AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

Report

AIOTI WG04 – Policy

15 October 2015

Table of Contents

1- Executive Summary

The Internet of Things ('IoT') has the potential to transform European industry and the activity underway within the Alliance for Internet of Things Innovation ('AIOTI') represents an important opportunity for European industry to promote sustainable IoT growth.

AIOTI Working Group 4 ('WG4') is the policy working group. At the time of writing, WG4 has over 200 members across various sectors of the economy. The scope of WG4, as per the AIOTI terms of reference, is to identify existing or potential market barriers that prevent the take-up of the IoT in the context of the Digital Single Market, as well as from an Internal Market perspective, with a particular focus on trust, security, liability and privacy. WG4 has also assessed the specific recommendations that can be provided on net neutrality and IoT, given the current relevance of net neutrality to the European policy debate, following agreement of the Telecoms Single Market legislative package.

In this document, which represents the initial output of the Policy group, WG4 highlights a number of key issues related to each of these areas. In so doing, WG4 also makes a number of recommendations to further inform both the policy debate and the activities of the Large Scale Pilots due to commence in 2016. We also make reference to other relevant stakeholders that are carrying out important activity in this field and which should be linked to the work of WG 4.

WG4 makes the following policy recommendations:

- In relation to **privacy**, we make ten recommendations to address key concerns that have been raised in this area. These range from European Commission sponsorship of an accredited Privacy engineering program for European educational establishments, to adoption of Privacy by Design best practice by AIOTI members.

- In relation to **security**, we make specific reference to existing industry best practices on how IoT service providers can develop IoT enabled applications, which should inform the Large Scale Pilots. We also highlight the key stakeholder, technological and societal challenges in this area, and make recommendations in respect of each.

- In respect of **liability**, WG4 considers that the rapid development of IoT technology may raise certain product compliance, product liability and insurance-related issues in the future. At present we believe that these issues can be managed within the existing legal and regulatory framework. We propose that the emphasis should, in the main, be on the development of policy solutions to these potential challenges.

- In relation to **net neutrality**, we provide a number of case studies to help inform the activities of National Regulatory Authorities across Member States in light of the finalised text on net neutrality as set out in Telecoms Single Market package.

2 - Introduction

IoT is an innovation that is relevant to a wide range of different stakeholders across many kinds of markets. IoT brings together both the supply-side (i.e. those companies that may be active in designing the devices or providing the connectivity for IoT applications) and the demand-side (i.e. those companies that are integrating IoT technology within their operations and processes or providing IoT enabled products and services to end-users). Appropriate use of IoT data will also deliver many important socio-economic benefits. While IoT use is increasing rapidly, it is still in its nascent stages and the related technologies, business models and polices will undoubtedly evolve over a number of years.

To set the scene and provide a description of IoT, we refer to the previous definition of The Internet of Things by the ITU and IERC-Internet of Things European Research Cluster:

'The Internet of Things is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network.'[1]

IoT applications can be built using any number of technologies, and given it is a fast-moving market, it can be challenging to adopt precise technological definitions in a document such as this. WG4 has endeavoured to ensure that its policy recommendations are sufficiently flexible to cater for a range of IoT innovations, recognising of course that the specific risks (whether privacy, security, data management or liability) will differ according to the exact IoT use-case in question. In this document we refer to 'IoT applications' when we describe different types of IoT innovation. No precise legal meaning should be ascribed to this term.

It is also the case that certain IoT applications may prompt a wider societal debate. As WG4 notes in this report, the "ethical" implications of certain potential IoT innovations that involve automated decision making (such as autonomous cars) is a common topic among academics and in the popular press. WG4 believes that it is society that will ultimately determine whether such innovations take hold or not. WG4 hopes that the policy recommendations set out in this document will help improve individual understanding and awareness of potential policy challenges, and also solutions, related to growth of the IoT.

An important question that WG4 has considered in formulating the policy recommendations set out in this document is whether the emergence of IoT necessitates new regulation. Broadly speaking, WG4 does not believe that it does. Any regulatory proposal targeting the IoT should address only well-defined market failures that cannot be addressed through existing law and self-regulatory measures[2]. Furthermore, the IoT ecosystem is complex and fast-moving, creating a high risk of regulatory error[3]. Therefore any regulatory solutions should be technologically neutral, flexible, and respect the global, open interconnected character of the Internet[4]. On a related theme, WG4 does not make specific

1 ITU-T Y.2060, 'Overview of Internet of Things,' June 2012. White paper, 'Smart networked machines and Internet of Things, 'Association Instituts Carnot, January 2011.

2 European Commission, Better Regulation Guidelines, May 19, 2015, http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm, Better Regulation Toolbox, May 19, 2015 http://ec.europa.eu/smart-regulation/guidelines/toc_tool_en.htm

3 Shelanski, H. A. (2013) "Information, Innovation, and Competition Policy for the Internet", 161 U. of Penn. L. Rev. 1663 http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1025&context=penn_law_review

4 OECD Principles for Internet Policy Making, 2014 http://www.oecd.org/sti/ieconomy/oecd-

recommendations in the context of ongoing legislative processes (in particular the ongoing review of the General Data Protection Regulation) as we do not consider it within WG4's mandate to do so.

Again on a related theme, interested parties may wish to note that previous work has been undertaken by DG Connect, DG Justice, ENISA, NIST and approximately 200 companies in relation to Cloud SLA Standardisation Guidelines. This activity considered topics such as performance, security, data management and Personal Data Protection in a Cloud environment and provides some context to the work of WG4.[5]

Finally, given the range of stakeholders relevant to IoT, WG4 has focused on those policy topics which are of 'horizontal' application (i.e. they have immediate relevance to both the supply-side and the demand-side of the market). There are other important topics relevant to the continued development of a vibrant European market for IoT, including harnessing use of IoT data, free-movement of IoT data, access to spectrum, interoperability and numbering. These topics have not been considered by WG4 in this document, given the time available. WG4 remains ready to make policy recommendations in relation to these topics in the future.

principles-for-internet-policy-making.pdf

[5]See https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

3 - Privacy

Regulatory and Policy Context

In considering privacy policy options to promote the development of the IoT across Europe, it is first necessary to highlight the outcome of the previous IoT policy review initiated by the European Commission, which concluded in May 2013.[6]

Europe's policy options for a dynamic and trustworthy development of the Internet of Things

This report was commissioned by the European Commission and aims to inform the development of a consistent European policy stance capable of fostering a dynamic and trustworthy IoT that helps meet key European challenges. It was written following an extensive consultation with industry and identified potential gaps in the regulatory framework in respect of privacy and data protection (in particular regarding liability and responsibility). It identified three policy options that could be pursued, namely 'no action', 'soft law' and 'hard law', as follows:

Figure 3.1 – IoT Policy options presented to the European Commission in May 2013

Option	EC activity	Efficiency	Efficacy
No action	Current trajectories continue	No guarantee for development in accordance with EU objectives	Market players retain complete freedom
Soft law	Using monitoring, innovation policy, industrial policy	If sufficient incentives for adoption and uptake exist, high effectiveness is possible, while incentivising coherence with EU policy objectives	Market players retain some freedom in deciding the most effective manner of complying with requirements
Hard law	Harmonisation and enforcement in IoT-related areas (e-commerce, data protection etc)	Depending on enforcement, mandatory compliance can be highly efficient	Negative externalities are hard to foresee given the early stage of technology development, therefore are difficult to avoid in legislation

After consideration of these three options, the report recommended an initial soft law approach combining standards, monitoring, 'information remedies' and an ethical charter to facilitate IoT self-organisation[7] and clarify the need for and nature of effective regulatory interventions.

There have been two subsequent privacy developments of note particularly relevant to the

[6] http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=11701

[7] In making the recommendation for an 'ethical charter', the report noted that that this recommendation did not receive consistent support among those responding to the EC public consultation on the development of the IoT. The report stated that this was because of a division among those who felt the proposals did not go far enough, those concerned about its feasibility and those who doubted that it could work without a
stronger overarching governance structure, rather than a repudiation of the principle.
See http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-publicconsultation.

work of WG4, which will now be considered.

Article 29 Working Party - Opinion 8/2014 on the Recent Developments on the Internet of Things – September 2014[8]

This Opinion identifies the main data protection risks that lie within three specific IoT developments (namely wearable computing, quantified self and home automation). Although the Opinion is limited in scope, it does however highlight most of the main privacy issues related to the IoT. Therefore it provides an appropriate framework for assessing how the AIOTI should respond to possible IoT privacy challenges, subsequent to the last Commission review. The Opinion identifies the following IoT challenges:

- Lack of control by the user over an IoT device and information asymmetry between the user of the IoT application and the developer of the application
- Quality of the user's consent being poor
- Privacy challenges associated with inferences being derived from data, and repurposing of original processing
- Intrusive bringing out of behaviour patterns and profiling
- Limitations on the possibility to remain anonymous when using services
- Security risks.

After consideration of these challenges, the Opinion then highlights the following recommendations, common to all stakeholders, which therefore provides some context to the work of WG4:

- Privacy Impact Assessments should be performed before any new IoT applications are launched.
- Stakeholders must delete raw data as soon as they have extracted the data required for their data processing
- Every IoT stakeholder should apply the principles of Privacy by Design.
- Data subjects and users must be able to exercise their rights and be "in control" of their data at any time
- The methods for giving information, offering a right to refuse consent should be made as user-friendly as possible
- Devices and applications should also be designed so as to inform users and non-user data-subjects.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – June 2015[9]

The key legislative initiative in the field of data protection and privacy that needs to be highlighted in order to adequately frame the work of WG4 is clearly the reform of the EU General Data Protection Regulation (GDPR).

At the time of writing, the relevant European institutions are negotiating the amendments adopted by the Parliament in March 2014 and the general approach of the Council (June 2015). A detailed analysis of the GDPR is outside of the scope of this report and the primary focus of our recommendations is not framed towards changing the GDPR text but how to work within the framework once it is adopted. However, in protecting individual privacy,

[8] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[9] Interinstitutional File: 2012/0011 (COD)

policy makers should take into account that the IoT is characterised by cross-fertilisation of data, individualised approaches, ubiquitous devices – often without user interfaces – and free flow of data. As such, data protection legislation should consider the context of data use and reasonable expectations of users, and not take overly-prescriptive approaches to purpose limitation, notice, consent, profiling and cross border transfer. These remain concerns in the current negotiations.

In line with the WP29 Opinion, the current draft of the GDPR envisages use of Privacy Impact Assessments (where processing is likely to result in a high risk to the rights and freedoms of citizens) and use of data protection by design principles. The Regulation also emphasises that codes of conduct should help illuminate Privacy by default and by design principles. The principles and processes underpinning the GDPR will equally apply to those that are designing and developing IoT applications.

Starting point for AIOTI WG4 IoT Privacy policy recommendations

The starting point for the work of WG4 should therefore be to ensure that, where required, IoT applications are developed with privacy compliance in mind. We should also work to evaluate if and when a Privacy Impact Assessment is necessary in the context of the IoT, and develop a standardised approach to performing such assessments, in accordance with Privacy by Design best practice. Such an approach is consistent with both the recommendations of the Article 29 Working Party Opinion and the current scope of the GDPR. This should provide the correct frame of reference for the WG4's policy recommendations and also provide guidance for those developing IoT applications in the context of the Large Scale Pilots.

Existing or potential privacy barriers to take up of IoT across Europe

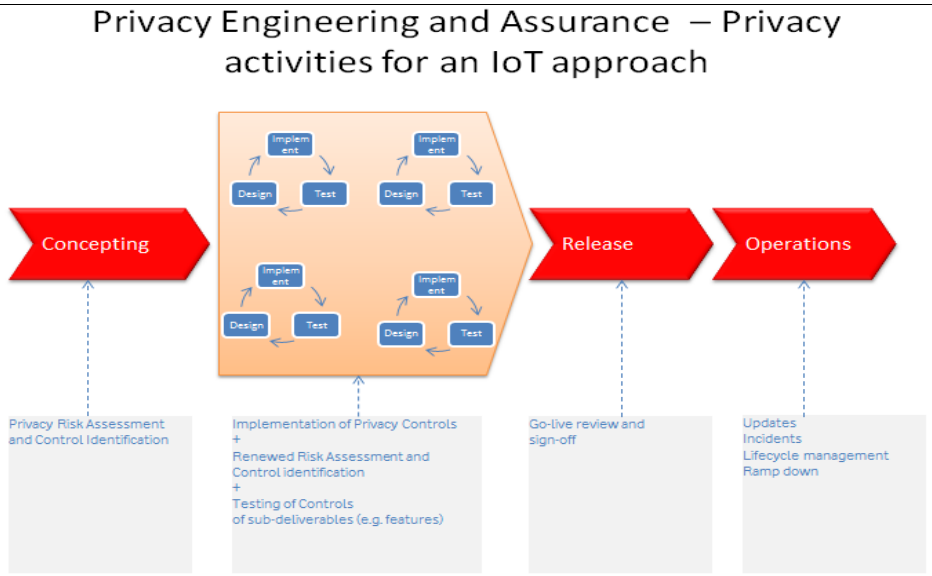
Within this framework, WG4 has identified ten specific privacy barriers that may pose a threat to take-up of IoT across Europe, and which must be addressed. WG4 believes that the adoption of these ten policy recommendations provides a comprehensive basis for addressing privacy concerns associated with IoT.

	Privacy Barrier	**AIOTI WG4 response**
1	'Privacy Engineering', an integral component of a Privacy by Design approach, is not yet embedded within the engineering community	**Context** - Education programmes are needed to create a new type of professional, the privacy engineer. European students are gaining engineering qualifications but privacy is not part of the curriculum. **Case study –** the UK government recently announced funding for a £10m IoT research hub[10]. The Research Hub will combine a small number of leading universities. The research focus will be on the challenges associated with privacy, security and trust in the IoT, including the various interactions, policy and governance, beliefs and behaviours between people and the IoT systems. **Policy recommendation -** DG Education and Culture to raise awareness within relevant EU academic institutions. It should consider schemes for sharing educational materials as recommended by PRIPARE[11]. It should consider sponsoring an accredited 'Privacy Engineer' scheme.

[10] https://www.epsrc.ac.uk/newsevents/news/iothub/
[11] http://pripareproject.eu/research/ see WP4

2	There is no commonly applied framework for privacy risk that can be translated into engineering objectives to help companies implement their own privacy impact assessments.	**Context –** Privacy Impact Assessments are an important way of identifying privacy risk. However, these can be complex. We need a commonly accepted way of analysing privacy risks for IoT applications and a standardised method to carry out such assessments. **Case study 1** – The 'Privacy Risk Framework Project', established by the Center for Information Policy Leadership[12]. This project aims to develop a methodology and tools to apply, calibrate and implement abstract privacy obligations and to prioritize compliance based on the actual risks (likelihood and severity) and benefits of the proposed data processing. It also aims to build consensus about privacy harms to individuals (tangible, intangible, societal). **Case study 2** - There are positive examples of industry associations communicating to their members the use of risk-based methodological approach to privacy. One such example is the 'Milton Keynes LPWAN IoT demonstrator', facilitated by Digital Catapult, and which has been highlighted as a case study as part of the Society for Motor Manufacturer and Traders' (SMMT) Connected & Autonomous Vehicles Forum. This approach differentiates between four different classes of data that may be collected on the platform, with the different levels of potential harm involved, as follows: (i) data from internet of things devices (ii) Personal data (iii) data that has ownership and rights and (iv) data closed in organisations. This may not be the final answer, but it shows the ways in which some analysis is developing. **Policy recommendation** – AIOTI members should encourage their industry associations to adopt privacy risk frameworks[13] which they should then communicate to all members for use in developing IoT applications.
3	There is a lack of widely acknowledged and endorsed privacy engineering approach	**Context** - examples of best practice are available, such as iPEN[14] , PRIPARE[15] and the Privacy Patterns repository[16] in the EU and NIST[17] in the USA **Case Study** Example 'IoT Privacy Engineering approach', developed by Vodafone, as follows:

[12] https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Centres_Privacy_Risk_Framework_Workshop_I_Initial_Issues_Paper.pdf
[13] See for instance ISO29134, CNIL privacy assessment methodology (http://www.cnil.fr/english/news-and-events/news/article/privacy-impact-assessments-the-cnil-publishes-its-pia-manual/), NIST risk management framework (http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf)
[14] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN
[15] http://pripareproject.eu/
[16] www.privacypatterns.eu
[17] http://csrc.nist.gov/

		 **Policy recommendation** –Connect/DG Grow to support best practice on privacy engineering in IoT. AIOTI members should encourage their industry associations to adopt a privacy engineering approach[18] which they should then communicate to all members for use in developing IoT applications.[19]
4	There is insufficient usage of pseudonymised and anonymized data by those designing and developing IoT applications	**Context** – use of pseudonymised and anonymised data would go a long way to addressing privacy concerns associated with IoT applications. **Case Study** – The Article 29 Working Party has also provided guidance on the types of anonymization techniques that can be used to ensure that a data holder's private data is not re-identified, while still allowing the data itself to remain practically useful.[20] **Policy recommendation** – the use of pseudonymised or anonymised data should be encouraged as the 'default' design principle for IoT applications. This can of course be subsequently changed as required in accordance with Privacy Impact Assessment and Privacy by Design best practice. But having it encouraged as 'default' will go some way to encouraging more widespread use. More broadly, the provision of less stringent rules in the case of processing of anonymised or pseudonymised data will be a real incentive for the adoption of these techniques, as well as other Privacy Engineering Technologies, by the industry. The chosen method of pseudonymisation and anonymisation must

[18] For instance PRIPARE contribution: http://pripareproject.eu/wp-content/uploads/2015/08/WG5_N94_PRIPARE_Contribution_SP_Priv_engineer_frmwk_v2.pdf
[19] Accountability is also a relevant concept here (see section 4 for more details on accountability).
[20] Opinion 05/2014 on Anonymisation Techniques. at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

<table>
<tr><td></td><td></td><td>however be proven to be resilient against inversion attacks, as it has been demonstrated that certain methods are vulnerable to re-engineering the original privacy sensitive data[21].</td></tr>
<tr><td>5</td><td>Lack of commonly understood and acknowledged knowledge bases of documented solutions to various recurring privacy problems.</td><td>Context - ‘Privacy knowledge bases’ are an important part of an effective Privacy by Design approach. There is, however, insufficient sharing of best practice which would address potential consumer concern, Industry should be proactive in sharing examples and best practice.[22]

Case Study – Vodafone Automotive Usage Based Insurance (UBI) product: example application of Privacy by Design principles

<table>
<tr><th>Privacy by Design Principle</th><th>UBI Product</th></tr>
<tr><td>1. Proactive not Reactive; Preventative not Remedial

Privacy by Design is characterised by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. It does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.</td><td>The UBI product adopts proactive privacy. It has been subject to legal reviews as well as checks against industry guidance, and consumer-protecting controls such as the ability to check and dispute records. These are built into both the technology and the partner contracts</td></tr>
<tr><td>2. Privacy as the Default Setting

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the product, by default.</td><td>The UBI solution is designed around a philosophy of privacy as the default setting.

For example, datasets for driving records (held by Vodafone and its partners) and policyholder records are only brought together in an aggregated statistical data in order to allow the Insurance provider to prepare the premium, to provide insurance services and respond to a customer request.</td></tr>
</table>
</td></tr>
</table>

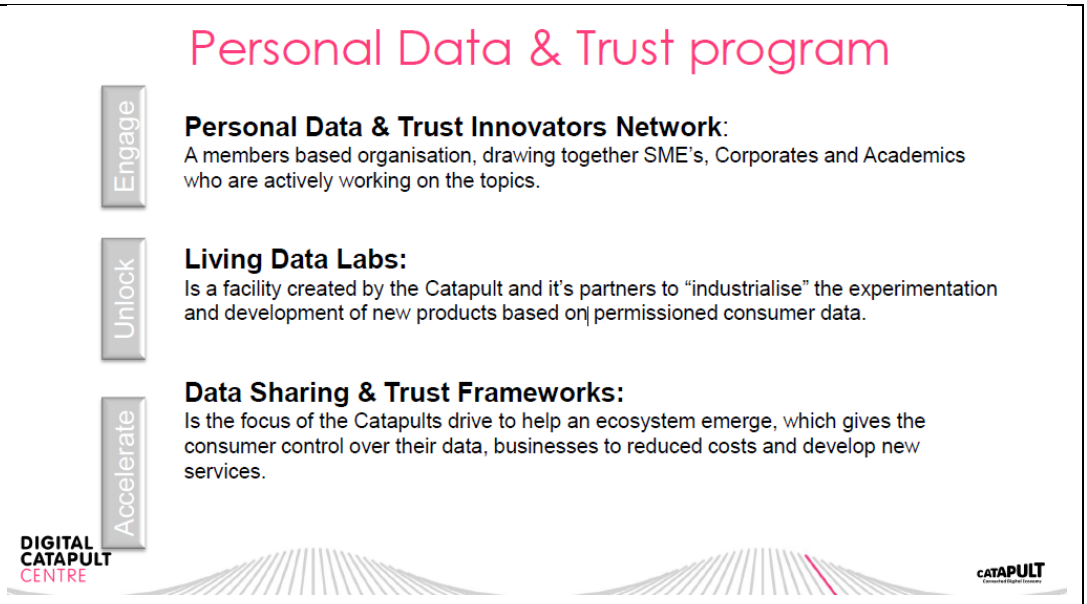
[21] “Model Inversion Attacks that Exploit Confidence Information” and Basic Countermeasures”, M. Fredrikson, S. Jha, T. Ristenpart, 2015 ACM Conference on Computer and Communications Security (CCS).

[22] There are examples from other industries that provide examples of best practice in a multi-stakeholder environment, such as the GSMA’s Mobile Privacy Guidelines for App developers (http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development) and the GSMA’s Privacy Accountability Framework for the implementation of the App Guidelines (http://www.gsma.com/publicpolicy/accountability-framework-for-the-implementation-of-the-gsma-privacy-design-guidelines-for-mobile-app-development).

		3. End-to-End Security – Full Lifecycle Protection Privacy by Design extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion.	UBI is subject to stringent information security policies and practices. . Delivery partners, including insurers, are contractually obliged to offer comparable levels of security.
		4. Visibility and Transparency – Keep it Open Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike.	The UBI product allows consumers to interrogate their driving records from a smartphone or PC, providing complete transparency of the data collected. Data is provided, with uploads from the in-car device at the end of each journey or uploads daily through the batch procedure.
		5. Respect for User Privacy – Keep it User-Centric Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.	The UBI product has been designed from the outset to respect driver privacy, through architecture and design, to the driver experience and interface. The policyholder can review their driving records, and the derived driving behaviour scores, through a web portal interface or through a smartphone. If the policyholder has reason to believe that the telematics record is erroneous, the policyholder can register or dispute data where appropriate to maintain their driving behaviour profile.
		Policy recommendation – AIOTI members should share and publicise case studies of how they have embedded a Privacy-led approach within their IoT application development. They should store these resources in an 'AIOTI Privacy	

		Knowledge Base' to be made available to Large Scale Pilots.
6	There is currently no 'Privacy by Design' technology guideline or standard.	**Context** -Technology standardisation is not subject to a mandatory Privacy Assessment to understand the privacy impacts of the technology in question. **Case study 1 -** there is experience of defining privacy and security standards in a Cloud environment, as per ISO/IEC 27018[23] and ISO/IEC 27034[24]. **Case Study 2** – activity is already underway by the European Commission[25] (Mandate 530) for **European standard(s)** addressing privacy management in the design and development and in the production and service provision processes of security technologies and European standardisation deliverable(s) giving **practical guidelines** for the practical implementation of the requested European standards. **Policy recommendation** – the European Commission should place greater emphasis on adoption of this technologically neutral 'Privacy by Design' methodology in the context of its Digital Single Market activity. It should also ensure that IoT applications are considered within scope of the practical guidelines and liaise internationally as required. AIOTI members should encourage their industry associations to participate to the current standardisation work (CEN/CENELEC JWG8, ISO/IEC JTC1/SC27/WG5, OASIS).
7	Data subjects and users may not able to exercise their rights and be "in control" of their personal IoT data, and so may not be able to give adequate consent where this is required.	**Context** - this is a legitimate concern that may be associated with certain IoT applications, however it does not need regulation to address it. Industry needs to proactively respond to this concern. There are already good examples of best practice here. Transparency to the end user is key. **Case Study 1 –** Digital Catapult 'Personal Data & Trust Program' in the UK.[26] The Network aims to build and nurture a community that brings together industry, the public sector, funders, research organisations, individual researchers and innovators to support the UK in becoming the global leader in trust and responsible innovation with personal data (see reference to 'Data Sharing and Trust Frameworks' in slide below), as follows:

[23] Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors at http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
[24] Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts at http://www.iso.org/iso/catalogue_detail.htm?csnumber=44378
[25] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#
[26] http://www.digitalcatapultcentre.org.uk/personal-data-and-trust-network/

		 **Case study 2 –** The European Commission has recently agreed new EU-wide technical standards that will help users of Radio Frequency Identification (RFID) smart chips and systems comply with EU Data Protection rules and the Commission's 2009 recommendation on RFID (see IP/09/740).[27] People using electronic travel passes, or buying clothes and supermarket items with RFID tags in the label, will know that smart chips are present thanks to the RFID sign. **Policy recommendation**: The European Commission should highlight and coordinate examples of best practice across the EU, and publish information on best practice privacy-effective solutions. . There are opportunities for regulatory authorities and industry to work together more closely in this area (e.g. research on end-user consent and IoT applications)
8	Data associated with IoT applications can be cross-correlated in way that that creates privacy risk – i.e. 'repurposing of original processing'.	**Context** - As the Article 29 Working Party Opinion highlights, data originally collected through a device (e.g. the accelerometer and the gyroscope of a smartphone) can then be used to infer other information with a totally different meaning (e.g. the individual's driving habits). The Opinion states that, at each level (whether raw, extracted or displayed data), IoT stakeholders should make sure that the data is used for purposes that are all compatible with the original purpose of the processing and that these purposes are known to the user. **Case study** – The GSMA's guidelines on use of mobile phone data in responding to the Ebola outbreak[28] show the steps that need to be taken before such data can be used for a different purpose. Consistent with these guidelines, mobile operators will anonymise CDRs and adopt robust technical and organisational measures to protect them against unauthorised access and use. The analysis of the anonymised records by third parties (including research agencies, aid agencies and governments) and the sharing of any output from the analysis will take place under legal contract(s) based on these guidelines.

[27] http://europa.eu/rapid/press-release_IP-14-889_en.htm

[28] http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-Ebola-outbreak-_October-2014.pdf

		Policy recommendation – AIOTI members to highlight their own examples where data can be repurposed in a way consistent with applicable law, keeping in mind that applicable law is still under debate for the GDPR. Examples to be stored in the AIOTI Privacy Knowledge Base.
9	The rules are not enforced	**Context** – Regulatory authorities should enforce existing horizontal rules against those who do not comply. **Case study** - The FTC in the USA has shown that existing horizontal legislation can be equally applied to IoT applications.[29] **Policy recommendation –** there is a place for robust, harmonised and predictable law enforcement.
10	Not all companies place sufficient importance on privacy	**Context** – there is a perception that some companies do not do enough to put privacy at the centre of their activity. There is also a perception that only companies with data protection obligations (e.g. data controllers or data processors) place importance on privacy while suppliers (e.g; sensors, IoT capabilities, IoT platforms) do not do enough. **Case study 1** –Vodafone has privacy principles which are aligned with the OECD privacy principles, and include an explicit commitment to use of Privacy by Design.[30] ISO29100 also provides a list of principles These principles equally apply to IoT applications. **Case study 2** –The European Commission[31] (Mandate 530) for European standard(s) addressing privacy management in the design and development and in the production and service provision processes of security technologies involves all types of stakeholders including suppliers. **Policy recommendation** – all AIOTI members to publicly commit to develop IoT applications and subsystems consistent with Privacy by Design and AIOTI knowledge base best practice.

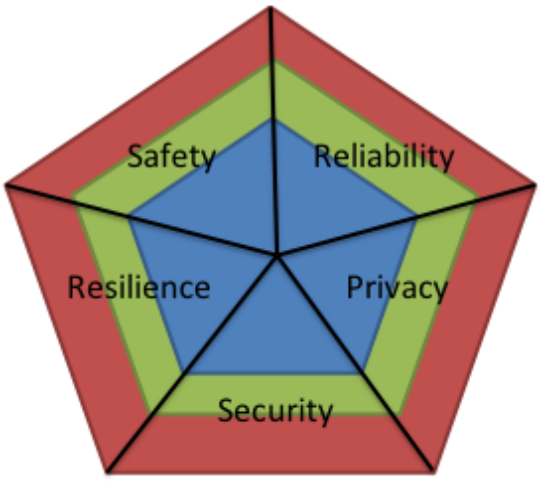
[29] https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter
See also https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices for further information on the FTC's activity in this area
[30] http://www.vodafone.com/content/index/about/sustainability/sustainability_report/issue_by_issue/privacy/our_approach.html
[31] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#

4 - Security

Regulatory and Policy Context

Security cannot be studied in isolation. Other aspects such as safety, reliability, resilience, and privacy are tightly linked as illustrated in Figure 4.1 below. Security does, in particular, tend to go 'hand in hand' with privacy when considering potential barriers to growth of IoT across Europe. Therefore many of the principles underpinning WG4's recommended approach to Privacy (for example a focus on the importance of a design led approach which is context dependent and usage of pseudonymised and anonymized data) will also be relevant here.

Figure 4.1 - Interdependencies of security with privacy and other domains.



As with technological progress in general, IoT brings benefits and improved productivity to users and organizations. Successful adoption of IoT systems depends on many factors, including security levels, related features, and measures to protect their assets and associated services. Protection of IoT related applications and services and the information they generate is necessary to ensure sustainable trust in IoT environments. Ongoing media reports of alleged security failures associated with IoT applications show that the public's perception of security issues associated with IoT applications have brought attention to security in IoT and highlighted the importance of adequate security support.

Security is a visible aspect of IoT applications and services, and there are numerous initiatives and projects relevant to the security work of WG4, some generally applicable to security in ICT and some specific to IoT. Regulatory activities such as the EU General Data Protection Regulation, the ePrivacy Directive review or the NIS Directive draft have some impact on security emphasis in IoT.

In member states, national 'Big Data' or IoT strategies, cybersecurity strategies reviews and and a number of other initiatives have addressed security in IoT or adjacent spaces more directly. In international standards bodies, several direct projects focusing on IoT appeared, such as IoT work in JTC1 SC10 and SC27. European mandate on cybersecurity standardization pursued in ETSI, CEN, and CENELEC also address standards and issues relevant to IoT.

Among some of the activities, we can mention:

- **ENISA (**European Union Agency for Network and Information Security).ENISA has undertaken several projects relevant to IoT, starting in 2008. It developed a view of risks specific IoT applications, and has considered IoT in multiple other reports[32].

- **NIS Platform** - The Working Group on Secure ICT Research and Innovation of the Network and Information Security ('NIS') Platform has produced a Strategic Research Agenda ('SRA') in the area of secure information and communication technologies. This SRA complements and underpins the EU NIS Directive, and provides input to the secure ICT Research & Innovation agenda at national and EU level, including the Horizon 2020 programs. The SRA has outlined multiple viable research areas and takes into consideration IoT challenges mainly in Privacy, Identity management, technical trust, lightweight cryptography and several other fields. It uses the example of smart building in smart cities and is organized around three main areas of interest:
  - Individuals' Digital Rights and Capabilities (Individual layer).
  - Resilient Digital Civilisation (Collective layer).
  - Trustworthy (Hyperconnected) Infrastructure (Infrastructure layer)

- **UK Government Cyber Essential Scheme :** Although IoT concerns were not specifically within the scope of the Cyber Essential Scheme, the different outcomes are equally applicable for those developing IoT applications. The key considerations in this respect are Trust ("Social acceptance") and Cyber-security ("Technological challenges").

- **Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)** as defined by the German Federal Ofice for Information Security (BSI).

- There is also **detailed sector specific activity** that has been previously undertaken, such as the 2011 CEN/CENELEC/ETSI Mandate 490 on smart grids (including the security and data privacy issues on the roll-out of smart metering systems), and the 2009 CEN/CENELEC/ETSI Mandate 441 on smart meters, as well as the guidance on software in smart meters, provided by WELMEC. Much work has also been undertaken in the context of Smart Grids for connected systems, particularly those built on open architecture.

- **ISO/IEC JTC 1/SC 27** maintains an expert committee dedicated to the development of the Information Security Management System (ISMS) family of standards. Through the use of this family of standards, organizations can develop and implement a framework for managing the security of their information assets. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

- **NIST CPS PWG (**Cyber Physical Systems Public Working Group**)** included significant EU participation and produced a reference architecture to address a number of issues relating to trustworthiness, security, and privacy.[33]

[32] See for example, https://www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel

[33] http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf

Starting point for WG4 IoT Security Policy recommendations

WG4 believes that a fit-for purpose security model for IoT should address the following policy objectives:

- It should be able to offer an adequate, affordable and 'desired' security level relevant to each application, matching users' needs and business requirements.
- As IoT applications have different connectivity requirements, they also need several scales of security, recognising that IoT applications may operate on a single platform/device or on several platforms/devices.
- Security requirements should offer flexibility that doesn't impede innovation of the technologies. The time to market and time on market considerations should be taken into account, without jeopardising the essential security needs.
- The model should also meet the desired security protection goals and privacy protection goals, e.g. confidentiality, integrity, availability, anonymity.

WG4 further believes that privacy-impacting IoT applications that deal with personal data should:

- Guarantee privacy and confidentiality of data exchanged through or in transit on the networks or stored in the IoT application or in the Cloud[34].
- Guarantee data authenticity to enable trustable exchanges (from data emission to data reception - both ways).
- Preserve integrity of a connected device (or system) for trustable solutions and services.

For those developing IoT applications as part of the Large Scale Pilots, it is vital that Security issues are addressed as part of the design and development phase. As the Large Scale Pilots address a variety of industry sectors, each should tailor security requirements according to their sector, to fulfil the adequate prerequisites, and balance the security risks to cost, throughout their life cycle.

Existing or potential security barriers to take-up of IoT across Europe and associated WG4 policy recommendations

Diverse stakeholders

Specific challenges include:

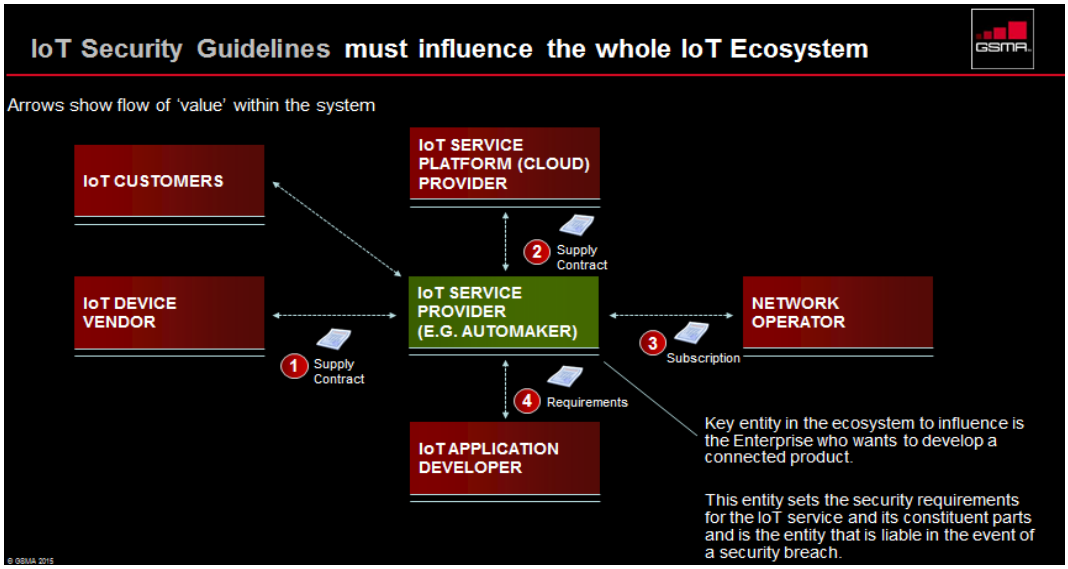
- The scale and diversity of IoT connected products will be enormous and their components may be developed by many different providers and not all of them may be able to provide the same level of security.
- Metrics and approaches associated with composite security necessary to support IoT infrastructure have not yet been developed.
- Access control for a large installed base of IoT applications can be onerous (i.e. to provide seamless access control which is fully scalable across all types of such IoT applications)
- There can be a security/go-to-market 'trade off' – IoT applications may be driven by disruptive products that are quick to market and may only spend a short period of time on the market – and security has cost implications.
- There may be interoperability and complexity challenges due to the more varied 'industrial value-chain' associated with IoT applications.

[34] WG4 notes that previous work on security and privacy in a Cloud context has previously been undertaken and which led to the formulation of the EC Cloud SLA Standardisation Guidelines (available at https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines)

WG4 policy recommendations

- There are examples of industry best practice that we can leverage to promote best practice across the diverse IoT ecosystem. One example is the ongoing GSMA activity to develop a set of security guidelines for the IoT. Another is the oneM2M project. By way of example, the GSMA guidelines (that will be included in the AIOTI Security Knowledge Base) are underpinned by principles that they must influence the whole IoT Ecosystem and are industry agnostic, as follows:

Figure 4.2 – GSMA's IoT Security Guidelines



Technological

Specific challenges include

- Securing connections with an increasing amount of devices based on different technologies, and acquired from various suppliers on the global market.
- Multi-criticality: e.g. security under real-time and non-real-time requirements.
- Verification and certification of complex systems and reconciliation of the cycles of security requirement with 'time to market' response.
- Cyber-Security solutions to protect a system when its attack surface is increasing:

WG4 policy recommendations:

- Embed 'safe and secure software'[35] design and development methodologies across all levels of device/ application design and development and implement security into that life cycle at the same time.
- Design, deliver and operate adaptive and dynamic end–to-end security over

[35] For example. in ISO 27001:2013 certification, a similar concept to "Safe & Secure software" is defined by referring to generally accepted safe coding practices (see for example https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide and http://cwe.mitre.org/top25/). The ISMS (Information Security Management Systems) Controls related to software development practices in ISO 27001:2013 generally includes a SECURE DEVELOPMENT POLICY which states that safe development practices as stated above need to be observed.

heterogeneous infrastructures integrating IoT, networks and cloud infrastructures. We recommend underlying standardised OS and hardware security features where architecture permits. The deployment should not be specific or propose a modification of existing OS and hardware already integrated by IoT.

- Develop best practices confirming minimum requirements for provision of secure, encrypted and integrity-protected channel, mutual authentication processes between devices and measures securing that only authorised agents can change settings on communication and functionality.
- Develop a 'New identity for Things' – To date, Identity and Access Management (IAM) processes and infrastructure have been primarily focused on managing the identities of people. IAM processes and infrastructure must now be re-envisioned to encompass the amazing variety of the virtualized infrastructure components. For example, authentication and authorization functions will be expanded and enhanced to address people, software and devices as a single converged framework.
- Develop a Common Authentication architecture **–** WG4 recommends investigation of a Secure Identity and Trusted Authentication mechanism, for example one which takes into account different authentication standards and will provide a single-sign-on solution for IoT applications moving between different systems.
- Certification **–** the certification framework and self-certification solutions for IoT applications have not been developed yet. The challenge will be to have generic and common framework, while developing business specific provisions. This framework should provide evaluation assurance levels similar to the Common Criteria for Information Technology Security Evaluation (IS0/IEC 15408), which should serve as the reference.

Societal

Specific challenges include:

- To ensure that potential societal concerns related to security of IoT applications are adequately addressed and so do not unduly restrict take –up of IoT applications.

WG4 Policy recommendations

- The ten recommendations as set out above in relation to privacy are relevant in addressing societal concerns associated with IoT.
- In particular, industry must promote use of privacy/security by design framework (see privacy section above in relation to the Mandate 530 activity which is addressing privacy management in the design, development, production and service provision processes of security technologies[36]. This methodology will enable enable manufacturers and/or service providers to design solutions consistent with this approach.

[36] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#

5 - Liability

Are there legal and regulatory barriers in existing EU laws?

The IoT means a remarkable number of devices can be connected to, and can operate through, a multitude of different technologies and services (which are often provided by many third parties). This raises complexity in terms of dealing with product liability risks. Privacy, security, safety and reliability are intertwined: product liability issues cannot be considered in a vacuum, and need to be considered in the full context of the IoT and associated potential legal risks.

In terms of whether there are legal and regulatory barriers in existing EU laws, WG4 considers that the existing regime needs to be evaluated carefully as the market develops, with an identification of key areas where *some* change may need to be introduced.

Identifying issues raised by IoT

Interdependency

Increasingly, the development of IoT technologies creates sophisticated interdependencies between product and service producers:

- By the nature of its design, an IoT product is dependent on third party technologies to perform its basic functions and to maximise the benefit to the user.
- These dependencies are not static: they can increase, and become more complex, over the life of the product.

Any interdependency gives rise to a number of questions. For example:

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

Further, any interdependency can also give rise to challenges in identifying the root cause of product failures, and in determining where fault lies in the event of a problem. Issues relating to liability when products involve third party components are (of course) not new. They are, however, emphasised when products are increasingly connected and complicated in both design and system integration.

Product vs. service

By their nature, IoT devices utilise electronic data to perform functions. Where that data is not embedded in the device, it can give rise to questions as to the applicability of laws intended to deal with "product liability". Again, this is not isolated to the IoT industry.

The distinctions between "products" and "services" made by courts and authorities when dealing with product liability in the past have been, often, unhelpful. The principles developed previously in this area may not be apt for dealing with the technology being developed now: some evolution in the "products" vs "services" debate is likely to be

required. In the UK for example, digital content will soon be regulated (for the purposes of consumer protection) separately from goods and services under the Consumer Rights Act 2015 ("CRA").

Legal implications of "ethical" considerations

IoT technology is increasingly able to replace decision-making functions that were previously only capable of being made through human judgement. The "ethical" implication of this is a common topic among academics and in the popular press. One of the emerging questions is whether there should be a legal or regulatory response to these ethical challenges.

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.

Accountability

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 certifications[37], seals, third-party audits[38] attestations[39], 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.

Cross-border issues

Consumers are increasingly sophisticated and can circumvent hurdles that sellers put in place to prevent the use of products and/or software in non-intended countries. This is an issue, of course, that is not restricted to the IoT; but IoT technology can give rise to cross-border issues with a higher level of complexity to be resolved.

Product liability issues

"Strict liability" for IoT technology?

At the heart of product liability law in Europe is the "no-fault" liability regime introduced by Directive 85/374/EC (the "Product Liability Directive"). This imposes liability for damages caused by a defective product on the "producer" of that product. Generally, the "producer" is either the manufacturer or the EU-importer.

37 E.g., ISO/IEC 27018 and ISO/IEC 27001 certifications, CSA STAR certification.
38 "Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion. Such certification would, as a minimum, indicate that data protection controls have been subject to audit or review against a recognised standard meeting the requirements set out in this Opinion by a reputable third-party organisation. In the context of cloud computing, potential customers should look to see whether cloud services providers can provide a copy of this third party audit certificate or indeed a copy of the audit report verifying the certification including with respect to the requirements set out in this Opinion." See A.29WP05/2012, Section 4.2, p.22.
39 E.g., SOC 2 attestation, CSA STAR attestation

Are certain IoT technologies "products" within the meaning of this legislation?

Some clarification may be needed over time in that regard. At a broader policy level, there arises the question of whether it is appropriate to extend a "no fault" liability regime to technologies that are more in the nature of a service than a product.

The Product Liability Directive was the result of a long period of negotiation and consideration, and it involved a careful balancing of many (and sometimes competing) interests in order to produce a workable and appropriate liability regime for products. It should not be assumed that the same "balance" will be achieved if this regime is extended to risks beyond its original remit. Consideration of whether the Product Liability Directive is fit for purpose should recognise the benefits of the current developed framework, and should not be rushed: careful thought is prudent before any legislative changes.

Product liability issues generally

Are there outstanding questions around who can be identified as the "manufacturer" or the "importer" of certain IoT technologies?

As connected products develop and become more complicated in both design and connectivity, for certain IoT applications it may become more difficult to prove the elements required for product liability claims to succeed (e.g. defect/negligence etc; identity of the proper defendant). This is bought more sharply into focus in the context of IoT products, in light of the interdependencies and level of complexity involved.

Product safety issues

Who is responsible for pre-market testing and certification?

It is important to assess how requirements for pre-market product testing and certification should be managed when dealing with complex products that operate interdependently with third party technologies, and where those interdependencies may change over the life of the products. It is also necessary to assess who is responsible for such testing and compliance and what level of responsibility should they be held to.

Again, while these questions are not novel, they may be challenging when dealing with certain IoT products. This is because of the level of complexity involved with certain IoT products, and the intertwined nature of diverse products, services, and providers.

Standards

The European product regulatory regime relies heavily on the development and application of standards – a system more flexible and efficient than reliance on prescriptive regulations. However, current technical standards are often inadequate to deal with emerging and innovative technologies, as they were not designed with such technologies in mind, and are not sufficiently flexible. IoT, by its nature, is both emerging and innovative: an on-going challenge will be the development of appropriate standards. Naturally, some work is being done in this area, a referenced by the activity underway within the AIOTI Standards Working Group.

The process for drafting new, and developing existing, standards can be lengthy and require considerable resources and stakeholder involvement. If not done well, standards can lead to

insufficient flexibility for manufacturers of innovative products to demonstrate compliance. While some European standards provide a presumption of compliance with the essential safety requirements of applicable EU product safety law, it is possible for manufacturers to prove compliance with the essential safety requirements by other means (for example, by undertaking adequate internal testing or meeting the requirements of international standards). The basic principle of the New Approach Directives allows flexibility for innovation that still creates safe products.

This is not an issue specific to IoT devices, but a challenge for innovative products (even in established industries) and services generally.

Insurance considerations

The difficulties in the allocation of liability highlighted above present a challenge for the companies involved in the development of IoT technologies, insurers and legislators alike.

Developers of IoT applications need to consider carefully the risks they are running when participating in the development of IoT technology, and the different ways they might be fixed with liability if their involvement is causative of malfunctions leading to injury or damage.

Insurers will need to be ready to offer insurance products which respond to the risks run by companies in a cost effective way. Where the scale and complexity of potential liabilities is too great to be managed at corporate level through conventional liability insurance, it may be necessary to develop arrangements whereby there is a "pooling" of risk. At its simplest, this could be an arrangement whereby all the participants in the development of a particular technology pay in to an insurance scheme designed to meet the cost of claims arising from the operation of that technology. Such schemes are often statutory in nature.

Legislators may also need to consider existing requirements in relation to insurance to ensure they are meaningful in light of developments in IoT technology.

Case studies where change may be required – autonomous vehicles and drone technology

An example of mandatory insurance is motor insurance covering individual users of vehicles. It will be necessary to determine whether this model will be appropriate in an age where the car is not operated by an individual user but by a remote operating system; the way in which the current insurance is required may no longer be relevant. It has been recognised that existing laws concerning manufacturer defects are substantially sufficient for determining liability in an accident involving a car with *some* level of autonomy. However, it has also been stated that a framework for determining liability on the transition of control from the vehicle to the driver of semi-automated technology would provide clarity including the application of current civil and criminal law, so this could be an area of future focus.[40]

Increasingly, drone technology is also in the spotlight in general as new risks and potential legal liabilities emerge. This is an area where insurance considerations are being discussed, and it will be worthwhile to be mindful of the development of (and issues that shape) that discussion.

[40] See https://www.kpmg.com/BR/.../Connected-Autonomous-Vehicles-Study.pdf

Recommendations at policy level/ in legislation

Product liability/safety recommendations

While the perception may be that the IoT raises issues so novel that significant legislative and regulatory intervention is needed, on closer analysis it is apparent that many of the issues are not new or unique to IoT technology.

Case studies of existing regimes that can be flexibly applied – nanomaterials and Consumer Protection Regulation

In most respects, existing regimes are well-equipped to respond to the new challenges within the current structures. Previous experience shows that this process of consideration, clarification, and (as needed) evolution can be the appropriate regulatory and legislative response:

For example, REACH[41] and CLP[42] do no explicitly refer to nanomaterials. However, nanomaterials are regulated by REACH and CLP because they are covered by the definition of a chemical "substance" in both Regulations. There has been much consideration given to whether the regulatory regime needs to change to specifically refer to nanomaterials – but there has been no knee-jerk reaction in response.

In addition, the UK Consumer Protection from Unfair Trading Regulations (which implemented the Unfair Commercial Practices Directive in the UK) has been used by a National Consumer Protection authority in enforcement action against deceptive trading practices by third parties on social media, which did not exist when the Unfair Commercial Practices Directive Act was adopted in 2005.[43] This shows how existing regulation can be relied upon to cater for subsequent developments in technology.

Overall, WG4 considers that there must be a balance between ensuring consumer protection and efficient mechanisms for allocating responsibilities, and ensuring that the measures do not stifle beneficial innovation or lead to unwanted competitive disadvantages.

In some respects, the legal and regulatory principles may benefit from some clarification, where traditional definitions and distinctions allow room for uncertainty. In many cases, the current system/current laws and regulations could be leveraged by using new guidance/guidelines from the European Commission. In this way, the application of such laws can grow with innovation instead of struggling to keep up.

Any policy responses need to be implemented in a way that is sufficiently flexible to deal with the rapid development of technology, while also protecting the overall objectives outlined above.

[41] The Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) provides an over-arching legislation applicable to the manufacture, placing on the market and use of substances on their own, in preparations or in articles.
[42] Regulation 1272/2008 on classification, labelling and packaging (CLP) of substances and mixtures that must be classified and labelled.
[43] See "Investigation into inadequate disclosures in respect of commercial blogging activity", UK Office of Fair Trading, Case CRE-E-25932, 2010

This fundamentally means that policy-makers must maintain close dialogue with industry participants and other stakeholders to ensure:

- unnecessary regulation is avoided
- the approach taken is effective
- the approach is fit for the future, and
- excellent and beneficial innovation is promoted

Insurance recommendations

Insurers and other risk management experts should be included in the discussions as the management of risk is going to be a key factor in allowing innovators to make progress.

Legislative changes in relation to insurance (especially compulsory insurances such as motor insurance) may be necessary over time to reflect the real changes the IoT makes to the risks run by different constituencies. The best example of this is motor insurance because the IoT will fundamentally change the way that cars are used. Currently, motor insurance laws are drafted on the basis that a human will have control of the car. Fully autonomous vehicles will remove control from the human and give it to a system. This will mean that, in this instance, product liability insurance will be more important than driver insurance. The various participants in the development of IoT technologies may explore the pooling of risk to deal with liabilities on a large scale.

Conclusion

The rapid development of IoT technology may raise a number of product compliance, product liability and insurance-related issues for certain IoT products. While aspects of the IoT give rise to special considerations in these areas, WG4 considers that at present the compliance and liability issues do not give rise to a clear need for new legislation or new types of regulation. Many of the product liability risks highlighted with regard to existing IoT products are not unique to these products and platforms. Such risks exist in established industries and, certainly, with regard to connected technologies in general. In light of this, WG4 considers careful consideration and dialogue should take place before the existing regulatory regime is amended.

It is possible to conceive of future IoT innovations that potentially challenge existing legal regimes (such as the autonomous car). Policymakers should maintain a watching brief with respect to how such technology develops. Forward-thinking responses may be needed to deal with the product liability issues associated with such IoT applications. Changes may be necessary to existing insurance legislation. Issues arise around the distinction between a "product" and a "service", and some clarification in that area may be needed to avoid uncertainty. However, these are not new issues in themselves, and do not give rise to insurmountable challenges within the existing regime.

Key to the development of IoT is striking the balance between ensuring consumer safety and promoting good innovation. Related to this is how to ensure the development of regulatory policy is sufficiently flexible to deal with the needs of an industry that is constantly evolving and which will be considerably different in just 5 years' time. An attempt to deal with the liability issues raised by the IoT through regulation that is not sufficiently flexible will generate inefficiencies and costs, which will benefit only those who operate outside those regimes. The development of policy solutions to the challenges that are raised needs close and on-going dialogue between policy-makers and industry. This will, hopefully, ensure that the approach taken is effective, fit for the future, and promotes excellent and beneficial innovation in an efficient way.

6 – Net Neutrality

Regulatory and Policy context

Given projected requirements for IoT quality of service differentiation, net neutrality is a subject which is of particular relevance to the growth of IoT across the EU. Machina Research estimates that the number of M2M devices requiring some form of differentiation of quality of service is likely to grow significantly over the next few years making up over 50% of all M2M devices by 2020. Those M2M devices requiring comprehensive or stringent Quality of Service (QoS) standards are estimated to increase from 1 billion to 3 billion units.[44] Net Neutrality is also an important topic for WG4 as it is of 'horizontal' relevance – i.e. regulation could materially impact on both IoT suppliers and customers alike. It is therefore an important part of the policy landscape affecting the broader IoT ecosystem.

In terms of the overarching regulatory framework, a political agreement, incorporating provisions on net neutrality, was reached on the Telecom Single Market Regulation (the 'Regulation') in July 2015 between the European Parliament, Council and Commission.[45] This text represents the most comprehensive pan-European net neutrality legislation to date and has been assessed by WG4 as part of its analysis of net neutrality and the IoT.[46]

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

The Body of European Regulators of Electronic Communications (BEREC) has been charged under the Regulation with laying down guidelines for implementation of the net neutrality provisions by national regulatory authorities (NRAs) within nine months of the adoption of the Regulation. WG4 considers that thought should be given to how these rules will play out in the IoT context and would like to take this opportunity to provide recommendations on the issues at hand.

Service categories under the Regulation

In terms of application of the net neutrality rules, there are three categories of service that matter in IoT's relation to the Regulation.

Internet Access Services

Internet access services (IAS), broadly speaking publicly available electronic communications services that provide access to the internet, are subject to the traffic

[44] Source: Machina Research (2015), DNA of M2M, www.machinaresearch.com.
[45] This text is expected to be formally adopted by the Council and Parliament in September/ October and enter into law in November 2015. It will apply from end of April 2016 or, in certain circumstances, end of December 2016.
[46] WG4 notes that some provisions relating to an open internet already exist under EU law. The 2009 revision of the Telecoms Framework ensures that internet users are able to access content, applications and services of their choice, introduced transparency measures and enabled minimum quality of service requirements to prevent service degradation. Moreover, at the national level, the Netherlands and Slovenia already adopted net neutrality laws in 2012 and 2013 respectively.

management and related consumer protection requirements of the Regulation.[47] Therefore, certain IoT applications will run over IAS and will be affected to the extent that the IAS provider is required not to discriminate against their application within the terms of the Regulation.

Specialised Services

'Specialised services', although not defined as such in the Regulation are services other than internet access services that are optimised for specific content, applications or services. The Regulation notes that such specific quality levels may be required by some new machine-to-machine services.

The Regulation introduces two important safeguards in the Regulation to ensure that specialised services are not used to circumvent the net neutrality rules and do not negatively impact the general quality or availability of the internet access service:

- The first of these states that optimization for specific content, applications or services must be necessary to meet a specific quality level.[48]
- The second safeguard only allows for the provision of such services if there is sufficient capacity to do so alongside any IAS provided.

Therefore, certain IoT services will fall under the 'definition' of specialised services, and hence will need to take care not to impact the quality or availability of IAS and to assess whether optimization is necessary to meet the quality level envisaged.[49]

Services which are neither IAS nor Specialised services

The third category of service are those which are neither IAS nor specialised services and hence fall outside the scope altogether and are not subject to any requirements. The important distinction between these and specialised services appears to hang on whether these services are being provided by providers of electronic communications to the public.[50]

Many more IoT services will fall entirely outside the scope of the Regulation as they do not relate to public provision of electronic communications.

Case studies

In order to inform the policy discussion around the application of Net Neutrality rules to IoT applications, WG4 sets out five IoT case studies which we believe will help clarify the regulatory environment and ensure there are no barriers to IoT take-up across the EU. For

[47] Article 2(2) "internet access service" means a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used

[48] Regulators will have the powers to verify if this is objectively necessary as opposed to granting general priority over comparable content, which would be infringing the non-discrimination requirement for traffic management in the provision of Internet access services and the ban against paid prioritization.

[49] It is worth noting that in this circumstance, the statutory responsibility is on the service provider in question to meet the obligations. Other actors in the IoT ecosystem may need to design their elements of the solution with this in mind but are not directly responsible.

[50] This is defined in the Regulation as: Article 2(1) "provider of electronic communications to the public" means an undertaking providing public electronic communications networks or publicly available electronic communications services;

each IoT case study, WG4 considers the position vis-à-vis the Regulation, given the approach that the Regulation takes to IAS and specialised services.

1. Telecommunications service provider offers IoT services alongside IAS

Case study

A telecommunications service provider offers an Internet access service to a location over the same connection. An example could be offering home security and automation (incorporating video and door security) and Internet access to a residential household. The home and security automation services are connected over the Local Area Network to the access network in order to allow for remote control and other functionality.

Analysis

In this case, a provider of electronic communications to the public (the IAS in particular) is offering the home security and automation service and hence the automation service qualifies as a specialised service They would therefore be subject to the optimisation as necessary requirement and to not negatively impact the quality or availability of the IAS by making sure there is sufficient capacity to offer this alongside the IAS.

Recommendation

In order to determine whether optimisation is necessary (consistent with the requirements of the Regulation), WG4 believes it should be measured against the specific requirements as requested by the customer. As such, in this instance the home security service would require optimisation to guarantee reliability of data transmitted in the case of a burglary. Without reliable data the purpose of the service itself would be defeated – it is therefore a necessary requirement.

2. IoT application strikes deal with telecommunication service provider for quality of service

Case study

The IoT application provider has an interest in establishing a guaranteed quality of service for their offering and pays the telecommunications service provider (in this case a mobile operator) to make such an agreement. The end user subscribes to an Internet access service provided by the telecommunications service provider alongside the IoT application.

An example could be a smart grid fault repair that provides real time service repair in emergency situations. The fault repair functionality sends signals via a mobile network in the case of an incident. The smart grid operator wants to guarantee that such a signal always gets through immediately, over and above the IAS provided to the end-user in the home for IAS, and hence contracts with the mobile operator to provide such service levels.

Analysis

Given the provision of the IAS, the mobile operator has the responsibility to ensure that the fault repair functionality is subject to the requirements of the specialised service, namely the necessary optimization requirement and impact on the IAS. From the point of view of the smart grid operator, they do not have any direct obligations but will have to make sure their service is devised in a way that will allow the service provider to meet their obligations.

Recommendation

In this case, it is hard to imagine that the service would impact the IAS in a meaningful way. The mobile operator is likely to be serving a large population with the same capacity such that prioritisation of the smart grid repair functionality is unlikely to have a significant impact and in any case, that prioritization would be an irregular occurrence and hence not have a general impact on the quality or availability of the IAS.

3. Provision of independent IoT application/ service over best-effort IAS

Case study

This is likely for many consumer-facing IoT applications, such as smart thermostats that connect over the LAN for remote control, or wearables that connect locally to a mobile device in order to upload location and health data.

Analysis

The IoT application or service has no specific deal in place with the telecommunications provider and offers their service over the best-effort Internet without additional guarantees of quality of service. Technical requirements such as low latency or packet loss are not deemed necessary in order to offer the service at the requisite level.

Recommendation

Under these circumstances, the application does not qualify as either an IAS or a specialised service and the IoT provider has no direct obligations to meet any of the provisions under the Regulation.

4. Private IoT network

Case study

The IoT networks in this situation are not available to the public. In many cases these will be the internal corporate networks of private or public sector entities.

Analysis and recommendations

To examine the implications for the implementation of the Regulation's net neutrality rules, we will break these private networks down into three subgroups

1) Private networks managed by a telecommunication service provider that do not include internet access

- Under the first subcategory, a telecom service provider manages a private network that is not an IAS. Take smart farming as an example. A smart agriculture network may collect information on crop yields, soil mapping, fertilizer applications, weather, machinery and animal health. A telecom service provider may provision and manage such a network but would not be providing any internet access services to the owners of the farm. Such private networks should not be subject to any of the provisions of the Regulation.

2) Private networks managed by a telecommunication service provider that include internet access

- Under this second subcategory, a telecom service provider's offer to an enterprise or other entity may include an internet service alongside other types of network. Such

an example may include an optional closed WiFi service offered by a telecommunications service provider to a car owner (in addition to the vehicle diagnostics service provided to the automotive manufacturer) and which is not an IAS, given it is limited only to the passengers within the car.

3) Private networks where the telecommunication service provider does not have a role beyond backhaul.

- In the third subgroup, either the enterprise itself manages the private network or a third party uninvolved in the provision of IAS does. In this situation, the role of the telecom service provider (if at all) is limited to backhaul at the point at which the private network connects to the public network. The Regulation would not be applicable to such a network.

5. Non-traditional 'internet access provider' alongside IoT services

Case study

Like the second subcategory in the section above, this situation involves the provision of a private network alongside internet access, but in this case at least one part of the internet access is publicly available. One could consider a smart city where sensor networks and other interconnected technologies are used to manage traffic flows, waste and water or save on energy from lighting, alongside an RLAN network for use by all citizens (e.g. the public network includes access to government and local information services).

Analysis

In many cases these networks will share capacity, with priority given to the private networks whose use cases are more essential than the public network. The pertinent question, therefore, is whether such public provision of internet access qualifies as an IAS and as a result whether the private networks are seen to be specialised services.

Recommendation

WG4 considers that this scenario should be interpreted based on Article 14.6 of the original Commission proposal on the draft Regulation. This article was deleted when the Parliament and Council decided to focus the Regulation specifically on roaming and net neutrality, but gives us our best indication of the Commission's thinking. It states *"An undertaking, public authority or other end user shall not be deemed to be a provider of electronic communications to the public solely by virtue of the provision of public access to radio local area networks, where such provision is not commercial in character, or is merely ancillary to another commercial activity or public service which is not dependent on the conveyance of signals on such networks."*

As an IAS is a publicly available electronic communication service by definition, and a provider of electronic communications to the public is one who provides such services, it follows from the clause that public access to RLANs should not be considered access to an IAS, as defined in the Regulation. WG4 considers that the provision of internet access to the public under the scenario envisaged in this section does not qualify as the provision of an IAS, which is subject to the open internet access provisions. Furthermore, the private IoT networks running in parallel to the public offering would not qualify as specialised services and hence would not be subject to the requirement not to negatively impact the quality of the IAS or the necessary optimisation requirement.

7 – Stakeholder activity

The table below suggests a number of stakeholder channels and events that we communicate the recommendations set out in this report.

Event/channel/medium	Date / frequency	Venue	Notes
European Data Forum 2015 – organised by European Commission and Luxembourg's Council Presidency	16-17 November	Luxembourg	The European Data Forum (EDF) is a meeting for industry professionals, researchers, policymakers and members of community initiatives to discuss the challenges of Big Data and the emerging Data Economy and to develop suitable action plans for addressing these challenges. Of special focus for the EDF are Small and Medium-sized Enterprises (SMEs), since they are driving innovation and competition in many data-driven economic sectors. The range of topics discussed at the European Data Forum ranges from novel data-driven business models (e.g. data clearing houses), and technological innovations (e.g. Linked Data Web) to societal aspects (e.g. open governmental data as well as data privacy and security).
The Future of Digital Content & Services	19 November	Brussels	Discussion topics still open – opportunity to present IoT within a holistic context looking at many other DSM initiatives like AVMSD, copyright, platforms, e-commerce and geo-blocking. *However, we should only target this event if we believe that there is a clear MEDIA angle on IoT.*
Brussels conference circuit	tbd	Brussels	This refers to a number of miscellaneous organisations (FT-ETNO; Forum Europe; EUagenda.eu; CEPS, Politico, etc.) setting up conferences on a range of "Brussels topics" from time to time. Whereas for Autumn 2015 most agendas are quite advanced for these events, it is at least possible to stimulate these organisations for organisation of ad-hoc IoT conferences around

			the turn of the year / Q1Y16.
European Internet Foundation (EIF)	Dinner debates, etc. ad-hoc. TBD	European Parliament (accreditation badge)	AIOTI + EC to approach EIF and agree an event on IoT. E.g. the next EIF event (on 15th September) focuses on bridging the ICT skills gap. The EIF is traditionally a good platform to bring together EP and all-industry stakeholders on Internet development and policy issues.
GSMA Mobile World Congress (MWC)	22-25th Feb.'16	Barcelona	This is where strategic steers are given to the world's GSM community (not just operators but the entire ecosystem) at the highest possible level. The Call for Papers closed on Friday, 4 September 2015. This was too early for the AIOTI WG4 recommendations, but we could formally request a speaker slot and obtain an extension for our submission, on the basis that it first needs to be approved by the EC. Similarly through GSMA Europe, we would agree a number of intermediate presentations at relevant GSMA working groups (identified by GSMA; at the very least the GSMA PSMC) – by the time this comes up to MWC, ideally recs would have already been endorsed by PSMC and CEO's of the leading operator groups.
GSMA Mobile Meeting Series (MMS)	To be created (AIOTI+EC sponsors, GSMA sets up)	Brussels	Small-format focused meetings (e.g. around dinner) for a variety of Brussels institutional and industry stakeholders, hosted by GSMA at their Brussels office (e.g. the next one takes place on 30th September and focuses on cybersecurity).