficiently flexible to deal with any "novel" issues that might arise in practice? In WG4's view, broadly speaking, there is no strong evidence from affected stakeholders that the existing regimes are incapable of dealing with the issues that may arise. Albeit, this needs to continue to be monitored. In due course, it may become appropriate for regulatory guidelines to be introduced and/or for jurisprudence to respond to specific needs for clarification.

- *If* there is any legal uncertainty regarding product safety or liability at present, it's not apparent that this is adversely affecting stakeholders or slowing the pace of

IoT innovation.[32] However, there *is* a real risk of innovation being held back if new binding laws and/or regulations are introduced and are not fit for purpose.

- With regards to product liability specifically: liability is – of course – relevant in both the B2B and B2C space, and each may lead to different considerations (as explored further below).

  (i) The B2B space may be satisfactorily and appropriately addressed through, for example, commercial contractual arrangements (in other words, the approach that industry is currently taking when pairing up IoT products and services).

  (ii) Legislative or regulatory intervention of any kind is not necessarily needed in the B2C space; and in any event, the involvement of directly-affected stakeholders will be key to understanding what is required.

5.9 The IoT presents challenges. At this stage, however, there's no evidence that the current product safety and liability regimes, which have proven themselves both robust and adaptable, are not sufficiently flexible to deal with new challenges as they emerge.

Analysis: Product safety

The current framework in the EU

5.10 Product safety law in the EU is, broadly speaking, a framework of directives and regulations, supported by a structure of industry (harmonised) standards. Some of the legislative measures have broad applicability to products across sectors (such as the General Product Safety Directive (Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety] and REACH (Regulation (EC) No 1907/2006 of the European Parliament and of the Council on the Registration, Evaluation, Authorisation and Restriction of Chemicals)), while others deal with products in particular sectors (eg the Toys Directive (Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the Safety of Toys) or Machinery Directive (Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC)). In most cases, EU product safety legislation has been developed around a model that sets out at a high-level the essential requirements for a product to be considered "safe", and addresses the specific obligations of those in the supply chain and others involved with ensuring the safety of products on the EU market.

5.11 The framework sets out an important role for industry-developed product safety standards. Where those standards are of the type published in the Official Journal of the European Union and harmonised to a particular product safety law, compliance with the standard will tend to lead to the benefit of a "presumption of conformity", as set out in the relevant product safety laws (albeit, generally, meeting the requirements of such standards is not mandatory). These standards are much more detailed in nature and might set out, for example, specific safety requirements for (or test methods to test for the safety of) particular types of products. The development of harmonised standards

[32] As was noted in the AIOTI Working Group 4: Policy - Report dated 15 October 2015: *"Designers of innovative products are already mindful of new (and significant) areas of legal exposure that may arise in future. In order to support an environment where innovation is encouraged, it may be necessary (in some cases) to legislate to "protect" innovators who produce beneficial technology that is deployed to manage certain risk scenarios. This is to ensure that the risk of potential liability does not act as a deterrent to the development and commercialisation of beneficial technology."*

involves a range of stakeholders, and standards can be amended and updated relatively quickly to meet changing technologies (without the need for legislative change).

5.12 Of course, product safety standards can also come from a number of other sources (and, depending on both EU law and member states' laws, might be mandatory or voluntary). Product safety standards might result, for example, from national standard-setting organisations, or might arise directly as a result of industry input and design. To an extent, the development and design of product standards can be seen as an opportunity for industry best practice to evolve, and for industry to – in effect – self-regulate.

5.13 In addition to laws and standards, the EU product safety framework is strengthened and clarified through the contributions of authoritative guidance documents. For example, the recently updated "Blue Guide" (The ‘Blue Guide’ on the implementation of EU products rules 2016) published by the European Commission is directed at member states' surveillance authorities to assist with the interpretation and application of EU product safety laws. The Blue Guide is also, however, an important and helpful resource for those in the product supply chain as it helps businesses to understand better the detail of what is required by EU product safety law. Although such guidance documents are non-binding, they serve a critical role – often assisting in clarifying product safety laws and so helping to achieve consistency and certainty. Guidance documents are often the result of the consideration and analysis of current challenges and/or uncertainties in the product safety framework, and help that framework to remain robust yet current.

Currently: is it enough for the IoT?

5.14 It's noteworthy that the current regime has evolved over time – with amendments as needed to product safety laws to take account of advancements in technology generally. The pace of legislative change has been gradual while the pace of technological advancement has been swift: and yet, consumers in the EU enjoy the protective benefit of some of the most rigorous product safety laws and standards worldwide.

5.15 The current product safety legislative and regulatory regime in the EU is robust: and it has also proven itself to be flexible and capable of responding as needed to deal with new issues that materialise, for example as a result of product innovation, or supply chain issues. A good example of this is the way that the European Commission has recently responded to the developing nature of the supply chain and the way in which consumers purchase products: the April 2016 edition of the Blue Guide, introduces, for example, new guidance to enhance product safety and consumers' access to information where products are purchased online.

5.16 Certainly, IoT products raise some interesting questions. One challenge presented by IoT is how to establish who is responsible for ensuring the on-going safety of an IoT product, given that the product's full uses – and the extent of its interoperability – may only become known at a much later stage. However, challenges presented by inter-connected products are not, in themselves, new concepts. Similar issues have had to be considered in the context of third party components and after-sales accessories.

5.17 At present, there is no clear case for legislative amendment in the context of product safety in light of IoT products. If it becomes clear that additional clarification is needed, it may well be that this can be achieved first and foremost by the publication of guidance documents – and, potentially, through the careful and measured development of product safety standards.

Analysis: Product liability

The current framework in the EU

5.18 At a high level, any product liability regime is primarily about the allocation of risk, and providing an appropriate level of protection for those who might suffer injury or loss as a result of exposure to products. A key objective of product liability policy is to ensure that liability rests on the most appropriate party, and that those who might be injured by products have appropriate remedies in the event that any injury is caused. In turn, the potential for liability may incentivise the development of safer products – and so product liability and product safety are intrinsically linked. While the liability regime has the potential to improve product safety, it also has the potential to slow the pace of change and innovation; the possibility of (and uncertainty around) significant liability may be a deterrent for the product innovator – resulting in a cost to society at large. There is therefore a fine but important balance to be struck.

5.19 The allocation of risk – and the question of "who pays" in the event that a product causes harm – is relevant in both the B2B and B2C contexts. Typically, businesses are well-placed to take appropriate steps to allocate risk as between themselves (eg contractually, and perhaps by working with insurers) – in contrast, product liability law takes special steps to provide protection for consumers.

5.20 In the EU, the product liability regime is dominated by the Product Liability Directive (Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products) ("**PLD**"), which co-exists alongside national systems of tort and contract liability. Naturally, the practical interpretation and application of the PLD (and member states' national laws implementing it) is an area for judicial involvement; at an EU-level, it's the role of the Court of Justice of the European Union ("**CJEU**") as ultimate arbiter. Courts, by their nature, are used to dealing with the interpretation and application of law – and having to deal with applying that law to both novel and complex situations.

Currently: is it enough for the IoT?

5.21 One reason often cited in support of the need for legislative and/or regulatory change in the context of product liability is that the PLD was adopted in 1985, before even the internet rose to prominence[33]. In light of this, it's tempting to conclude that the PLD is not an adequate solution for dealing with liability questions in the IoT space on the basis that the legislation was drafted long before the possibility of IoT products was contemplated.

5.22 As a starting point, however, the time that has passed since the PLD was introduced does not, of itself, justify the need for its amendment to deal with IoT issues. The PLD has so far had a 30 year lifespan, and there have been many advancements in technology and the supply chain during that period which were not envisaged by those who drafted the legislation. It's a credit to the drafters of the PLD that – despite regular reviews of its implementation and contribution to member states' legislative landscape – the PLD has consistently been considered, overall, a good piece of legislation that strikes an appropriate balance between all interest groups.[34]

[33] Reiner SCHULZE, Dirk STAUDENMEYER (eds), *Digital Revolution: Challenges for Contract Law in Practice*, Nomos, 2016

[34] See for example: "*Product liability in the European Union – A report for the European Commission*" – (The Lovells Report) 2003; Fourth report on the application of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative

5.23 Examples of suggested potential weaknesses of the current EU product liability regime when applied to IoT products include the following:

- The definition of 'product': The distinction between "product" and "service" is not a new issue, and is one that has been the subject of much academic debate, and occasionally has arisen for consideration by courts. The development of the IoT raises the prospect of further situations in which these blurred lines arise, and the possibility of ambiguity as to the application of the PLD in particular situations. It will always be necessary to rely on the courts to resolve ambiguities in the interpretation of legislation as they arise, and this area could be considered familiar territory for European courts. Having said that, if there emerges evidence that ambiguities in the interpretation of the PLD are creating problems for stakeholders in practice, there may be a case for taking steps to clarify the position, whether by way of the publication of guidance, or by amending the PLD itself.

- The burden of proof: the person suffering damage from a defective product has to prove the damage, the defect of the product, and the causality between both. Broadly speaking, it's been suggested that the complexity of IoT products means that this burden of proof is *especially* onerous, and so the liability system cannot achieve the same level of consumer protection as initially intended.

  Until such time as practical experience proves that the above is true, it's suggested that the "burden of proof" challenge is one of fact and evidence and, while in the spotlight due to IoT complexities, it is not *novel* to IoT complexities. This is an area where we should have confidence that the judiciary will be well-equipped to make the difficult judgments that need to be made. This issue was anticipated by the drafters of the PLD, and the allocation of the burden of proof was an important consideration in ensuring the legislation struck the right balance between the various interests. The national courts have proven themselves flexible in dealing with the burden of proof issue in specific cases, ensuring that the law is applied in a way that strikes the appropriate balance between stakeholders[35].

- The development risks defence: the defence is set out in Article 7(e) of the PLD, and provides the producer with a defence to (otherwise strict) liability if he can show *"that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered"*. This provision is intended to balance commercial innovation

provisions of the Member States concerning liability for defective products amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999.

[35] For example: In *A & Others v National Blood Authority* [2001] 3 All ER 289 a group of patients brought a group action having been infected by the Hepatitis C virus following transfusions or treatments that made use of infected blood. The blood being considered to be the product, and the virus the defect, the court determined that infected blood products were non-standard, and dismissed the assertion by the Defendant that the public were not entitled to expect 100% clean blood. This example illustrates the court's ability to apply the provisions of the directive to challenging factual scenarios in order to protect consumers.

Recent cases such as *Ide v ATB Sales Ltd; Lexus Financial Services (t/a Toyota Financial Services (UK) plc) v Russell* [2008] EWCA Civ 424 and *Hufford v Samsung Electronics (UK) Ltd* [2014] EWHC 2956 (TCC) have shown that courts will continue to develop their application of the PLD, in a manner widely perceived to be make claims under the PLD more 'consumer friendly'.

with consumer protection. It's been suggested, however, that given the pace of change and potential for uncertainty in terms of the full potential of IoT products, it would be more appropriate for the producer to bear the cost of harm in this situation since the producer would be much better placed to consider potential risk, and perhaps (even) to insure against such risk.

This argument overlooks the fact that the development risks defence has in fact been interpreted very narrowly by the courts: and almost never applied outside of the pharmaceutical sector. It is probably unlikely the defence would ever be applied in practice in the IoT context.

- The definition of "defect": Article 6 provides that a product is "defective" when it doesn't provide the safety which a person is entitled to expect. A product is not defective, however, if only an improved product is subsequently available. It's been suggested that, in light of the limitless potential for IoT products and connectivity, the definition of "defect" becomes uncertain and unworkable in practice – because it's not sufficiently prescriptive to help determine what a person is "entitled to expect" as technology advances at an unprecedented rate.

  This, however, is a concern that is not unique to the IoT space – and the CJEU and member states' courts have been able to appropriately consider the definition of "defect" in practice. There is no reason to believe that the courts would be unable to manage any difficulties in determining the level of safety a person is entitled to expect when the product is a sophisticated IoT device.

5.24 At this stage, there is no clear evidence to conclude that the provisions of the PLD could not be applied effectively in determining liability and providing an appropriate remedy for IoT claims. There may be areas of application where clarification is needed and so judicial interpretation helpful, and, as is usual, the law will have to be applied to unforeseen sets of facts. This is a challenge whenever there is technological advancement that may raise novel issues – however, this has not meant, and does not necessarily mean now, that the legal regime is not fit for purpose.

5.25 IoT innovations will mean that European courts, including the CJEU, will continue to interpret the PLD and to apply it in light of the PLD's aims in the face of challenging scenarios. This is consistent with the recitals to the PLD, which note that its objective includes *"solving the problem, peculiar to our age, of increasing technicality, of a fair apportionment of the risks inherent in modern technological production".*

It's important not to consider any review of the PLD for the IoT in isolation

5.26 The European Commission is currently preparing for a review of the PLD, as is required under Article 21 of the PLD. These reviews have been carried out regularly and this will be the fifth review. While the fifth report has not yet been published, it's useful to have reference to some of the conclusions that the previous report reached.

5.27 The report of the fourth review, published in September 2011[36], concludes that the PLD is *"seen as achieving a balance between consumer protection and the producers' interests"* and that it would be *"premature to propose a review of the [PLD] at this stage"*,

[36] Fourth report on the application of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999

a view shared by the previous reviews. It also would be premature to consider further steps in the regulation of the IoT sector – and potential revisions to the PLD – before the report from the fifth review has been published.

PRODUCT SAFETY AND LIABILITY: THE CASE FOR THE DEVELOPMENT OF POLICY AND GUIDANCE, *AS EVIDENCE OF NEED EMERGES*

5.28 When contemplating the current product safety and liability landscape, a number of potential options arise with regards to how to deal with issues resulting from IoT. These include:

- new IoT specific laws regarding product safety and liability (eg to sit alongside the existing legislative and regulatory landscape applicable to products in general);
- amendments to the current product safety and liability regimes (eg to specifically deal with IoT products, services, and supply chain issues);
- clarification of the existing product safety and liability regimes by means of policy documents and guidance, at both industry and government level; and
- in line with the example of the development of the internet itself, allowing the market to "self-regulate" within the existing frameworks with regards to product safety and liability as the technology develops, eg developing industry safety standards, codes, best practices, and the contractual apportionment of risk driven by the natural market and consumer influences.

5.29 The latter approach (self-regulation) has an important contribution to make in the further development of IoT products and services in terms of *safety*.

5.30 WG4's recommendation is that the third of the above approaches is currently the better course – combined with appropriate contributions from industry self-regulation. This is because:

- New IoT specific law and regulation may create a dual landscape for safety and liability (ie one being IoT specific), and there is no evidence that such a regime is needed – or would be beneficial. Such an approach is likely to lead to complexity, inefficiency, and uncertainty.
- With regards to liability in particular, there is no justification for dealing with IoT products that cause harm separately to other products – some of which already raise challenging legal issues arising from complexity and product interactions. This would lead to over-regulation and laws and regulation that, in all likelihood, would be a significant block to the full potential of IoT. This would be an unwarranted cost to wider society.
- The IoT is a rapidly developing industry, and the complexities and opportunities of IoT technology are far from known. Against this backdrop, it would be very difficult, if not impossible, to develop a legal or regulatory landscape to cover IoT issues relevant to product safety or liability, as those issues and challenges are not yet well defined or articulated.
- Any legislative or regulatory intervention should be in response to a clear need. There is otherwise the risk that IoT developments, products, and uses develop ahead of law and regulation (which becomes outdated quickly), or – in a worst case scenario – the intended purposes of law/regulation are not achieved *and*

beneficial innovation is constrained. Presently, it would be a considerable challenge for any change to the legislative or regulatory regime to 'future proof' itself against unforeseen innovations.

- It's also important to note that the creation of new laws, regulations and/or guidance does not automatically guarantee legal certainty. Until laws, regulations and guidance are implemented in practice, for example, the practical interpretation and application of new law is not known. For such a wide sector at the forefront of technological developments, this is particularly true.

- Until the existing legal and regulatory framework has been meaningfully challenged by any problems presented by IoT technology and products, in a real world environment, it is premature to seek to formally control this emerging technology.

- Consumer trust and engagement is key: and in this regard, the development of clarification/policy for the industry may contribute to consumer confidence in IoT technology – and so help IoT to achieve the many benefits that are available to modern society. To best contribute towards an environment where consumers and other users feel confident to explore the potential of IoT, it's most appropriate for industry, government, the judiciary, and other stakeholders (both in the EU and worldwide) to work together to clarify and apply the existing legislative and regulatory regimes.

Some hypothetical QUESTIONS presented by the IoT for product liability

5.31 Below is a generalised use case that illustrates some potential liability issues in the IoT space. It supports the case for further monitoring, consultation, and *potential* clarification of the existing product liability regime and it's applicability to IoT products. However, while it's relatively easy to outline a hypothetical risk scenario intended to create liability conundrums, care should be taken when trying to find guidance from such scenarios that might not typically manifest themselves in the real world in the way envisaged.

Hypothetical use case

5.32 Product A is a connected home appliance. It communicates with, and connects to, a number of other home appliances by the same manufacturer and third party manufacturers and shares and uses data from these other appliances. Data collected from a third party Product B was incorrect/deficient, resulting in Product A taking a decision which resulted in property damage. If the data from Product B had been correct/not deficient, Product A's decision would not have resulted in damage.

5.33 The above use case raises some novel questions, such as:

- Would Manufacturer A be liable under the existing regime? How would the claimant show that Product A was 'defective'?

- If the interaction with Product B was not anticipated by Manufacturer A, would they have a defence?

- Would Manufacturer A have a cause of action against Manufacturer B if the claimant successfully claimed against Manufacturer A?

- Would the consumer have a cause of action against Manufacturer B? How would the claimant show causation if Product A is the product that actually caused damage?

- Could Manufacturers A and B seek to disclaim liability against the consumer for the use of the product with a third party product?

What the use case shows

5.34 First, the use case shows that there is role to be played by the development of globally aligned safety standards – these might be expected to contribute to, for example, issues around ensuring the reliability of communications between devices, and how that can be tested as between connected products.

5.35 Second, the use case indicates that the apportionment of liability B2B is almost certainly something that the relevant product manufacturers will have already considered. Depending on the factual circumstances (including how "open" the devices' communication systems are), contractual arrangements may deal with this type of liability risk.

5.36 Third, the use case shows that – in terms of B2C liability – the relevant court would need to apply the current definitions and case law relevant to the PLD. There is clearly a role for jurisprudence.

5.37 Fourth, there would be evidentiary challenges for the consumer (ie the "burden of proof" challenges considered earlier in this paper). But very similar challenges exist in much simpler settings – for example, the interaction of two pharmaceuticals.

Recommendations of WG4 at this stage

5.38 WG4 recommends that policymakers take a gradual, reasoned and cautious approach to the development of a response to address any product safety and liability issues in the IoT space.

5.39 WG4 notes that many stakeholders are in favour of organic development for the IoT when contemplating issues relating to product safety and liability. For example, this view was very recently reflected in the comments responding to the United States Department of Commerce's *"Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things"*[37].

5.40 By maintaining a watching brief, the legislature and policy makers can observe how the existing regime is being applied to product safety and liability issues, and how the market is resolving safety and determining issues around liability (in a B2B setting, at least). This approach has shown promising signs in the connected cars space, for example where private-public partnerships such as ERTICO are moving towards common industry standards[38].

5.41 While the IoT industry develops, WG4 considers that policymakers:

[37] https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things

[38] ERTICO – ITS Europe is currently working to develop the open platform SENSORIS vehicle sensor data exchange platform into a new global standard: http://erticonetwork.com/ertico-coordinate-standard-development-vehicle-cloud-data

- Engage with industry to discuss novel applications of IoT technology and to investigate areas where failings in the current product safety and liability landscape may hinder the development of new technology.

- Monitor the development of the IoT industry and technology and how the industry is working to set its own guidelines or codes of conduct.

- Continue to work with the international community – IoT products need to connect internationally, and a global response will be key to enable IoT innovation to reach its potential and to bring the fullest benefits to both industry and consumers.

- With regards to liability in particular:

  (i) Consult further with consumer representatives, innovators, manufacturers and service providers to assess their perception of how the liability regime applies to IoT, and to investigate whether uptake of IoT technologies may be inhibited by uncertainty of who will be responsible should a problem occur.

  (ii) Monitor jurisprudence (within the EU and beyond) for how IoT technology is being treated and consider whether the current liability regime provides a satisfactory regime[39].

  (iii) Engage with the insurance industry to investigate potential effects of IoT and liability and whether insurers can help to address issues that arise.

Conclusion

5.42 At this moment in time, billions of devices are already online, connected, communicating, and responding – and, increasingly, without immediate prior instruction from humans. And yet: internet-connected devices, with sensors and sophisticated means of communicating with, and controlling/responding to, other devices are still in the very early days of development and uptake by society. Already, these products are providing considerable benefits in many areas of life: such as in medicine, transportation, cities, factories, agriculture, wearables, and the home. The full potential for IoT products and connected services is vast, and is still being explored.

5.43 Both industry stakeholders and policy-makers have commented that there are analogies to be drawn between the evolution of IoT products, and the evolution of the internet. The internet now permeates almost every facet of life (including the home, workplace, communications, transportation, business, leisure, and healthcare). This tidal-wave of progression has only been possible because of the carefully balanced approached to the legislative and regulatory framework applicable to the internet that was adopted by government and policy-makers from an early stage, globally. This enabled the creative development of a system that has brought previously unimaginable benefits to communities on a world-wide basis. In the opinion of WG4, it's important for a similarly considered and thoughtful approach to be taken with regards to safety and liability issues associated with IoT products.[40]

[39] The first case in the US involving IoT technology was *TRENDnet*: http://www.hldataprotection.com/2013/10/articles/consumer-privacy/ftc-brings-first-internet-of-things-enforcement/

[40] As was noted in the AIOTI Working Group 4: Policy - Report dated 15 October 2015:

5.44 WG4 recommends that policymakers adopt a "wait and see", and consultative, approach – and continue to work closely with innovators and other stakeholders to determine the best response in both the short and long term.

5.45 **In the meantime, AIOTI WG4 recommends as follows**:

- The current product safety and liability regimes, and the suite of other legislation applicable to IoT products but beyond the scope of this paper (such as consumer protection legislation), are potentially as applicable to IoT as they are to other products founded on technological advancement and innovation. There may be challenges in that application, but challenges are not novel, and jurisprudence and regulatory guidance may be satisfactory in the near future to respond to those challenges.

- For IoT products to thrive and reach their full potential, users must have trust and confidence in the safety and security of these products; this is as important in terms of digital safety as it is in terms of the more traditional areas of "product" safety. Industry therefore has a very real incentive to innovate in a way that ensures the safety and security of users; and a very real incentive to innovate in a way that is responsible and forward-thinking.[41] A significant contribution to safety and liability issues can be made by the self-regulation of those involved with the development of the IoT.

- With the considered involvement of eg government, policy-makers, industry and other stakeholders, the stage is well set for immensely valuable and exciting IoT product advancements and innovation to be realised in Europe. This will benefit the global community.

"Previous experience shows that this process of consideration, clarification, and (as needed) evolution can be the appropriate regulatory and legislative response".

[41] As was noted in the AIOTI Working Group 4: Policy - Report dated 15 October 2015: it is also important to bear in mind the accountability of innovators and industry involved in the development of the IoT and connected devices. *"The concept of 'accountability' is related to, but distinct from, liability. A detailed analysis of this relationship is outside the scope of this document. However, it is important for companies active in the IoT environment to have policies and procedures in place to ensure and demonstrate compliance by way of adoption of internal policies and mechanisms, which can include certifications37, seals, third-party audits38 attestations39, logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all operations under an organisation's sphere of responsibility. This will demonstrate compliance to external stakeholders, including supervisory authorities that are relevant for the particular industry/market. A pro-active approach to accountability should help address some of the perceived concerns related to liability of certain IoT applications."*