CREATE-IoT

H2020 Work Programme 2016-2017
H202-IoT-02-2016
Duration: 36 months

European Large-Scale Pilots Programme

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 05.03

IoT Data Value Chain Model

Revision : 1.0
Due date : 30-09-2017 (m09)
Actual submission date : 30-09-2017
Lead partner : AL

European Commission

Dissemination level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	X
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Summary					
No and name	**D05.03 IoT Data Value Chain Model**				
Status	Released	**Due**	m09	**Date**	30-09-2107
Authors	Ovidiu Vermesan (SINTEF), Roy Bahr (SINTEF), Soichi Nakajima (IDATE), Bertrand Copigneaux (IDATE), Arthur van der Wees (AL), Dimitra Stefanatou (AL), Jiri Svorc (AL), Marieke van den Ham (AL), Janneke Breeuwsma (AL)				
Editors	Arthur van der Wees (AL), Jiri Svorc (AL)				
DoW	The present document falls under the scope of the "Task 05.02: Data in the context of IoT applications". It is the initial report focusing on one of the key traits of the IoT environment, digital data flows. The discussion will identify the main challenges regarding data flows including data classification, data life cycle, digital rights management and personal data protection. The document will pave the ground later on for the creation of a set of recommendations by Work Package 5 to mitigate these challenges endorsing, to this end, a cross-domain approach in line with the strategy adopted by the Digital Single Market. Note that the aforementioned deliverable is the first out of the two deliverables provided under the aforementioned task. The second deliverable producing the final IoT data value chain model is due in December 2019.				
Comments					

Document history

Rev.	Date	Author	Description
0.00	04-09-2017	AL	Template and input
0.01	15-09-2017	AL	Further development of introduction, introductory part of Chapter 2, sections 3.2 and 3.4
0.02	19-09-2017	IDATE, SINTEF	Input sections 1, 2 and 5
0.03	20-09-2017	AL	Alignment of discussion, further input under sections 1 and 5
0.04	22-09-2017	SINTEF	Input Section 5
0.05	25-09-2017	SINTEF	Merge contributions Sections 5
0.06	26-09-2017	AL	Incorporating internal comments relating to the entire document
0.07	27-09-2017	SINTEF	Update formatting and layout.
0.08	27-09-2017	BLU, PHILIPS	Final review
0.09	29-09-2017	AL, SINTEF	Pre-final version
1.00	30-09-2017	SINTEF	Final version

Table of contents

1. EXECUTIVE SUMMARY

Internet of Things (IoT) data value chains place emphasis on the potential of IoT data, rather than on the data per se. This may result in the addition of several layers of value on top of the original raw data, which can be both private and public. As IoT data value chains are non-linear, they allow for the continuous use and re-use of data, which creates a series of challenges of legal and strategic relevance to be partly discussed under this deliverable. This aspect of non-linearity and re-use is captured by the concept of "life cycles" that is extensively used in the present analysis in relation to devices, stakeholders, data and law. Recognising the complex and *n*-dimensional nature of the subject, this deliverable discusses the topic pointing at the interference of markets and of data relation flows, highlighting the proliferation of risk across data value chains.

Taking into account the overarching objectives of Work Package 5 "IoT Policy Framework - Trusted, Safe and Legal Environment for IoT", this deliverable sets the scene of the regulatory developments at EU level relevant for the IoT Data Value Chains. It does especially from the perspective of challenges arising from recent and upcoming legislative changes, such as the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NIS Directive), while making reference to the draft Regulation for the free flow of non- personal data that is being released at the time of drafting this document. In addition, complex issues arising in cases of contractual documents are addressed and discussed, resulting in a number of concluding remarks that aim to improve transparency in the respective relationships (e.g. between software providers and services providers).

In addition, the deliverable produces a preliminary IoT Data Model for reliable IoT Data Value Chains aiming to support and further unleash the potential of existing and future IoT value chains. Based on the earlier discussion, it focuses on the attributes of economic feasibility, liability and transparency.

This document is addressed to IoT European Large-Scale Pilots Programme partners as well as the broader community of the IoT stakeholders. The deliverable forms the initial report that precedes the final IoT data value chain model due in December 2019.

2. INTRODUCTION

2.1 Purpose and target group

This document forms the initial report due under "Task 05.02: Data in the context of IoT applications."[1] This section provides an overview of the relevant scene for IoT data value chains introducing the set of the associated concepts surfacing the particularities of the IoT data value chains and paves the ground for the final IoT Data Value Model to be presented under "D05.04: IoT Final IoT Data Value Chain Model", due in December 2019.

Considering the disruptive nature of the IoT, current approaches when developing IoT business models need to be adapted accordingly based on a dynamic flexible IoT business model framework. The important opportunity in this regard is convergence of value chains with value networks on the context of IoT ecosystems. This will also affect the IoT Value Chain Data Models developed and used by IoT architectures, IoT platforms, IoT applications and IoT ecosystems.

The value chain concept was introduced in the field of Business Management as a tool to model the chain of activities that an organisation performs to deliver a valuable product or service to the market [1]. The value chain categorises the generic value-adding activities of an organisation allowing them to be understood and optimised. A value chain is made up of a series of subsystems each with inputs, transformation processes, and outputs.

In the context of IoT we can identify physical, digital and virtual data value chains as part of the different IoT ecosystems and over the IoT architectural layers.

The EC defines the data value chain as the "centre of the future knowledge economy, bringing the opportunities of the digital developments to the more traditional sectors (e.g. transport, financial services, health, manufacturing, retail)" [11]. This brings at least three distinct aspects along which the development of European data standards ought to be fostered:

- Standardised entity identifiers (i.e. identifiers of legal and physical persons, artefacts and their components, as well as time and location)
- Standardised, compositional concept systems (thesauri, taxonomies, ontologies)
- Standardised formats

These elements are key for IoT as standardised identifiers allow entities of interests (i.e. legal and physical persons as well as artefacts and their parts) and "things" to be reliably traced across independently established processes, managed by different applications, stakeholders, across connected supply, logistics chains and value networks. Standardised systems of concepts allow for IoT semantic integration, while standards need to be established for the actual formats in which data will be recorded on a medium for substrate or communicated across IoT networks and platforms [12].

From a similar standpoint, one can think of IoT as of a highly complex supply chain which connects an unlimited number of various devices together making it possible for the devices to communicate and operate through different infrastructures across various supply chain layers. As the supply chains extend across borders and industry sectors and domains, this supply chain in the existing and rapidly developing hyperconnected world is no longer linear. As a result, relations between the developers, vendors, consumers and other stakeholders of the digital economy and society (including but not limited to IoT enabled devices, systems or services) are non-linear. Collectively, they create an extensive multi-dimensional system which can also be referred to as

[1] D05.04 IoT Data Value Chain Model Evaluation & Final IoT Data Value Chain Model: The evaluation report as well as the updated IoT Data Value Chain Model (D05.03) and a recommendation report beyond this project is due in December 2019.

the *supply chain ecosystem*. Every participant within this multi-dimensional ecosystem is relevant and plays an important role in the design, engineering, manufacturing, deploying and functioning of both a connected device, system and service, as well as hyperconnected (IoT) ones [1]. Figure 1 presents a supply value chain in two dimensions (2D):

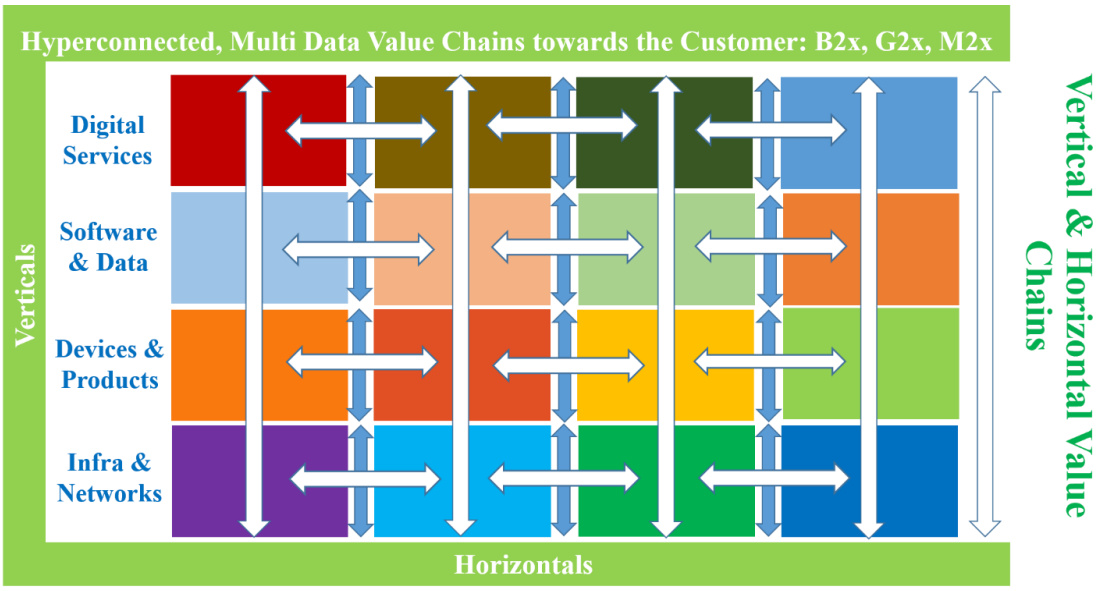

Figure 1: Hyperconnected, vertical and horizontal value chain [1]

Figure 1 illustrates the complexity of the ecosystem. If a consumer is placed at the very end of the supply chain (downstream), it becomes apparent that numerous different parties located up the stream participate in providing manufacturing and assembly of all software and hardware parts, as well as the functioning of the device on the digital network.

In addition, IoT devices themselves also represent highly complex value chains, connecting various hardware and software components together, while being connected to and communicating with one or more networks and other devices. This accounts for situations in which a user may not always have a good and complete understanding of what actions the device carries out, how it works and more importantly, what a device is capable of doing and the way it works within the ecosystem. As a result, situations may arise in which damage occurs without the consumer even knowing how the damage has occurred and what the cause has been.

The data value chain reflects not only the existing value, but also the value that can be derived for economy and society at large. In other words, data value chains place emphasis on the potential of data, rather than on the data per se, that may result to the addition of several layers of value on top of the original raw data, both private and public.

Given the central role of data for IoT data value chains, it should be noted that this document endorses the definition of data under ISO/IEC 2382-1, considering data as "a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing." It is, thus, needed that *"Data should not be treated as a four-letter word. The concept of data encompasses data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with cloud services and/or cloud computing, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as other human readable or machine-readable data"* [20].

Moreover, given that data value chains are non-linear, there can be continuous use and re-use, which creates a series of challenges of legal and strategic relevance to be partly discussed under this deliverable as well as under the forthcoming deliverables due under "Work Package 05: IoT Policy Framework - Trusted, Safe and Legal Environment for IoT." This aspect of non-linearity

allowing continuous use and re-use is captured by the concept of "lifecycles" that will be extensively used in the present analysis in relation to devices, stakeholders, data and law.

In particular, the **IoT Device/Product Life Cycle** is used to capture whether and how long whether a device/product can remain connected to an IoT ecosystem in a secure, safe and compliant manner. It also refers to what the user/customer expects, and how both the device/product and the user/customer are able to keep up to date with (at least) the state of practice. The different stages of the IoT device lifecycle are further captured in the figure below.

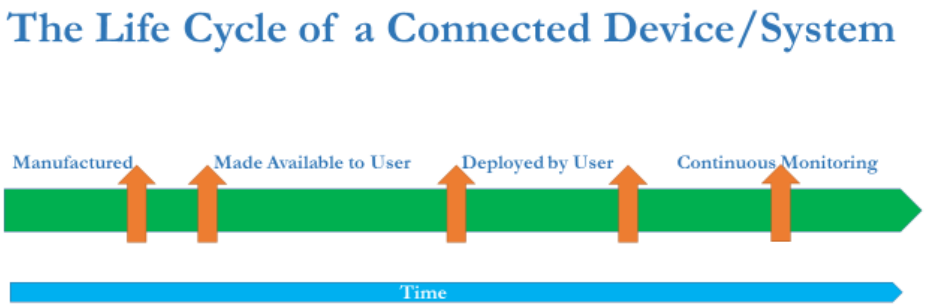

Figure 2: The Life Cycle of a Connected Device/System

The **Stakeholders Life Cycle** refers to the entire spectrum of stakeholders with a role in relation to an IoT device/product. This lifecycle provides the ground for attribution of responsibilities – also, allowing for changes in initial dynamics - and, consequently, what happens in case an incident incurs within an IoT ecosystem. Stakeholders Lifecycle also implies keeping stakeholders up to date.

The **Data Life Cycle refers to the data collected,** created or otherwise concerned and to the way that these data can be segmented, minimised and isolated. The data lifecycle further paves the ground to determine what happens if data have multiple classifications or if these classifications change. The figure below captures the distinctive phases of the personal data lifecycle.

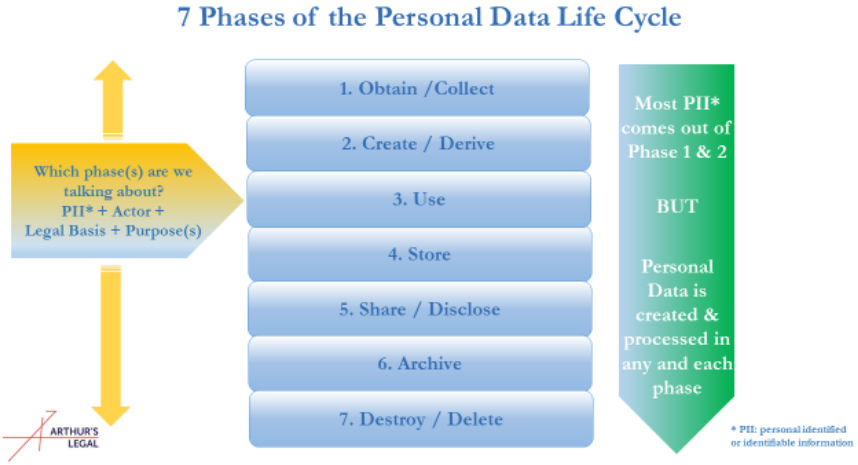

Figure 3: 7 Phases of the Personal Data Life Cycle

Contextual Life Cycle refers to the specific context that a device/product is being used and the persona under which a stakeholder acts with respect to the specific device/product. The contextual lifecycle is taken into account when allocating responsibilities (e.g. who is accountable in what context) and, similarly, how to make stakeholders aware of changes in best practices, rights and obligations when the context changes, as well as how to secure the rights and obligations of the other relevant stakeholders.

Finally, **the Legal Life Cycle should be conceived on the basis of all the earlier mentioned lifecycles.** It refers to person or legal entity, with whom another person or legal entity wishes to

engage and, if this is the case, what are the steps to assess, prepare, negotiate, conclude, execute, operate, update, amend, escalate and terminate such an engagement and, in essence, legal relationship.

Note that there are natural interdependencies in the IoT environment between all the earlier stated lifecycles, in the sense that the issues that impact upon on the IoT data lifecycle are relevant for the stakeholders' lifecycle; changes in data classification may create an impact on the distribution of responsibilities between stakeholders. The same applies to the responsibilities emerging from the meta-data and derived data.

This document is addressed to IoT European Large-Scale Pilots Programme partners as well as the broader community of the IoT stakeholders. The deliverable forms the initial report that precedes the final IoT data value chain model due in December 2019.

2.2 Contributions of partners

AL is the task leader of "Task 05.02: Data in the context of IoT applications". AL coordinated the activities in this task and produced the overarching roadmap addressing key aspects in relation to IoT Data Value Chains such as the latest regulatory developments (eg. draft Regulation on the Free Flow of Data) and the role of liability and transparency for the sustainability of trustworthy IoT Data Value Chains. Moreover, Arthur's Legal provided background information concerning fundamental issues relating to this discussion including the introduction of the distinctive phases of the personal data lifecycle.

IDATE provided an analysis of the chain of markets of IoT Data by looking at the economic value chain. The analysis looks into the general, horizontal, value chain of IoT data, as well as more vertical analysis focused on key verticals of the Large-Scale Pilot projects (health, automotive). The power structures of the value chain and key players are presented. IDATE also provided an analysis of the economic feasibility of data monetization in the IoT domain. This analysis concentrates on the main opportunities and barriers toward monetization and present the potential of new revenues streams.

SINTEF contribute to solutions related to data value chain, data classification, data life cycle, identity and access, management, data access, digital rights management, security, data management and data protection with a cross-domain IoT approach as part of the Digital Single Market strategy. The work considers the policies of data management for IoT applications that are context-aware and situational, and thus more complex to identify and assess, while data protection and security risks depends on the context and the purpose of the objects that are considered (e.g. health, geolocation autonomous device, etc.).

Note that it is intended that the rest of the project partners formally involved in the relevant task will make use of the allocated resources for the delivery of the final report due in December 2019.

2.3 Relations to other activities in the project

The discussion on IoT Data Value Chain Model is relevant for all activities falling under the scope of CREATE-IoT project. As data present one of the building blocks of IoT ecosystems, an IoT Data Value Chain Model stands at the core of the IoT debate.

As has been mentioned earlier, IoT ecosystems are extensive and actions within can have far-reaching consequences. It is important to consider these from the perspective of each individual Large-Scale Pilots as well as from broader and cross-cutting perspective of CREATE-IoT. The analysis of the IoT Data Value Chain requires a holistic approach, that incorporates numerous relevant perspectives, including technological, economical, as well as legal.

The analysis presented within this deliverable cancan contribute to other deliverables of WP 5 on "IoT Policy Framework - Trusted, Safe and Legal Environment for IoT". In addition, certain topics have also been identified of particular relevance for related Work Packages, namely WP 4 on "European IoT Value Chain Integration Framework" and WP 6 on "IoT Interoperability and Standardisation ".It is, also , closely linked to the discussion on the IoT Policy Framework produced under "D05.01 IoT Policy Framework" given that certain elements of the policy framework (e.g. Data Life Cycle, Device Life Cycle etc.) constitute main traits of the IoT Data Value Chains to be discussed.

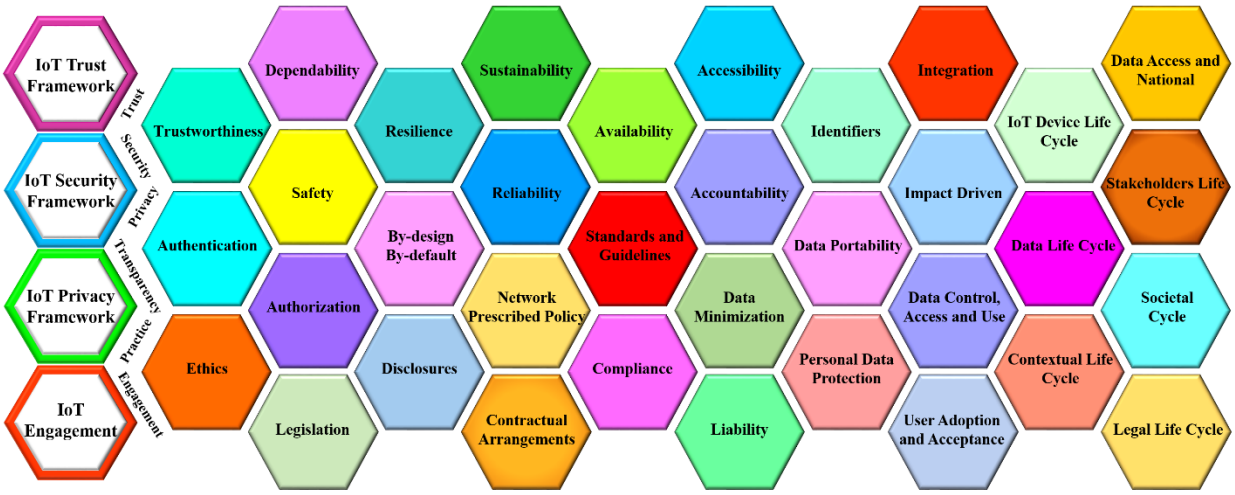

Figure 4: IoT Policy framework elements view[2]

[2] See also Deliverable D05.01 on "IoT Policy Framework".

3. THE MAIN TRAITS OF THE IOT VALUE CHAIN

This chapter deconstructs the IoT Value Chain into its constitutive chains, expanding on the markets involved revealing the economic value chain and identifying the set of actors involved. The analysis explains the data relation flows involved and briefly touches upon how these chains may interact[3].

3.1 Chain of markets

As mentioned earlier, the value chain of data within the IoT field can be observed from two different angles; a horizontal approach and a vertical approach. The former approach could be thought of as the conceptual framework for IoT data (in this case the data being created through IoT platforms), which provides the foundations for how data is passes along the chain. The latter approach, looks at the specific value chains in in any given vertical. Both of these approaches will be considered further in the paragraphs that follow.

3.1.1 The horizontal value chain (generic use of IoT data)

3.1.1.1 Vast ecosystem mainly from IT and software sectors

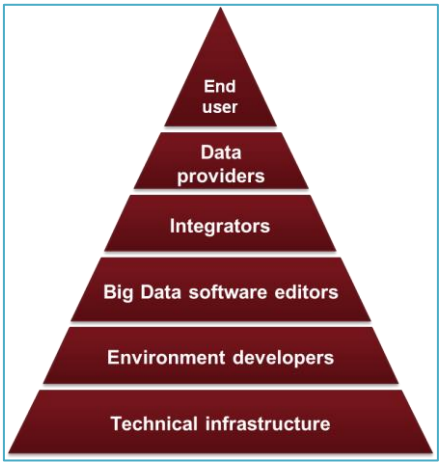

Figure 5: Big data value chain [3]

In relation to the conceptual framework for IoT data, different categories of actors are involved in implementing the technology:

- **Data providers**: These are companies and organisations that provide free and/ or paid data sources[4]. It can include social networks, public administrations or private businesses that provide access to some of their own data. These players do not necessarily send their data; they can simply make them available through APIs.
- **Integrators** offer businesses the opportunity to build an application which meets their own needs and then 'integrate' or install it on the server of the customer. These applications typically operate with multiple elements of a company IT system. For example, an application can automatically extract data from the customer database and subsequently analyse it with a big data 'integrated' application.
- **The big data software editors**, generally using a development environment, will offer different types of applications to analyse or 'draw' the data. In addition, some vendors are developing business intelligence software that enables the end client to make strategic

[3] A more elaborate discussion will be provided under the final deliverable due in December 2019

[4] In the form of single or multiple streams

decisions. For example, analysis of data may show that a particular demographic tends to gather at a given location at a given time, aiding marketing campaigns and decisions.

- **Environment developers**: In order to develop an application, it is often necessary to use a development environment. This facilitates developing the application and is intended to allow it to perform such specific tasks as parallel computing and management of very large databases. Hadoop is one example of a big data environment based on distributed computing.
- **Technical infrastructure providers** include all stakeholders providing infrastructure for big data technologies. It can typically be a telecom operator providing Internet access and a server manufacturer, on whose equipment big data applications will be installed. Data centre builders are also included in this category.

3.1.1.2 Major players are IT and software companies rather than pure big data players

Today, over one hundred players claim to be working in the big data field.

The pioneers of big data are actually players from scientific research and major Internet companies, including Google, Amazon and, more recently, Facebook who have used very large amounts of data as a core part of their businesses since inception. Among the major names covering the complete big data value chain are Oracle, SAP, IBM and Microsoft.

They have either developed proprietary technologies for mastering such data or they are specialised players in data processing through data mining, business intelligence and database management.

Figure 6: Big data landscape [3]

Competition is already considerable on lower stacks of big data due to standardisation (Hadoop's open source platform has contributed to this) and the extension of traditional infrastructure providers and integrators. No single player has a clear leadership position.

Despite this considerable competition in the lower stacks, most of the value is captured by the data providers, who generally keep control of their most valuable data. Internet giants dominate this field of owning data, plus to a lesser extent, retailers, telcos and banks.

3.1.2 The vertical value chain (vertical specific value chain)

Following are examples of vertical value chains of the IoT markets in "connected healthcare" and "connected cars".

3.1.2.1 The connected healthcare value chain

Across the value chain of connected healthcare, the data life-cycle is a core issue, since data silo and security concerns have historically been severe challenges for the highly-regulated health sector. Connected devices and services hold significant potential to generate value by developing and placing "new generations" of sensors on the market for both caregivers and patients, and by providing new business opportunities around emerging services such as telemedicine, remote monitoring and home-care delivery respectively. The reduction of readmission and overall care costs, and the optimisation of the care path and efficiency are also of great interest, not just to the public health authorities, but to private health sector stakeholders too.

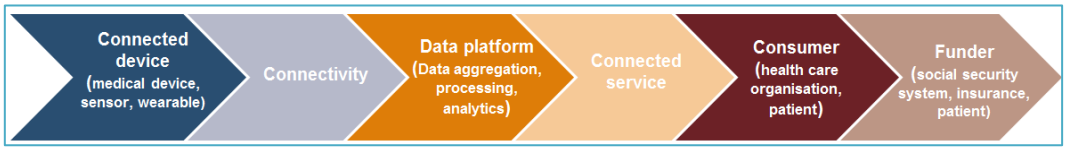

Figure 7: Healthcare value chain [4]

Where connected healthcare differs from other connected markets is that the funder, which may be a public health authority or a private health provider or insurer (i.e. not necessarily the end user / patient), plays an essential role in propelling the market's progress. In some markets, such as home monitoring, the technology adopter may be the carer of the patient.

3.1.2.1.1 Medtech companies reign supreme

The position of the medtech companies in health industries is firm, and not at all likely to be shaken in the near future, as their initiatives are spanning out across full range of products and services. Medtech companies have inherent advantages over others in medical device/sensors development and in their knowledge of regulatory affairs, care delivery paths and care providers' working modalities. By comparison, Internet players are intervening in this market in a relatively subdued way. Their main purpose here is to seize opportunities out of their core business – Apple and Samsung are all seeking industry partners for health-related research by intermediating on the hardware-generated data. Google goes further by developing its own biotechnological products and services through its Verily and Calico divisions.

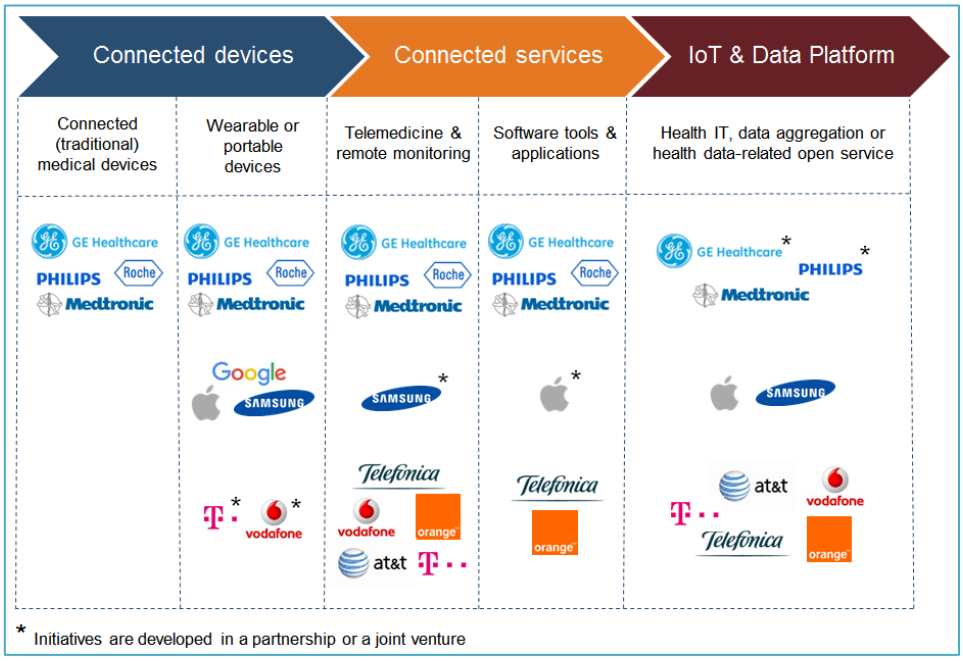

Figure 8: Initiatives by giant players in connected healthcare market

Telcos are active in this promising market and regard connected healthcare as an essential part of their IoT strategies. They have, though, adopted a wait-and-see approach. Their main initiatives

refer to the "connected hospital" topic. The new and rising application is in remote patient-monitoring products, through a wholesale approach.

More generally, telcos are developing services for healthcare often through a specific division. Vodafone appears to be the most advanced player, while DT positioned itself early on and has interesting credentials. The majority of models are logically B2B2C solutions.

Security and fluidity of health data among different stakeholders is another key element to propel the connected healthcare market, driving more corporation between telcos, other ICT actors and medtech players to build open data platforms and services.

3.1.2.2 The connected car value chain

The figure below illustrates the whole automotive value chain including the main players.

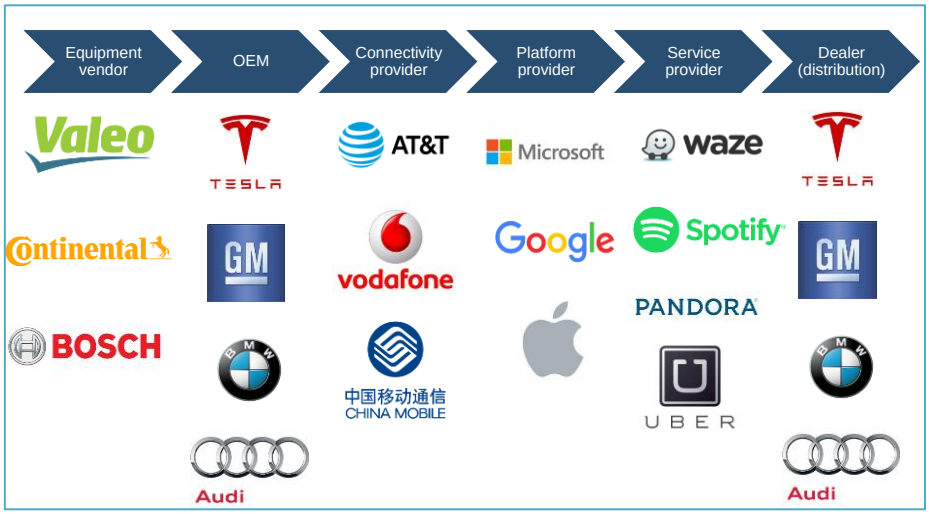

Figure 9: Initiatives by giant players in connected healthcare market

3.1.2.2.1 Premium brand car manufacturers leading the way

It is no surprise that the premium brands are leading the way in the connected cars market. Their service portfolio is broader and more innovative by far. Moreover, their clientele is the most willing to pay for such services. The brands have implemented an embedded architecture to provide the best services in terms of QoS.

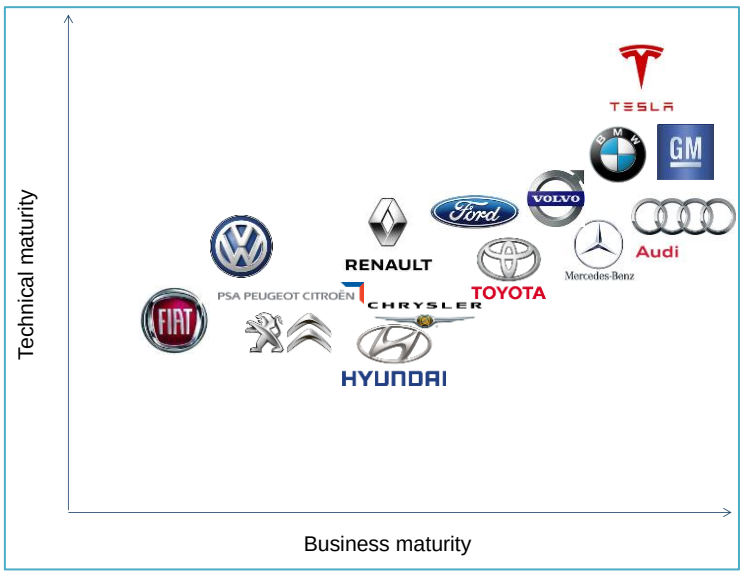

Figure 10: Main positioning of car manufacturers regarding connected-car market [3]

3.1.2.2.2 Main connectivity providers

All telcos are very involved in the automotive space. For them, the automotive and related connected-car topic is a top priority driver in their M2M and IoT strategy mix. Many regulations throughout the world will impose the presence of a dedicated SIM card in each vehicle.

In this, AT&T and Vodafone have a clear leadership. If wholesale rules, AT&T stands out with its B2C business model, through different business models including the integration of the car into a share plan.

- Both provide global SIMs which simplifies sourcing for manufacturers as they look at a global approach rather than a series of local SIMs from multiple telecom operators.
- AT&T and Vodafone also both provide vertical services (beyond connectivity services). The AT&T Drive platform and the recent Vodafone acquisition of Cobra has also generated significant interest from the automotive industry: both have multiplied their partnerships in the recent past.

It is also worth noting that China is a specific market and therefore China Mobile is seen as a key partner in this region.

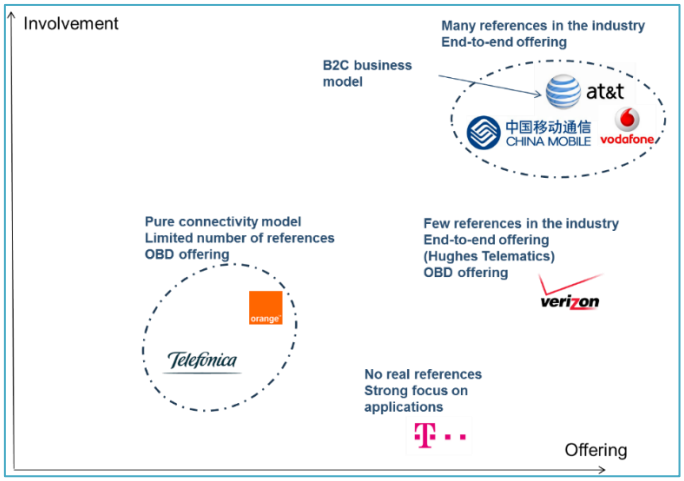

Figure 11: Key differentiation in carrier positioning in the automotive market

3.1.2.2.1 Main Internet player strategies

In the automotive market, Google seems to lead among the players under review here, as they provide not only a wealth of building blocks but even a car itself – in addition to being highly involved in the R&D automotive space. In terms of communication, Apple is also very involved with CarPlay and has been at the centre of rumours concerning the potential purchase of a car manufacturer, although at present its offering does not go further. Other OTT players are strictly positioning on the platform and application layers.

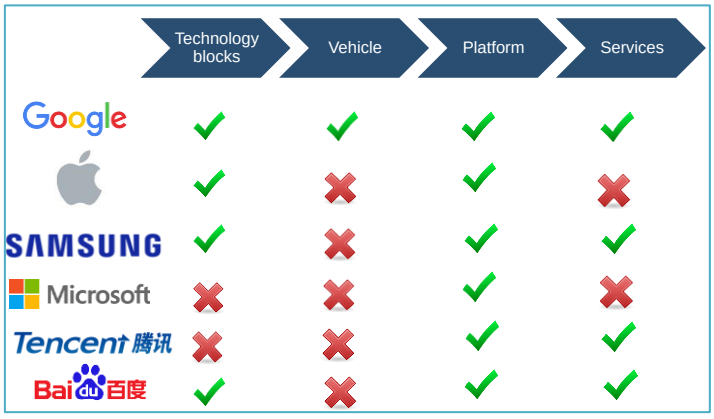

Figure 12: Key differentiation in positioning among Internet OTT players in the automotive market

3.2 Chain of data relation flows

On the free flow of data, it can be established that restrictions on the free movement of data within the European Union and unjustified restrictions on the location of data for storage or processing purposes are generally not addressed in generic IoT products and services.

This is understood as most restrictions are only applicable to certain industries, markets or use. It is however a main challenge as hyperconnected ecosystems are borderless and the data therein should be able to flow freely and unrestricted, at least within the European Union. Quite a few member states have implemented sector-specific rules and regulations that differ per member state, thus hampering the DSM (Digital Single Market) and limit the competitiveness of European manufacturers, service providers and other vendors and their ability to benefit from marketing respective products, services and data across borders.

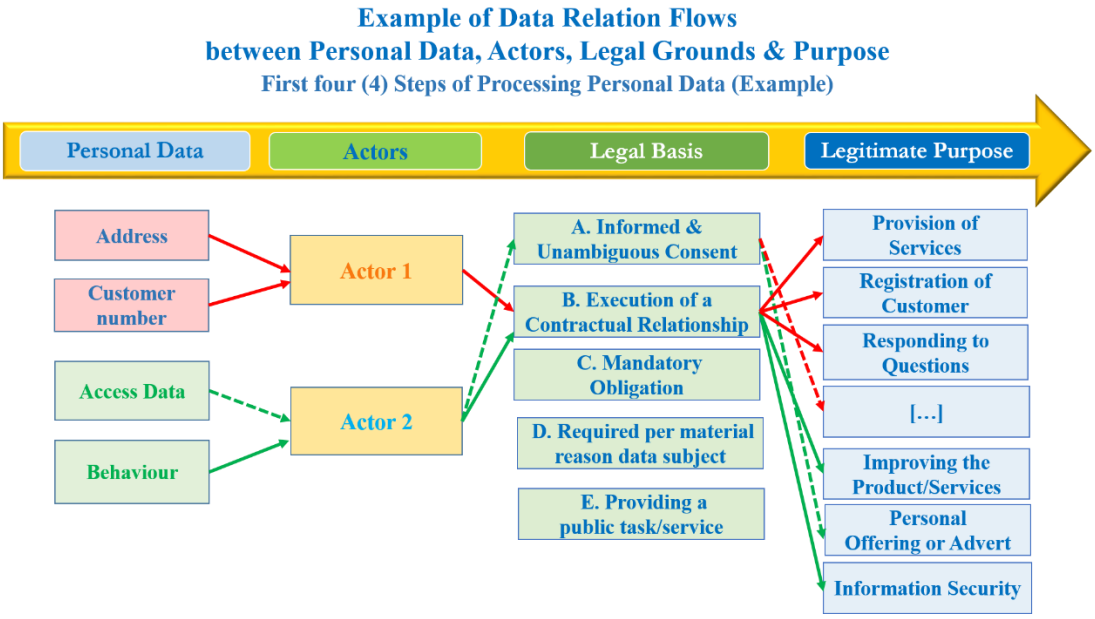

Figure 13: Example of Data Relation Flows between Personal Data, Actors, Legal Grounds & Purpose [5]

Note that currently only personal data is allowed to freely flow across EU Member States. The recently published draft Regulation on the free flow of non-personal data [6] aims to lift the existing barriers, also, discussed under the following chapter of this deliverable.

3.3 Chain of triggers

IoT devices are usually not operated in safe environments. It is therefore possible for hackers to access or obtain such devices and attempt to locate the key data on their microchips. In addition, due to the hyperconnected nature of the IoT environments, gaining access into an individual device, hackers may also access other connected devices and the network.

As the devices in an IoT ecosystem are connected to each other, communication between them often takes place rapidly, without human interference. This also means that any incident compromising security of a device may trigger a security compromise of other devices. The extensive degree of interdependencies creates high risk of a domino effect of different consequences potentially relevant for all value chains discussed. In other words, security risk in IoT ecosystems is diffused, as opposed to isolated.

The emerging risks and their multiplication is, of course, of great relevance, also, from a legal standpoint, and it will, therefore, be extensively addressed under the forthcoming deliverables due under WP 05. It has been argued, though, that "all other risks, liabilities and other elements, which could not be defined by legislation, standardization and agreement should in best case scenario be

covered by insurance" in order to create sufficient guarantees for the IoT market [5]. In practice, insurance covers know risks and this approach is unlikely to afford protection to start-ups and SMEs developing new IoT products and services.

Incidents occurring in the cloud computing domain may well serve as an example of harm being diffused. In case of an intentional or unintentional incident, files containing data may be affected. This may cause downstream applications or systems relying on the affected files may cease to work properly. As a consequence, the consumer is likely to suffer harm. While this harm may in some cases be expressed in monetary terms, certain harms cannot always be adequately remedied by monetary damages, such as the consequences of data protection breaches, for example [7].

An in-depth assessment of security risks inherent to a device which becomes a part of an IoT ecosystem is essential. In carrying it out, one must first carry out a security analysis, e.g. identify the threats, the assets to be protected and the level of desired security also has to be decided. The challenge is that the developer/actuator might not know in which system or environment the device will later be used. This can be countered effectively by introducing a classification (or certification) system that would certify devices for use in particular use case scenarios depending on the level of risk. With this type of system, it would be possible to prevent devices entering the market without the appropriate security.

Note that the introduction of a certification system as a means to prevent proliferation of risk in the IoT environment will be discussed extensively under the final deliverable due in December 2019.

4. THE EMERGING LEGAL CHALLENGES OF DATA FLOWS

This section produces an overview of the relevant challenges from a legal point of view linking to data flows and, thus, relevant for the IoT Data Value Chain. These challenges either relate to this specific momentum of the European regulatory scene or are innate to the very nature of data flows. Note that a more elaborated discussion on the related legal challenges will be produced under the deliverables due under "Task 05.03: Legal support, accountability and liability."

4.1 The changing regulatory landscape

It is apparent that the EU lawmakers have started taking initiative again and following years of preparation and laws lagging behind technology developments, their efforts are likely to bear some fruit soon. The first five months of 2018 will see the entry into force of three very important pieces of legislation and hopefully some rapid progress being made on the e-Privacy Regulation front. It is important that organizations of all sizes remain vigilant and adjust their approach to the issues in question accordingly. Just as it is important for the EU lawmakers to monitor the implementation process, enforce the new rules and quickly release further updates where needed with due regard to the impact frequent changes can have on SMEs.

Although technology and innovation tends to be considerably ahead of legal regulation, European lawmakers have taken steps to catch up on regulating the recent technology developments. As a result of their efforts, numerous legislative acts will enter into application in the first five months of 2018, as further updates to the related laws are expected along the way. The discussion below points at the most relevant for the IoT domain.

Figure 14: From 2018, Digital & Data become Highly Regulated Domains

General Data Protection Regulation (GDPR) [14]

Entering into application on 25 May 2018, GDPR is currently in the spotlight and receiving much attention from organizations as well as governments around the world. This is not surprising, since it places obligations upon everyone handling personal data of EU citizens, irrespective of where the data is collected, stored or processed. Given its rather consumer-focused character, the Regulation considers privacy and processing of personal data of natural persons a fundamental right. While emphasizing key principles related to the processing of personal data, including lawfulness, fairness, transparency, data minimization and accountability, the Regulation grants numerous rights to users (data subjects). These include the right of access by the data subject and the right to be forgotten.

GDPR takes a more stringent stance towards data protection and security requirements by requiring organizations to assess the level of protection from a wider perspective. The GDPR offers an equation for finding the appropriate level of protection, per purpose, per impact assessment, et cetera. The level of having state of the art security measures (both technical and organizational) in

place is the benchmark in the GDPR, where (i) the related cost of implementation, (ii) the purposes of personal data processing and (iii) the impact on the rights and freedoms of the data subject (also good, bad and worst-case scenarios) need to be taken into account, whether one is either data controller or data processor. We call this the appropriate dynamic accountability (ADA) formula:

State of the art security – Costs – Purposes + Impact

The GDPR aims to ensure up-to-date levels of protection by requiring the levels of data protection and security to continuously meet the ADA formula. Failure to comply with the Regulation may result in some hefty penalties which may to amount to several billion Euros for some large enterprises, since the Regulation allows for penalties of up 4% of the total worldwide annual turnover.

Directive of Security of Network and Information System (NIS Directive)) [15]

While the GDPR focuses on privacy, NIS Directive aims to achieve a high common level of security of network and information systems within the EU by improving cybersecurity capabilities at national level, increasing EU-level cooperation, and setting out risk management and incident reporting obligations for operators of essential services (banking, energy, transport, financial market infrastructure, health, drinking water and digital infrastructure) and digital service providers (online marketplaces, online search engines and cloud services). Operators of essential services and digital service providers are tasked with ensuring the security of their networks and systems to promote a culture of risk management and ensure that serious incidents are reported to national competent authorities and computer security incident response teams (CSIRTs).

In case of a "significant" impact on the provision of the operator's service, the operators of essential services will have to notify the national competent authorities. Digital service providers will have to notify any incident having a "substantial" impact on the provision of the service. Notification processes have also been put in place to ensure effective communication of incidents across members states' CSIRTs. In order to support and facilitate strategic cooperation and the exchange of information between member states, the Cooperation Group has been established, consisting of representatives of Members States, European Commission and the European Union Agency for Network and Information Security.

The complex institutional ecosystem set out by NIS Directive shall be in place by 9 May 2018 when the Directive enters into application. Therefore, Member States have until then to transpose the Directive into national laws, while having been offered additional six months (until 9 November 2018) to identify the operators of essential services.

Payment Services Directive 2 (PSD2)

PSD2 entering into application on 13 January 2018 addresses better integration of internal market for electronic payments. It puts in place comprehensive rules for payment services, with the goal of making payments between Member States as easy, efficient and secure as payments within a single country and equating costs. By setting out strict security requirements, transparency and the rights and obligations of users and providers of payment service, PSD2 seeks to open up payment markets to new entrants leading to more competition, greater choice and better prices for consumers.

In addition, the Directive aims to open up the EU payment market to companies offering consumer- or business-oriented payment services, in particular account information services allowing users to have an overview of their financial situation, and payment initiation services allowing consumers to pay via simple credit transfer for their purchases.

From the consumer point of view, it is also important to note that the Directive significantly reduces consumers' liability for non-authorised payments, introduces an unconditional refund right for direct debits in euro and puts in place an obligation to remove surcharges for the use of a

consumer credit or debit card. A user-friendly leaflet on all consumers' rights is expected to be published by the European Commission by early 2018.

Proposal for Regulation on Privacy and Electronic Communications (e-Privacy Regulation)

Finally, it is worth noting that both the European Commission and the European Parliament have recently initiated steps with the view of updating rules relating to privacy and electronic communications, and reinforcing trust and security in the Digital Single Market. Having identified areas to be addressed (including stronger protection online, simpler rules on cookies, and transparency on direct marketing, to name a few), the Commission released a Proposal for the Regulation in January 2017.

In June 2017, the Parliament's Committee for Civil Liberties, Justice and Home Affairs (LIBE) published a draft report on the Commission's Proposal. Overall, the resulting text of the Regulation strengthens privacy protection for individuals. Amongst others, it provides clarity regarding what legitimate grounds for processing prevail if both the GDPR and the e-Privacy Regulation apply to a processing operation, and prohibits all further use of electronic communications data collected under e-Privacy rules. In addition, significantly stronger obligations for privacy by default are proposed, including end-to-end encryption (with no backdoors) proposed as a security default measure for ensuring confidentiality of communications, and a national Do Not Call register for opting out of unsolicited voice-to-voice marketing calls. Finally, the amendments provide for an extension of the principle of confidentiality of communications to machine-to-machine communications as well as enhanced definitions of "electronic communications metadata" and "direct marketing".

The Committee's decision on the adoption of the proposal is shortly expected. If adopted by the Committee and later by the Plenary of the Parliament, the Parliament will then sit in the trialogue together with the European Commission and the Council, and agree a common position.

4.2 The existing localization restrictions within EU

The discussion on IoT data value chain, and consequently data flows, is closely inter-linked to the discussions at EU level regarding the free flow of data. The free flow of data is highly relevant for the IoT domain, as data is what actually keeps the IoT moving and alive. The free flow of data concerns data in any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or within the IoT. It includes, amongst others, proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as all other human readable or machine-readable data.

Despite the de facto need to liberalize flows of data, the current legal regime governing data flows is highly rigid and fragmented. More specifically, and as has been mentioned earlier, a significant number of Member States have implemented their own sector-specific rules and regulations.[5] These rules impose, in essence, data localization restrictions inhibiting the free flow of data within EU and will in effect stop the Digital Single Market from becoming a reality.

In particular, there is a plethora of data location restrictions within the individual Member States, as well as an amplified set of diversified approaches at national level, which are often largely unreasonable or highly disproportionate. This plethora of data localization restriction results from the absence of well-defined standards and practices at the level of the European Union, while the absence of well formulated standards fosters further the implementation of data localization

[5] Note that an extensive discussion concerning the existing data localisation restriction across Member States falls outside the scope of the present deliverable. A more extensive discussion on the free flow of data within the Digital Single Market will be provided under the upcoming deliverables falling under Task 05.03 on "Legal Support, Accountability and Liability".

restrictions, thus, catching market players in a vicious circle. The plethora of regulatory instruments relating to the scope of the aforementioned consultation, including the Software Directive (91/250/EEC), the Database Directive (96/9/EC), the Trade Secret Directive (COM/2013/0813), the EU Antitrust legislation, the E-Commerce Directive (2000/31/EC) and the Unfair Terms in Consumer Contracts (93/13/EC) Directive.

All these instruments of European law due to their nature as Directives are transposed in the national orders by virtue of legislative instruments of all kind, thus, adding complexity and discouraging companies expanding their business in other Member States. Those restrictions mostly relate to the handling of financial data, tax data, health data, and book keeping data, gambling data, banking, as well as public procurement at national & local level. For instance, in the Netherlands public records -both paper and electronic- have to be stored in archives in specific locations in the country. Furthermore, there is often a lack of common understanding and culture in key matters across sectors and Member States. Data localization restrictions bring about the absence of a harmonized understanding as companies processing data across different Member States face increased administrative burdens and need to comply with different legal systems.

Note that at the moment that this deliverable is being drafted European Commission released its proposal for a Regulation on the free-flow of non-personal data [6] that is of high relevance for the IoT domain and which will, therefore, be covered under the forthcoming deliverables due under "Work Package 05: IoT Policy Framework - Trusted, Safe and Legal Environment for IoT".

4.3 The outdated definitions: the consumer protection paradigm

The Directive 85/374 [16] constitutes the European legal framework proving for the protection of individuals in case of liabilities incurred by the use of defective products. Notwithstanding its noble goal of consumer protection, the previously mentioned directive was clearly written with consumers who only make use of standalone material products. There is a real need for it to be adapted into the current consumer environment in which software forms part of smartphones, as computers and as a (key) component of (domestic) devices.

In this respect, there is a series of challenges concerning the liabilities incurred by the use of the devices and services in the IoT domain. In particular, first, IoT devices and services can be subject to unauthorised access by third parties (individuals or machines) which could tamper with such device or service; second, sensitive (personal) data could be stored, processed or exchanged in an unauthorized manner and thereby breach the rights of a data subject (person); third, malicious data can be created/deducted by one IoT device and be exchanged with other IoT devices (and may there cause further harm); finally, this malicious data could lead to a malicious decision which could cause damage to other (IoT) devices or a human being.

Consequently, these triggers a series of questions regarding:

- What or who actually caused the damage and
- Who is liable for such damages?

Providing answers to these questions is complicated as the related applicable definitions are essentially not fit for the IoT environment. In particular, under the product liability directive, all movables are considered as products (even if incorporated into another movable or immovable) including electricity. The damages link to death or personal injury, while the injured person is requested to prove the damage, the defect and causal relationship between defect and damage.

It comes, thus, as no surprise that the European Commission under the Digital Single Market Strategy underlined the need for legal certainty on allocation of liability for roll-out of IoT.

4.4 The contractual complexities

This section gives an overview of the emerging contractual complexities in the IoT environment. Note that an extensive analysis of those will be provided under the deliverables falling within the scope of "Task 05.03: Legal support, accountability and liability."

IoT devices encompass and consist of numerous layers including hardware, software, data and service. This multi-layered structure often requires numerous different manufacturers and providers to participate in the production of the device as well as in the provision of services during its life time. This setting accounts for a large number of contractual documents, licences, notices, declarations and/or reports to be in place and effective, not only between the supply-side actors themselves, but also vis-à-vis the customer.

The resulting relationships tend to be very complex and bear a great deal of challenges in achieving transparency in allocating responsibilities and risks, as well as issues concerning jurisdiction and remedies. This section aims to address some of the most relevant challenges while noting that it only serves as an indicative overview as it will be treated more extensively in other deliverables related to this topic.

One of the main challenges customers are repeatedly faced with is the difficulty to understand applicable contracts, agreements and other legal documents. Numerous reasons account for this issue, but for purposes of further discussion it is mainly worth noting that, aside from the European versions of contracts often being verbatim reproductions of their US counterparts, (which may not be necessarily suitable), identifying all the applicable documents may be a challenge in itself. For example, in the case of Nest connected thermostat produced by Nest Labs owned by Google, this challenge is illustrated by about 13 legal documents which a user has to read in order to get a "clear" picture of the rights, obligations and responsibilities in the supply chain.

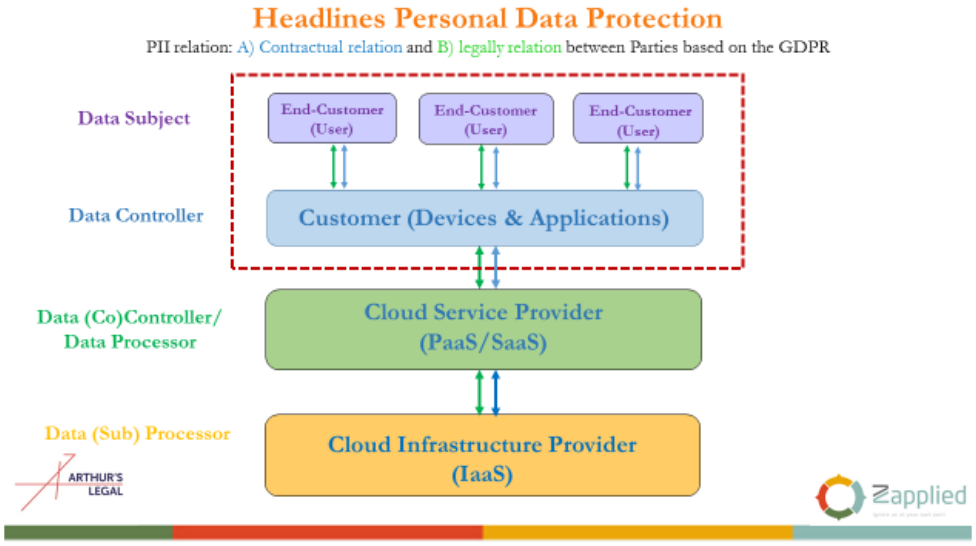

Figure 15: Headlines Personal Data Protection

Having a clear picture of legal relationships between the consumer and individual actors in the supply chain is also challenging from the perspective of the scope of the documents. While they may claim that they are only applicable to one separate part of the IoT device, due to the connected nature of IoT ecosystems it is difficult to imagine a part of the system or a separate layer functioning irrespective of the remaining parts or other layers, i.e. without affecting the whole ecosystem. However, in order to provide the customer with a sufficient amount of transparency, it is essential that the customer has a true and honest account of how the layers (and the respective contractual documents) interact and what supplier becomes relevant (not only active) in what layer. Just as the customer should be able to identify the parties upon whom the service is dependent and who are the processors and sub-processors of data. Not only does this information provide the

customer with greater transparency; it also helps them establish the extent of liability of various suppliers should a problem arise that requires legal redress.

Further questions concerning liability and other complex contractual issues arise in context of IoT devices that have the ability to make autonomous decisions and enter into legally binding agreements with third parties (e.g. connected home appliances purchasing products from third parties). On the one hand, questions of liability for actions of these autonomous devices are inevitable. On the other hand, although our traditional understanding of property is a static one, it is likely that that it will need to change and respond to the dynamic nature of IoT devices which are able to evolve and mature over time.

From a separate perspective, it is also important to consider the status and the role of the customer in the ecosystem. It has been argued that two further distinctions of legal consequence can be made [8]. "First, the end-user may be the contracting customer or a third party, such as a family member. Second, the device itself may be owned by the customer or may be leased to the customer by the supplier (or provided as part of rented or leased premises)." Considering the latter, "the distinction between the device and the associated services becomes critical, because the Nest ToS states that if the device owner does not agree with the terms 'you should disconnect your products from your account and cease accessing or using the services" [9]. However, in some jurisdictions, a disconnected IoT device would potentially breach the law. For example, according to the Sale of Goods Act 1979 of England and Wales, the purchasers of goods will "enjoy quiet possession", which term would be potentially breached if when the Nest device were disconnected it loses most of its functionality.

Last but not least, complexities also arise in the context of clauses relating to selection of jurisdiction in contracts relating to IoT devices. Most commercial contracts explicitly stipulate applicable law and jurisdiction governing them, to the maximum extent permitted by law. However, in cases where mandatory national laws apply, judges will have to abide by those. As a consequence, cases may arise in which the judge will have to apply different pieces of legislation to the same product. Already in today's connected world it is not difficult to imagine a scenario in which a Dutch customer uses a US-manufactured IoT device during their holiday in Tunisia, where the device was purchased in Venezuela, consists of software running in Ireland and uses applications developed by a Chinese company. This presents a very complex setting where different pieces of legislation are likely to apply in respect of aa single device.

5. BASELINE REQUIREMENTS FOR AN IOT DATA VALUE CHAIN

Based on the earlier discussion, as well as on, the existing literature expanding on the requirements for an IoT data value chain model, this section will produce a preliminary IoT Data Model. In essence, this chapter suggests using the traits –and the requirements of IoT Data Value Chains- to extract the relevant properties. The discussion presents an abstract model for reliable IoT Data Value Chains aiming to support and further unleash the potential of existing and future IoT value chains. Building on the earlier analysis, the discussion below addresses the attributes of economical and legal relevance. The final set of attributes will be presented under the final deliverable "D05.04: IoT Final IoT Data Value Chain Model" due in December 2019.

Note that the attributes below are relevant for the associated IoT value chains across all Large-Scale Pilots (LSPs).

5.1 The benchmark scheme for an IoT Value Chain Data Model

The earlier discussion has shown that a hyperconnected society is, in essence, converging with a consumer-industrial-business Internet that is based on hyperconnected IoT environments.

The latter require new IoT systems architectures that are integrated with network architecture (a knowledge-centric network for IoT), a system design and horizontal interoperable platforms that manage things that are digital, automated and connected, functioning in real time, having remote access and being controlled based on Internet-enabled tools. The IoT value cycle and benefit paradigm is presented in Figure 16.

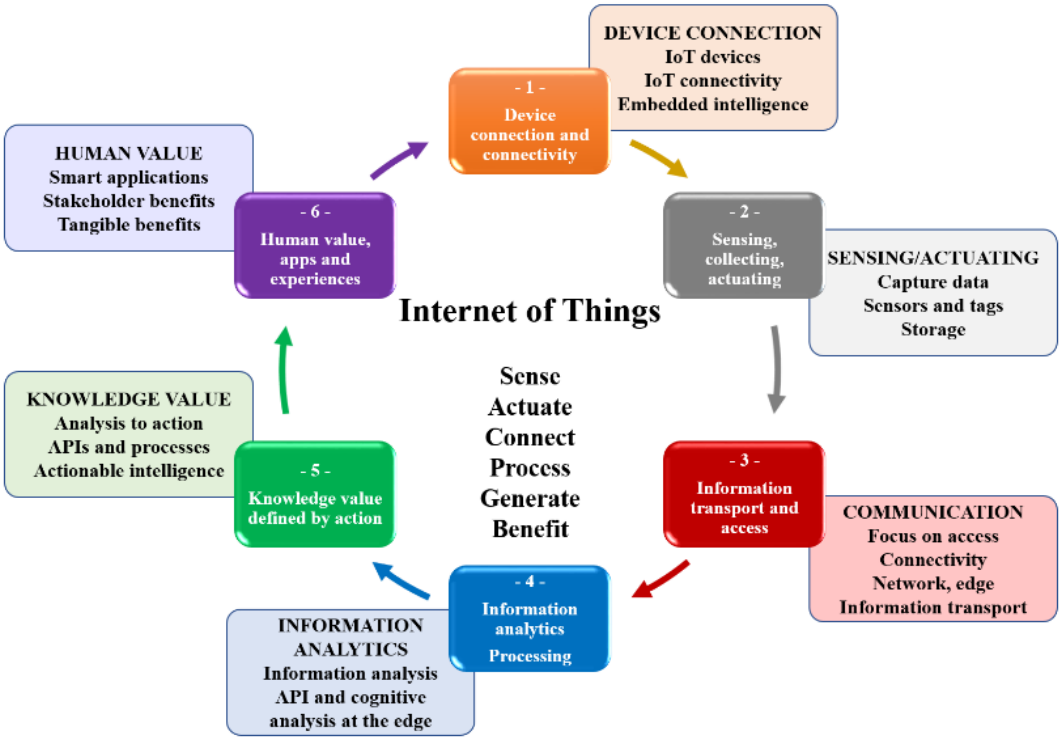

Figure 16: IoT value and benefit paradigm [13]

IoT across industrial sectors, based on knowledge-centric network, context awareness, the traffic characterisation, monitoring and optimisation, and the modelling and simulation of large-scale IoT scenarios all require an IoT Value Chain Data Model that reflects the data flow across the IoT architectural layers as presented in Figure 17.

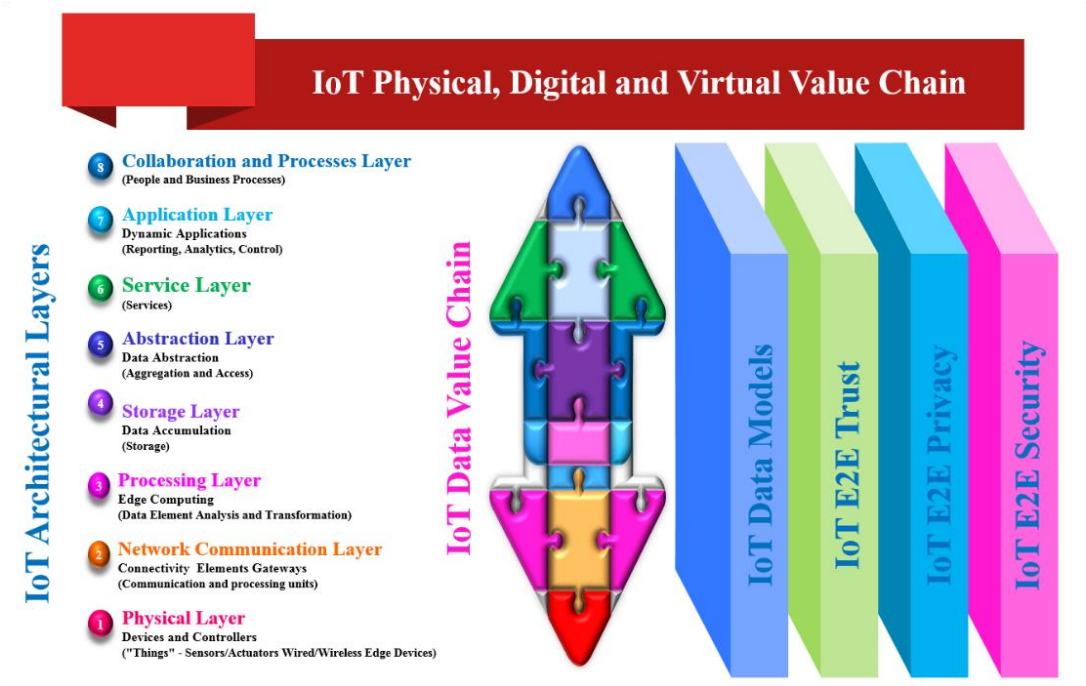

Figure 17: IoT data value chain across IoT architectural layers

The data flow and exchange across the IoT architectural layers is reflected in the IoT Data Value Chain that includes the following processes: data acquisition, data transmission/ingestion, data processing, data storage, data filtering, data analysis/analytics, data integration, data discovery, data usage, data exposure (openness), and data monetization.

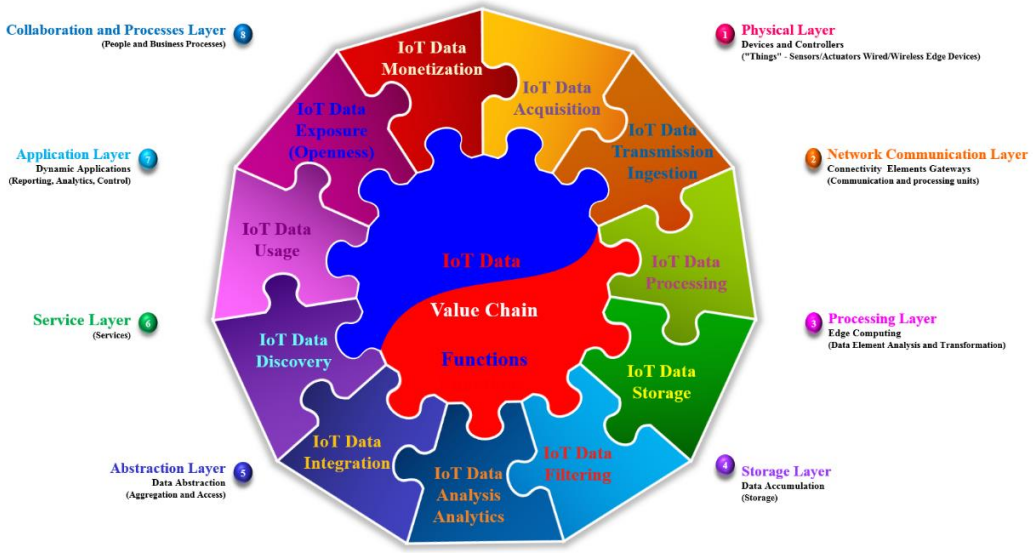

Figure 18: IoT data value chain functions

- IoT Data acquisition – addresses the process of gathering, and formatting IoT data before it is transmitted through different channels/pipelines for ingestion and processing. Data acquisition is one of the major IoT data challenges in terms of infrastructure requirements and edge heterogenous devices/nodes/things.
- IoT Data transmission/ingestion – addresses the communication channels and pipelines for transmitting the IoT data and the ingestion of data for enabling reliable operation of entire IoT platforms using various file formats and network connections while considering frequency, volume, data rates, neutrality, etc.

- IoT Data processing – addresses the processing of IoT data form different sources (sensors, actuators, processes, virtual things, etc.) for transforming the data into a format that facilitates its reuse or enables immediate action based on incoming events and interactions.
- IoT Data storage – provides cost-effective ways for distributed IoT data storage with the choice of format or database technology determined by the nature of other stages in the value chain (i.e. analysis, analytics, nature of applications – safety/mission critical). The IoT data storage assures the persistence and management of IoT data in a scalable way that satisfies the needs of IoT applications that require fast access to the raw or processed IoT data.
- IoT Data filtering – concerns the active management of IoT data over its life cycle to ensure it meets the necessary data quality requirements for its effective usage in various IoT applications across different industrial domains. The IoT data filtering processes include different activities i.e. content creation, selection, classification, transformation, validation, preservation, etc.
- IoT Data analysis/analytics – addressed at every layer in the IoT architecture and every step in the IoT data value chain, allowing the generation of new insights and actions based on the IoT data from various sources and enabled by the tools and IoT platforms used in different applications. IoT Data analysis transforms the raw IoT data into data for use in the decision-making as well as domain-specific usage, through exploring, transforming, and modelling IoT data with the goal of extracting the relevant "smart" data, synthesising and extracting useful "invisible" information with high potential from an IoT application point of view.
- IoT Data integration - combining a variety of IoT data sources to provide new insights, with IoT data integration as a key element for any IoT application.
- IoT Data discovery – addresses the localization and identification of IoT data sources need and the evaluation for different attributes, relevance, quality, integrity, security, privacy, cost, coverage, etc.
- IoT Data usage – considers the IoT data-driven applications that need access to IoT data, its analysis, and the tools and IoT platforms needed to integrate the data analysis within the different IoT applications and use cases. IoT data usage in use cases/applications/scenarios decision-making enhances effectiveness through reduction of costs, increased added value, portability, etc.
- IoT Data exposure (openness) – addresses how IoT data that are exposed to the other IoT applications and IoT ecosystems stakeholders in a way that makes them useful for value co-creation in order to generate value from IoT data from various edge and platforms sources.
- IoT Data monetization – addressing the IoT business models that support IoT ecosystems for determining the value of IoT data provided by different sources and available from different IoT applications and creating new opportunities for growth and economical and social benefits.

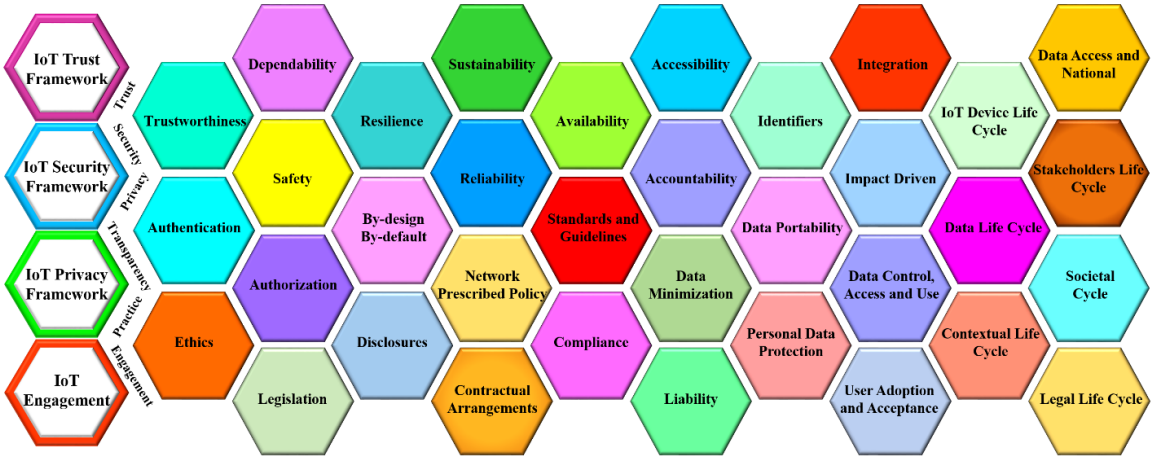

Figure 19: IoT Policy framework elements view

Note that the identification of the aforementioned processes should be placed within the scope of the IoT Policy Framework presented under D05.01 IoT Policy Framework, in the sense that these processes actually specify the related elements captured by Figure 19.

A more in-depth analysis of how the early stated processes relate to the elements of the policy framework and leading further to the abstraction of the associated attributes for an IoT Data Value Chain Model will be provided under the final deliverable "D05.04: IoT Final IoT Data Value Chain Model" due in December 2019.

5.2 Economic feasibility

Companies can revolutionise their business models by cross referencing disparate data from a host of sources (including external sources and IoT generated data) – a process which extends well beyond classic approaches to culling and mulling statistics. The first major applications today are in the area of sales and marketing, by analysing attrition rates and knowledge of consumer behaviour. But the range of possibilities is far vaster: from creating new services and fostering new business models, to optimising processes.

Figure 20: Policy sustainability

5.2.1 Major opportunities for exploiting IoT data for verticals

The data used in these solutions can come from various sources:

- Internal (such as internal databases)
- From data aggregation (forms, documents, sensors, web browsing), and particularly IoT platforms for this study
- From open data sources and APIs from third parties exchanging data (automatic data transfer). Open data and data provided through APIs often have limited value without further transformation from third parties, such as developers, start-ups or other SMEs developing new products or services.

Valuable data is generally blocked/controlled by the owners, as there is a competitive advantage attached to the data itself. This is especially the case with major OTT players like Facebook but also with major IoT players (data is generally only shared with explicit user consent on a case by case basis).

Beyond Internet giants, many vertical players have a wealth of information about millions of users. There are several opportunities for vertical stakeholders to use and share data:

- **Internal use**: data are analysed internally and are not shared with third parties

- **Intermediation for third parties**: data are analysed internally, but the result of the analysis is shared with third parties, whether monetised or not – a way to monetise data without disclosing them
- **Data sales to third parties**: data are directly shared and monetised with third parties. Data will generally be anonymised and sold in aggregated versions.

5.2.2 Main barriers

Most businesses are still struggling to pin down new business models, due to a lack of high-value unstructured data, and go beyond the proof of concept stage.

Added to which there is a plethora of disjointed products available, as IT and IoT companies alike are all trying to ride the wave of media hype, even if it means rebranding their old data processing solutions as big data and/or IoT data products. This plethora of activity only adds to the confusion, although a few major players are starting to emerge, as are concrete examples of a solid return on investment.

The main obstacle to the implementation of data monetisation models is more cultural than technological, fuelled by conflicts between departments and traditional approaches to sharing resources and knowledge, both within and outside organisations. Without a real change in philosophy over how to treat data, the harvest of big data will remain a poor one.

In addition, the fact of centralising data only increases data protection and privacy issues, which means business need to rethink how to manage the plethora of data, but also how to collect data from users who are increasingly reluctant to share them.

Such major barriers can be overcome over time, but this will require organisational and cultural change rather than greater technology literacy. Regulatory and privacy issues will remain important.

The growth of big data market would accelerate significantly if turnkey solutions easily integrating big data technology (likely cloud-based) were provided to extend the adoption from large accounts to SMEs.

5.2.3 The potential of new revenue streams through data monetisation

The two main pillars to generate new revenue through IoT data is by either

- Developing new products and especially new associated services (servitisation – i.e. the capacity to generate recurring revenues not from selling a machine and object but from services); or
- By selling the data to third parties (even where the data remains under the control of the data owner).

With this in mind, there are several potential approaches where vertical players can position to generate more revenues through data:

- More sales of core services. Improvement even by a few percent of conversion rates could bring in significant revenues, especially on expensive products and services.
- Sales of additional paid services on top of existing products and services (i.e. servitisation), sold directly, or commissions of third-party services. Typically, only a small fraction of existing product users will subscribe to these services (between 2 and 20%), but services can reach 5 to 10 EUR per month. The revenues from added-value services may be used over time to reduce the cost of the core product or service and attract more customers (in case of price elasticity).
- Sales of individual data, i.e. one-to-one advertising or marketing, or aggregated data (user data, performance data), namely insights. Players can leverage their entire user base, as they generally rely on anonymised data.

  - Nonetheless, revenues from advertising and insights need to be put in perspective. Revenues per user are generally quite low, even when involving very large amounts of data captured through many services. For instance, Google generates around 3 USD per month per user and Facebook close to 0.5 USD. Newcomers with limited data sets are likely to generate even less, even with brand new data. Insights are just giving patterns of consumption and are therefore even less valuable.
  - Sales of aggregated data allow a player to bypass the most controversial privacy issues, but offer fewer perspectives of revenues, as only patterns can be identified. The approach is therefore not as efficient as targeted advertising and does not allow for real-time interaction.
- Sales of tools leveraging certain types of data such as billing or APIs. Pricing is often independent of the value of the data, but more cost-oriented.
- Intermediaries leveraging data and user control to improve reselling third-party products (such as recommendations, or a platform and kiosk approach).

Verticals may position themselves across all types of approaches, but will have to arbitrate between the various business models, which may require investment, the expected value to be generated by each approach and the competition between models. Indeed, internal optimisation of core products and services can often have greater impact, due to the lack of competition compared with innovative products.

5.3 Liability and transparency

The discussion offered under Chapter 2 focusing on the data relation flow and the proliferation of risk, highlighted specific attributes, also, of legal relevance, namely, liability and transparency that can be of critical significance for an IoT Data Value Chain Model that aims for at a trustworthy and above all human centred IoT ecosystem.

5.3.1 Liability

Liability forms a legal concept closely linked to the notion of responsibility used across disciplines, yet substantially different.

The notion of liability implies an IoT stakeholder's legal responsibility for his actions and/or omissions. Depending on the point of view, liability may also be perceived as burdensome or discouraging for the stakeholder. As it has been argued in this respect, "Liability is the legal obligation (either financially or with some other penalty) in connection with failure to apply the norms." [18] Interestingly, liability links to the notion of responsibility, although being held liable does not necessary presume actual responsibility. For example, the Data Protection Directive that constitutes the applicable data protection framework at EU level considered data controllers as the entities that should be held always liable towards data subjects, even if the actual damage was caused by the data processors.[6]

At this moment of convergence of technologies, markets and stakeholders, the attribution of liability becomes more complex to answer compared to the physical society. For example, [1], a manufacturer of certain objects has to accept and address its respective and proportionate responsibility in the IoT ecosystem its objects are deployed. IoT will bring more responsibility for each stakeholder in the market, and each of such stakeholders will have to think and arrange for those effects in a transparent, diligent and ethical manner. Another example [1] is a security breach in an IoT ecosystem as per insecure coding of software somewhere in the multi-angled value chain. As long as related software companies cannot be held liable, a solid and stable digital economy and society will be difficult to create.

[6] consider [14] as opposed to [19]

Overall, though, it should be noted liability is of paramount importance with the sphere of rule of law, as it forms the emerging consequence of legal obligations created within the context of legal and contractual relationships; the latter are discussed under D05.01 IoT Policy Framework, while being at the heart of the research falling under Work Package 5 on "IoT Policy Framework - Trusted, Safe and Legal Environment for IoT".

5.3.2 Transparency

Transparency has been defined as "the property of a system, organization or individual that provides visibility of its governing norms, behaviour and compliance of behaviour to the norms." [17]. Furthermore, transparency forms one of the essentials of good governance as it allows individuals, organizations, society at large to assess risks and benefits and proceed in making the appropriate decisions. Transparency can either relate to sharing of information or, more broadly, to the adoption of a certain behaviour, before the occurrence of an unwanted event or it may concern informing on the associated consequence, after a certain event has already taken place. In view of materializing transparency in the IoT ecosystem, there are different mechanisms that can be of help to this end, including, the publication of transparency reports by the cloud stakeholders on annual basis and the conclusion of contractual agreements meeting certain criteria that will be briefly discussed below.

In particular, contracts regulating the relationships between IoT stakeholders should provide for a Data Management Service Level Objectives Overview, along the lines of the Service Level Objectives (SLOs) introduced by the Cloud Standardization Guidelines [20]. The appropriate data management SLOs could be assigned with a complementary function to the applicable security and data protection certifications afforded to the IoT stakeholders. Such an approach would mandate the provisioning of SLOs linking to four distinctive categories, namely, a) Data classification, b) Data Mirroring, Backup & Restore, c) Data Lifecycle and d) Data Portability that can be further subdivides to further categories.

Data classification refers to the detailed description of the classes of data involved to the provisioning of a specific service by a specific cloud stakeholder that may include –among other- cloud service customer data, cloud service provider data and cloud service derived data[7]. Should Service Level Agreements provide in a clear manner for the relevant SLOs linking to the particular relationships between the IoT stakeholders, consumers and organizations would be better equipped to make informed decisions, thus, competition would be significantly boosted.

As far as the data mirroring, backup and restoration is concerned, this category refers to the actual mechanisms guaranteeing the online or offline availability of data, in case of failures impeding access to it. These mechanisms falling under the scope of this SLO can be further divided in two widely-used categories (i) data mirroring, (ii) back up/restore.

Data Mirroring refers to refers to the difference between the time data is placed on primary storage and the time the same data is placed on mirrored storage. Furthermore, data back up and restoration refers –primarily- to the list of method(s) employed to back up data and to the time of completion of the back-ups.

As to the data lifecycle, it refers to the effectiveness of the IoT stakeholder's data lifecycle practices, with a special focus on the practices and mechanisms for data handling and deletion.

Finally, data portability –which is highly relevant for the free flow of data within the EU and the strengthening of the Digital Single Market- involves the specification of the data portability format, of the data portability interface and of the data transfer rate [21], as further discussed under the previously mentioned Cloud Standardization Guidelines.

[7] Note that the relevant definitions are provided under the above-mentioned Cloud Standardization Guidelines.

The discussion above aimed at serving as an example on how to increase transparency of IoT Data Value Chains through the provisioning of specific SLOs in the contractual arrangements regulating the relationships between the various IoT stakeholders. Although the discussion has been largely inspired by the cloud environment, it remains relevant for the IoT ecosystem as well.

Bearing in mind the aims of the present deliverable, it should be, thus, noted that the importance of SLOs with respect to transparency of IoT Data Value Chains does not lie so much in the concrete SLOs [20] deemed relevant in the context of specific relationship between cloud stakeholders, but rather on their determination and incorporation per se under a specific contractual agreement.

6. CONCLUDING REMARKS

The present document provided the initial set of valuable insights relating to the creation of a model for IoT Data Value Chains to be further elaborated under the final deliverable due in December 2019.

Recognising the complexity of IoT environments, this document has discussed the emphasis placed by IoT data value chains on the potential of data for the economy and society at large. Although the title of the deliverable suggests the discussion of data value *chains*, the actual discussion revealed that the focus should rather be on the data *value ecosystems,* given that data value chains are basically converging to value networks and more broadly to IoT ecosystems. Furthermore, the discussion has reaffirmed the *n*-dimensional nature of the subject which also accounts for the challenges faced when capturing and documenting its individual features and properties. While examining the subject from an architectural as well as model perspective, it has become clear that the notion of *context* is of paramount importance with respect to the perception of data in the IoT environment

Furthermore, it has been highlighted how the particularities of the IoT Value Chains based upon the dynamic flows of information render the attribution of responsibility across the supply chain is highly complex, thus, further challenging traditional concepts, such the concept of liability. This aspect, though, will be further examined in depth under the separate deliverables under "Work Package 05: IoT Policy Framework - Trusted, Safe and Legal Environment for IoT." Note, though, that the changing regulatory landscape at EU level including, for instance, the adopted General Data Protection Regulation (GDPR), NIS Directive, the draft Regulation on the Free Flow of Data as well as the ongoing public consultation on the review of the directive on the re-use of Public Sector Information (PSI Directive) creates an extensive impact for IoT Data Value Chains and will be, thus, monitored closely.

Also, based on the earlier analysis, the discussion produced a first set of attributes for an IoT Data Value Chain Model drawing links with the overarching IoT Policy Framework discussed under D05.01 and the concrete processes entailed. In this context, transparency surfaced as a key attribute given the labyrinth of contracts and the need of IoT stakeholders to be properly informed through the proposed introduction of specific SLOs. Transparency, though, also, implies the clear allocation of the roles of controllers and processors to those entities handling personal information, as being emphasized as well by the GDPR.

Overall, it should be noted that the creation of an IoT Data Model does not constitute a theoretical exercise; it rather forms a challenge of high practical significance and of value from a governance standpoint, as it can increase control within the fluid IoT ecosystems and augment the IoT benefits for the entire spectrum of the IoT stakeholders.

7. REFERENCES

[1] O. Vermesan and J. Friess (Eds.), *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*, ISBN: 978-87-93379-81-7, River Publishers, Gistrup, 2016.

[2] A. van der Wees, J. Breeuwsma and A. van Sleen, "IoT Societal Impact – Legal Considerations and Perspectives" in O. Vermesan and J. Friess (Eds.), *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*, ISBN: 978-87-93379-81-7, River Publishers, Gistrup, 2016, River Publishers Series in Communication, Volume 49, Chapter 7, page 220.

[3] IDATE DigiWorld.

[4] IDATE DigiWorld, Connected Healthcare, June 2016.

[5] A. van der Wees, J. Breeuwsma and A. van Sleen, "IoT Societal Impact – Legal Considerations and Perspectives" in O. Vermesan and J. Friess (Eds.), *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*, ISBN: 978-87-93379-81-7, River Publishers, Gistrup, 2016, River Publishers Series in Communication, Volume 49, Chapter 7, page 233.

[6] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union.

[7] Cloud Accountability Project, "D-4.4" Remediation guidelines and tools, 2015.

[8] G. Noto La Diega and I. Walden, "Contracting for the 'Internet of Things': looking into the Nest", in European Journal of Law and Technology, Vol 7, No 2, 2016.

[9] G. Noto La Diegaand I. Walden, "Contracting for the 'Internet of Things': looking into the Nest", in European Journal of Law and Technology, Vol 7, No 2, 2016.

[10] M. E. Porter, Competitive advantage: Creating and sustaining superior performance. New York: Free Press, 1985. doi:10.1182/blood-2005-11-4354.

[11] European Commission DG CONNECT, A European strategy on the data value chain, online at: ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=3488, 2013.

[12] European Commission, Towards a thriving data-driven economy, Communication from the commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions, Brussels, 2014.

[13] O. Vermesan and J. Bacquet (Eds.), *Cognitive Hyperconnected Digital Transformation Internet of Things Intelligence Evolution*, ISBN: 978-87-93609-10-5, River Publishers, Gistrup, 2017.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[15] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[16] 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.

[17] http://www.a4cloud.eu/lexicon/glossary/letter_t.

[18] Cloud Accountability Project, "D:C-2.1 Report detailing conceptual framework", 2014.

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[20] The Cloud Select Industry Group, "Cloud Service Level Agreement Standardisation Guidelines", 2014.

[21] SMART 2016/0032 Study, IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (Ongoing).