7

IoT Societal Impact – Legal Considerations and Perspectives

Arthur van der Wees, Janneke Breeuwsma and Andrea van Sleen

Arthur's Legal B.V., The Netherlands

7.1 The Relevance of Hyperconnectivity

Technology changes the world in a fast pace. Information, communication, internet and cloud computing technologies have shown and are showing this already on a daily basis, and have connected people, organisations and data. The Internet of Things (IoT) will push this process further, by hyperconnecting people, organisations and their data with billions of objects.

Where technology is global and evolving with lightning speed, regulation is local. Policy, deployment and enforcement mechanisms and instruments have not always shown to be able to adapt, react and govern new developments. With the introduction and global use of the IoT the related challenges will increase.

However, policy making and enforcing such policies, whether being legislation, regulations or otherwise, has valid and very relevant and important reasons and purposes, such as creating, influencing and setting a balanced, predictable trustworthy, fair, reasonable, transparent and open yet where necessary protective framework in order for the society and economy to operate in a trusted and civilised way and be monitored and fostered.

As per technological change, globalisation, worldwide competition and demographical challenges in most regions in the world, operating in a durable hyperconnected economy and society and boosting innovation and productivity are not nice to haves anymore. These are a necessity to have, in order to stay relevant as an economy and society but also to avoid social disruption.

In the Digital Single Market strategy the European Commission basically recognises the importance of these elements within the digital economy.

Within scope of the section on 'Maximising the growth potential of the Digital Economy' of the Digital Single Market strategy, the European Commission has proposed several initiatives to investigate, influence and in some cases propose new or updated standardisation, self-regulation or other policy mechanisms, which will offer new regulatory frameworks. It is part of any society, economy, market or ecosystem, including the IoT ecosystem.

IoT implies a high volume of relationships between many hyperconnected actors – whether human, organisations, algorithms or machines –, and those relationships will need to be arranged and catered for.

These actors within the IoT ecosystem and related digital markets need predictability and legal certainty on the numerous relationships as well as related issues in order to enter the market as vendor or buyer, invest in or procure new products, services and embrace new business models, irrespective of being a private or public organisation or community, or being a governmental body, large corporation, SME or consumer.

In order to make IoT and related hyperconnected ecosystems work, create space to innovate, modernise the society, build global connectivity, nurture internet openness, create trust, jobs and skills in the digital economy and society, and continue working on and safeguard an acceptable level of social prosperity that is durable. The two now colliding worlds of digital technology on the one hand and regulations and compliance on the other will need to be connected and hyperconnected as well.

From an IoT ecosystem and hyperconnected point of view, this Chapter will investigate, point out, explain and structure several of the main challenges, considerations and perspectives in the domain where these worlds meet, collide and will need to get used and adapt to each other in the best way possible.

This Chapter does not exhaustively identify or describe any and all challenges, considerations and perspectives in the domain, and does also not intent to be limiting those challenges, considerations and perspectives mentioned hereunder.

7.2 Unambiguous Definitions

It is fundamental and important to keep the definitions regarding and related to IoT well defined and unambiguous, in order to enable clear communication between multiple stakeholders, to ensure effective recommendations, and to come to a common understanding. Without such basis and common

understanding, it is quite impossible to build ecosystems, frameworks, policies and relationships that understand, interact and interoperate with each other in the IoT domain.

As technology and business models develop and new technology and models are developed and adapted, it will also be important to ensure definitions are technology neutral, business model neutral, principle based and consistent with fundamental rights and the fast evolving IoT landscape.

Definition of The IoT by ITU and the IoT European Research Cluster (IERC) is:

> *'The IoT 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]

The 'Thing' in the IoT can be anything, such as for instance (without limitation) devices, objects, algorithms, people, animals, plants or other Things (hereinafter: '*Things*'). What makes these Things so special is their connectivity via the internet and the ability to act in an orchestrated way, such as Machine to Machine (M2M), Human to Machine (H2M) and Machine to Human (M2H). The combinations are quite indefinite. Taking into consideration that each combination implies as least two 'Things' interacting with each other, there are a lot of legal relationships to address and arrange for.

As the markets and European Commission has currently chosen to use IoT to define this domain, it is good to mention that when one reads or hears about Internet of Everything, Internet of Customers, Internet of Everyone, Internet of Humanity or similar terms, one in essence means the same as the definition of IoT set forth above. However, there is an ongoing debate on whether humans are 'Things'. For the purposes of this book in general and this chapter in specific, it is understood that a human is not a thing but for purposes of setting the scene on legal and other relationships, and in order to easily work with the definition IoT it is within that definition.

In this document, the following terms used shall have the meaning as set forth in the European Commission Cloud Service Level Agreement

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

Standardisation Guidelines[2], ISO/IEC 17788, which guidelines have been initiated, discussed, set and endorsed by the European Commission and currently provide for the most up to date and generally accepted definitions that are to most extent quite relevant and useful in the IoT domain as well.

7.3 Converging Markets

The technologies that make IoT possible are converging existing markets and creating new markets, both physical and virtual markets, private and public markets and both vertical and horizontal markets. From the converging technical markets perspective, smart systems integration, cyber-physical systems, smart networks, data analytics, cloud computing, robotics and artificial intelligence bring together different generic technologies with nano-electronics, wireless networks, low-power computing, adaptive and cognitive systems.[3]

Basically, these can be divided in five main groups:

1. Things
2. Infrastructure
3. Data
4. Services
5. Connectivity and Interoperability

7.3.1 Things

The Things in the IoT are for instance (without limitation) devices, objects, algorithms, people, animals, plants or other Things and are provided with unique identifiers (or sometimes community identifiers) and the ability to transfer data over an infrastructure or network without requiring

[2]Cloud Services Level Agreement Standardization Guidelines, European Commission, DG Connect, Cloud Select Industry Group- subgroup on Service Level Agreement (C-SIG-SLA), https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

[3]ITU-T Internet Reports, 'IoT', November 2005. Lee, et al. The IoT – Concept and Problem Statement July 2012; F. Mattern and C. Floerkemeier 2010, Mattern, Friedemann, and Christian Floerkemeier, 'From the Internet of Computers to the IoT', in: K. Sachs, I. Petrov, P. Guerrero (red.), *From Active data management to Event-Based Systems and More*, Berlin: Springer 2010, p. 242–259.

human-to-human or human-to-machine interaction. These Things are all about collecting, deriving, using, storing and sharing data via the infrastructure.

7.3.2 Infrastructure

The infrastructure regards transmitting, collecting, storing and/or sharing the data within the ecosystem. It is a collection of hardware, software and other related products and resources that enables the provision of IoT and their services.

7.3.3 Data

The key aspect that keeps IoT moving and alive is data. Data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or within the IoT, including without limitation 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.

Data Life Cycle: the life cycle of processing data commonly includes seven (7) phases:

1. Obtain/collect
2. Create/derive
3. Use
4. Store
5. Share/disclose
6. Archive
7. Destroy/Delete

This data life cycle is also used for personal data, which is then called the personal data life cycle.

It should be noted that data does not only arise out of the first two phases, but data is created and processed in each and any phase. For example, when deleting data, other data describing the act of deletion may arise.

7.3.4 Services

One or more capabilities offered invoked using a defined interface. There is a seemingly endless amount of services offered within IoT in a countless amount of categories, as well as virtual as physical.

The services are extended into fields such as education, intelligent buildings, supply chain, health care, everyday life, disaster management, safety and transport to provide people with better services.

7.3.5 Connectivity and Interoperability

As above-mentioned IoT can be built by using any number of technologies and a particular technology stack should not be assumed. Essential hallmarks of IoT are connectivity and interoperability for which technology neutrality is required.

For example, many products and services are connected with REST interfaces or APIs to exchange data and interoperate with other products, services and Things.

7.4 Relationships and Markets

As the domain of IoT is vast, one needs to identify in which market it is operating and which relationship between which Things it would want to make possible and arrange for. This, as the characteristics of each market and each relationship may have legal consequences and may need specific frameworks and assurances.

The combinations of relationships are endless, as there are quite a few Things, and each combination is possible. For instance business to business, business to consumer, consumer to consumer, government to resident, resident to government, commuters to parking services, and so on.

Whether such relationships make sense, depends on the circumstances and purposes of the relationship and within what market. A whole new range of relationships will arise and on top of that can have multiple purposes.

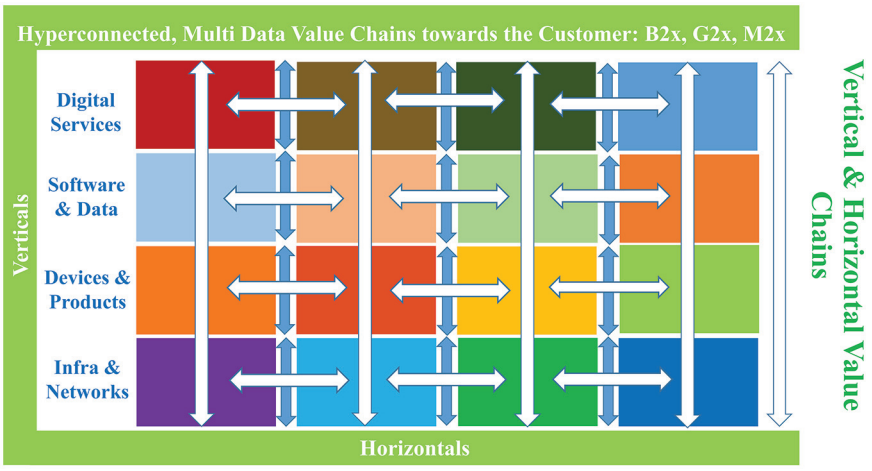

Figure 7.1 Hyperconnected, vertical and horizontal value chain.

For example the development of smart cities and communities is a vertical that has many verticals and cross-verticals combined, for instance without limitation government to business, government to visitors, residents to government, and commuters to business.

As another example, in the business to consumer market one already sees IoT in operation, for example wearables, smart meters, connected cars, smart mirrors and smart fridges. The end-user of IoT in this market is a consumer who uses the IoT in its daily life. It is well-known that a consumer has specific rights to protect its interest, including without limitation personal data protection and product liability.

7.5 What Are the Main Challenges

The Internet, cloud computing, data analytics and other advances in IoT have spawned a global digital economy and the continuing evolution of connected Things has added a new and growing dynamic. While IoT is increasing, it is still in its nascent stages and the related technologies, business models and polices will undoubtedly evolve over a number of years.

There are a number of challenges to facilitate sustainable growth of IoT by adding clarity to the challenges between the converging markets and stakeholders. Several of these main challenges are set below. Again, please note that these are non-exhaustive, and some will be adequately addressed or solved in the near future, where new challenges will surely arise with the emergence of improved or new technologies and combinations thereof.

7.5.1 Common Understanding

It sounds so logical and obvious: we need a common understanding of matters, challenges and solutions. But in fact and real life, it is quite a challenge and in this chapter identified as one of the main challenges.

Common understanding is a result from having found common ground, or a result from having established certain ground as deemed to be the common ground for the matter at hand. When addressing the matters at hand regarding and related to IoT, the same applies. Common ground starts with the basics: clear and unambiguous definitions. Some IoT definitions have been addressed a few paragraphs above. Once the definitions are clear, the next steps are principles and (legal) frameworks that stakeholders recognize and are able to identify themselves with.

Without such definitions, principles and frameworks as a basis for common understanding, it will be impossible to build ecosystems, frameworks, policies and relations that understand, interact and interoperate with each other. The recommendation here is that in case one finds out that a dialogue, discussion, debate or negotiations seem difficult to be resolved, it may be good to take a step back and return to the common understanding, before re-entering into such discussions to seek common ground on the pending matters.

7.5.2 Trust

Trust is always one of the challenges with new technologies and change. Regarding IoT, customers and users thereof may need time to adapt, learn that the opportunities benefits are, and how to mitigate or cope with the risks. Depending on the specific IoT, vertical it is used in, deployment thereof and impact it may have for the customer and users, trust will in some cases be obtained quicker than in other cases.

Integral parts of trust is security, data management, data protection and the way vendors, providers as well as co-users and the related community will act and react on a case to case basis. Another part of building trust is taking care of customers and users with insufficient knowledge. For instance, insufficient knowledge has been established by EuroStat to be the number one reason for businesses not to procure paid cloud services, and the IoT industry should try to avoid that such same barrier arises in the upcoming IoT market.[4]

7.5.3 Security

The technical architecture of the IoT has an impact on security and privacy of the involved stakeholders and data subjects. For example Denial-of-service attacks could be a major threat when it comes to the IoT ecosystem.[5]

Furthermore the security of both the relevant stakeholders in multiple horizontals and verticals is for sure a main challenge as well. The value chains are quite complex in IoT as per its hyperconnectivity and interoperability, which by nature results in customers and users not understanding the possible risks and impact thereof. Even though security is a horizontal itself, it is expressly mentioned as being relevant for other horizontals as well, as IoT

[4]Eurostat News Release 9 December 2014.

[5]Denial-of-service-attacks typically involve the overflow of a network device with more requests than it can process, leading to an overload that renders the service unable to answer legitimate requests.

verticals will generally be stacked with several layers, including without limitation infrastructure, networks, products, devices, software, data and services. The value chains of IoT are non-linear towards customers and users; they are multi-angle, cross-vertical, and multi-horizontal. For example, per layer in a vertical IoT ecosystem at least two security horizontal layers may be necessary; one upon entry of data in such layer, and one upon exit thereof.

A high degree of reliability is needed, since business processes are concerned. However there are a lot of similarities when it comes to cloud computing security standards which have already been developed and tested.

Specifying measurable security level objectives in IoT is useful to improve both assurance and transparency. At the same time, it allows for establishing common semantics in order to manage cloud security from two perspectives, namely (i) the security level being offered by a stakeholder and, (ii) the security level requested by a IoT user.[6]

The approach used in this section consists of analysing security controls from well-known frameworks[7] into one or more security objectives, when appropriate. These objectives can be either quantitative or qualitative. This section focuses on the definition of possible security objectives. Eight categories are provided, each with one or more objectives.

The categories represent some important security requirements. However, it should be noted that the list of objectives is not meant to be considered as exhaustive and that the objectives proposed are not meant to be considered as applicable in all individual cases. The applicability of particular objectives depends on the type of products and services offered (in terms of both of functionality and model) and pricing of it (free, paid, premium). It is important to understand that some of the objectives are interdependent: objectives relevant to security may also have relevance in the areas of data management and personal data protection for instance.

- Reliability: reliability is the property of a IoT system to perform its function correctly and without failure, typically over some period of time. The system has to avoid single points of failure and should adjust itself to node failures.

[6]Reference is made to Chapter 3 and Chapter 4 of the Cloud Service Level Agreement Standardization Guidelines regarding Security Service Level objectives overview. Furthermore, as an example for the security challenges reference is made to the report 'New security guidance for early adopters of the IoT' of the Cloud Security Alliance which includes an IoT Security Life Cycle.

[7]Relevant security frameworks include in particular ISO/IEC 27001 and ISO/IEC 27002.

- Authentication and Authorization: authentication is the verification of the claimed identity of a Thing. Authorization is the process of verifying that a Thing has permission to access and use a particular data or resource based on the (predefined) ecosystem it wishes to offer to the IoT user. As a principle, retrieved identity and data of a thing must be authenticated.
- Cryptography: cryptography is a discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use, also known by the term encryption. However stakeholders must be able to implement access control on the data provided in order to cooperate within the IoT ecosystem.
- Security incident management and reporting: an information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising operations and threatening information security. Information security incident management are the processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
- Logging and Monitoring: logging is the recording of data related to the operation and use of a IoT system. Monitoring means determining the status of one or more parameters of a IoT system. Logging and monitoring are ordinarily the responsibility of the relevant stakeholder's.
- Vulnerability Management: a vulnerability is a weakness in an IoT system, security procedures, internal controls, or implementation that could be exploited or triggered by a threat. Management of vulnerabilities means that information about technical vulnerabilities of information systems being used should be obtained in a timely manner, the exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
- Governance: governance is a framework by which IoT will be directed, controlled and governed.

7.5.4 Personal Data Protection

Data used to be quite static, and used to reside in one place. Digital data that is connected to internet and cloud, and that is hyperconnected through IoT ecosystems, travels. This may be the key catalyst of internet, cloud computing, IoT and data analytics technologies being in some kind of way used and embraced by each and any organisation in the worlds. The fact that data travels

is not new, but have come on the agenda in the past years of both the demand side as the vendor side, as well on the agenda of policy makers. As data subjects, data controllers, companies, organisations and countries feel they are losing control over their respective data, and do not always understand or know how the data is processed, it is only natural that some of those are reacting to try to regain control, whether it is personal data, sensitive data or otherwise.

New regulations and directives related to personal data protection, such as the General Data Protection Regulation (GDPR), and security breach notifications, such as the Network and Information Security Directive (NIS Directive) add to those concerns, but may also be part of the keys and mechanisms to resolve these concerns, if implemented in a transparent and understandable way for such data subjects, customers and users.

To understand (personal) data protection it is recommended to go back to the basics, which means that data is not a four letter word. The difference between the definitions of data and personal data should be clear and a common understanding. Reference is made to paragraph 7.3.3 for the definition of data where data is explained and what kind of data there are in the IoT ecosystem.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[8] For the protection of personal data the employment of technical, organisational and legal measures in order to achieve the goals of data security (confidentiality, integrity and availability), transparency, intervenability and portability, as well as compliance with the relevant legal framework is required.

The basis for personal data should be data minimization, where stakeholders are responsible for ensuring that personal data is erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes.

Based on the (new) regulations and directives related to personal data, the principle of purpose specification and limitation requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Therefore, the purposes

[8] Chapter 2 and Chapter 6 of the Cloud Service Level Agreement Standardization Guidelines regarding personal data protection.

of the processing must be determined, prior to the collection of personal data, by the data controller, who must also inform the data subject thereof. When the data controller decides to process data in IoT, it must be ensured that personal data is not (illegally) processed for further purposes by the relevant stakeholder, or one of the subcontractors.

Only if the data controller informs the data subject (the IoT user) about all relevant issues and being transparent which data will be collected, then the data controller is allowed and to process any (personal) data. The reason therefore is that the data subject is capable of fulfilling its obligation to assess the lawfulness of the processing of personal data. Moreover, the data controller shall make available the information that enables the customer to provide the data subjects with an adequate notice about the processing of their personal data, as required by law. Furthermore, the (new) regulations and directives related to personal data gives the data subject the right of access, rectification, erasure, blocking and objection.

One of the (new) requirements for the data controller as set forth in the GDPR are codes of conduct, standards and certification mechanisms. Such codes of conducts, standards and certification mechanisms for the stakeholders gives more and clear guidelines how the IoT user is protected. The data controller, must accept responsibility for abiding by the applicable data protection legislation.

In order to maintain the above (personal) data protection approach within IoT, the key is to adhere privacy-by-design in advance. In accordance with the laws and regulations regarding data protection and the challenge thereof within IoT, the main principles for privacy-by-design are the following:

- No personal data by default principle: avoid personal data collection or creation by default, except where, when and to the extent required.
- 'As-If' principle: design and engineer IoT ecosystems as-if these will process personal data, now or in a later phase.
- De-Identification by default principle: de-identify, sanitise or delete personal data as soon as there is valid legal basis anymore.[9]
- Data minimalisation by default: only process data where, when and to the extent required, and delete or de-identity other data.
- Encryption by default principle: encrypt personal data by default, and include digital rights and digital rights management thereto.

[9]For more information on this topic please refer to 'NIST Special Publication 800–88: Guidelines for Media Sanitization'.

7.5.5 Digital Right Management

As companies transition to IoT, the traditional methods of securing and managing data is challenged by IoT-based connections. Elasticity, multi-tenancy, new physical and logical infrastructures, and abstracted controls require new data security strategies. Managing data and information in the area of IoT can affect all organisations, users and Things. It begins with managing internal data and service migrations and extends to securing information in diffuse, cross-organisation applications and services.

The data management objectives cope with important quantitative and qualitative indicators related with data life cycle management, and can be considered as complementary to existing and applicable security and data protection certifications offered by the IoT stakeholders.

The presented data management objectives are subdivided in four (4) different top-level categories covering all aspects of the identified data life-cycle. Each category is subdivided in one or more objectives that are applicable to that specific category. Not all objectives may be relevant for each service, in particular depending on the type of Things and stakeholders as M2M, M2H or H2M.

7.5.6 Data Ownership and Data Access

Who owns the data? Why am I not able to retrieve my data? From the customer and users perspective, the existing awareness, expertise and transparency of both such customers, users as well as vendor level as well as policy makers and authority level is generally not sufficient to provide actors in the data value chain with trust, predictability and legal certainty each needs to be able to assess, make informed decision and have reasonable access and use of IoT and related services. The same goes for the existing legal frameworks and current contractual practices, although this obviously differs per product, deployment model and service model as well per vendor and the (envisioned or actual) use of the customer and users thereof. Contractual practices, including the arrangements in or related to IoT also create obstacles to data use, access, and in quite a few places create data lock-in effects as well.

One of the challenges with data ownership is that the concept of ‘owning’ digital data in the traditional sense of the word ownership in most cases in an oxymoron and leads to discussion and conflicts. Data ownership is generally not addressed in the IoT domain, because data ownership is a difficult domain, also as it is not defined. Vendors may have a totally other opinion or perception about data ownership than its customers and users, whether being SMEs or

not, and the laws and regulations that have deemed to be governing ownership are either outdated or are quite difficult to apply, interpret, use and enforce in the digital world.

It becomes even more problematic when some vendors have a traditional mind-set that owning assets, including data, is a goal in itself. From another perspective, ownership of digital data in general is basically not possible. The current framework of copyright regulations is not particularly designed for digital assets including data, while the redesign thereof in the early 90s regarding software (Directive 91/250/EEC) has not proved to be a transparent framework that resolves discussions and disputes on ownership as well. The Database Directive (96/9/EC) from 1996 also has lost its effectiveness, as a major requirement for protection thereunder is having done a substantial investment to build the relevant database, where such databases nowadays can be built and used for a fraction of the cost. The threshold to be eligible for protection thereunder is not met anymore, and lowing the threshold would even increase and not resolve the discussion on data ownership either. The upcoming Trade Secret Directive (COM/2013/0813) that is proposed, may resolve a minor part of the data ownership discussion, but in such case the protected data thereunder needs to remain secret and not generally known or readily accessible to third parties. In hyperconnected ecosystems where data travels and data can change from legal characteristics and purpose of travelling and being processed at any time, this will be quite challenging. Owning data is just very difficult, as one would like, or need to, share such data, have it processed and transferred. On the other hand, domain names and related domain name rights have been designed by law not to use the concept of ownership; it uses the concept of holdership of a domain name, which has proven to work quite well. Based on research done and ongoing research by Arthur's Legal, introducing and using the term 'data control' is the preferred way to move forward in the IoT and related digital and hyperconnected domains. This also to reflect on the challenges set above and to address the confusion and distrust that the term 'data ownership' leads to. Data control better reflects the rights a person or organisation may have, whether personal data or non-personal data, and the rights can grant others. It also reflects that digital data can and in most cases will be shared and processed. Data control will be one of the most relevant and essential components to boost trusted hyperconnectivity and the digital economy and society, as it is all about data.

The European Commission has data ownership and data-access on its agenda, and has started the dialogue about how to be able to address this domain of use rights and digital rights management. As Commissioner Oettinger put it on these topics: 'We need a single rule book for the Internet

of Things in Europe. Capable to properly address new challenges raised by the technology. This includes data protection, safety and liability rules, including the emerging issues of data ownership, rules on access and re-use of non-personal data in an industrial context, just to mention a few.'[10]

7.5.7 Free Flow of Data

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 digital single market and European manufacturers, services providers and other vendors to benefit from being able to market its respective products, services and data to other member states.

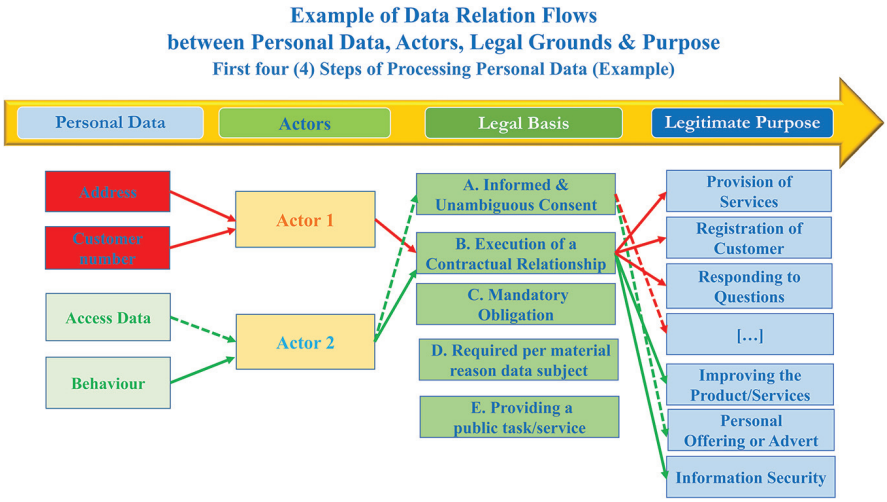

Figure 7.2 Example of data relation flows.

[10]http://ec.europa.eu/commission/2014-2019/oettinger/announcements/keynote-speech-closing-plenary-session-net-futures-2016-brussels_en

7.5.8 Accountability and Liability

As per the convergence of technologies, markets and stakeholders, and as these technologies, its manufacturers and vendors are diverse, the question who is accountable and liable for what will be even more difficult to answer and proof than in the physical society.

For example, 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 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 accountable, a solid and stable digital economy and society will be difficult to create.

Merely contractually re-allocating risks and damages to the customer and its users will not contribute to the creation of the Digital Single Market in general, and uptake the IoT ecosystems in particular.

In the field of data protection, accountability often takes a broad meaning and describes the ability of parties to demonstrate that they took appropriate steps to ensure that data protection principles have been implemented.

In this context, accountability is particularly important in order to investigate personal data breaches; to this end, the relevant stakeholders should provide reliable monitoring and logging mechanisms.

Moreover, the relevant stakeholders should provide documentary evidence of appropriate and effective measures that are designed to deliver the outcomes of the data protection principles (e.g. procedures designed to ensure the identification of all data processing operations, to respond to access requests, designation of data protection officers, etc.). In addition, IoT users that are deemed to be data controllers under the GDPR should ensure that they are prepared to demonstrate the setting up of the necessary measures to the competent supervisory authority upon request.

7.5.9 Too Much Data?

The billions of sensors and other objects and Things will generate so much data, most of which is expected to be unstructured and not necessarily useful yet making identifying relevant data more difficult. Commonly available data analytics technologies cannot yet cope with the amount thereof in a comprehensive, useful way. As data analytics is one of the pillars to make

IoT interesting, feasible and worthwhile, this can be seen as one of the main technological challenges. Data architecture will therefore be quite important to address. This, for instance also to comply to regulations and standardisation including without limitation regarding personal data protection, security breach notification and the like.

7.5.10 Regulation and Standardisation

As argued in the paragraph 7.1, technology is global and regulation is local, and new technology goes to market much quicker than regulations.

Policy makers are investigating and deploying other policy mechanisms such as industry guidelines, best practices, codes of conducts, international standardisation, community self-regulatory initiatives and the like, to find the right hybrid combination to be able to adapt, react and govern such technological and related developments.

Getting the right mix of policies in the market, in time yet in a durable and facilitating way, is quite a challenge nowadays.

7.6 Multi-Angle Stakeholders IoT Ecosystem

IoT can be built using any number of technologies, used by different stakeholders and for all kind of markets, whereby all kind of goals should be formalized and covered by ethics, accountability, standardisation, legislation agreements and insurance. Essential to reach this goal of IoT is that these are based on technology neutral wording as a necessary foundation.

7.6.1 Technology and People

The most important elements of the multi-angle stakeholders IoT ecosystem are the technology and the use thereof by the people. The technology of IoT should be neutral and monitored from time to time to be up to date and based on the state-of-the-art technology. Monitoring of the technology will be based on the principles of security, personal data, digital right management, usability, portability and accountability. If technology and for instance IoT will be a success the people have to accept such new connected technology. People play one of the key roles in the Ecosystem especially when it comes to implementation, acceptance and trust of IoT. The human factor is a big challenge of IoT. Both technology and people have influence on the other stakeholders of IoT as ethics, accountability, regulation, standardization, legislation and risk allocation, which will be further discussed in the paragraphs below.

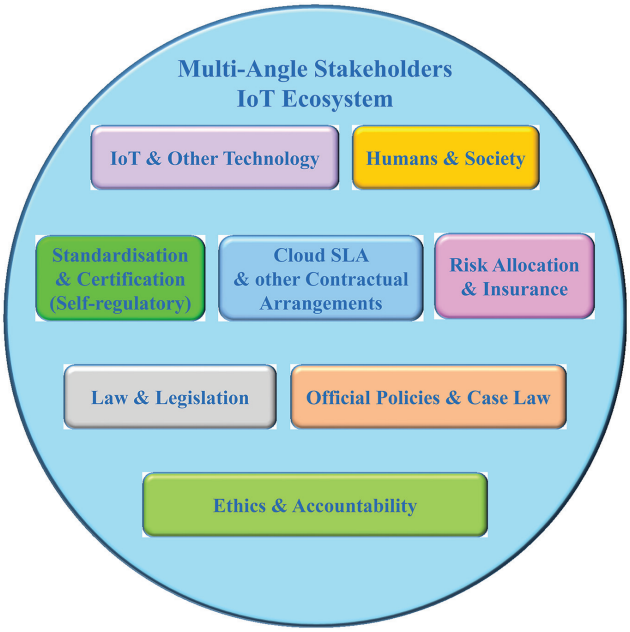

Figure 7.3 Multi-angel stakeholders IoT ecosystem.

7.6.2 Ethics and Accountability

In every converging market, each stakeholder has to deal with ethic and accountability regarding to IoT. For example, a manufacturer of certain Things has to address the challenges of ethic with the connected Things, and whereby such manufacturer has to accept its responsibility for all subjects of IoT. In case of safety of a product, it is not possible to cover all product liabilities, but IoT will bring more responsibility for each stakeholder in the market, and have to think and discuss those effects in a transparent manner prior to the other goals of IoT.

7.6.3 Regulation and Standardisation

The internet is a global communication channel and it is built on standards that are respected worldwide, which is also the basis of IoT. However, the government and compliancy of Things is covered by the current legislations, which will not fit completely for purposes of IoT. There are regional, national and local laws have to govern the use of Things and all other aspects of

IoT for all kind of converging markets, stakeholders and markets. The goal is that legislation should fit for IoT based on technology neutral legislation, because everyone benefits from globally common understanding vocabulary and legislation.

Standards and guidelines for IoT should specify the concepts and definitions necessary for the converging markets, stakeholders and markets to describe the Things, infrastructure, data and services life cycles. There are already standards and guidelines used and produced by organisations such as ENISA, NIST or ISO/IEC. For example, in the field of security, relevant work is using the approach to analyse and refine an individual control into one or more security objectives, which are then associated with metrics and measurements that can be either quantitative or qualitative. Before introducing a particular concept into a standard or guideline for IoT, one should seek proof to ensure the concept is viable from both technical and business perspectives. With standardization of guidelines in the relevant markets of IoT, it will create world-wide applicability, technology and business model neutral, unambiguous definitions and create conformance through a global, common understanding.

7.6.4 Contractual Relationships

The agreement between the stakeholders can refer to the clearly defined information in the legislation, standards and guidelines, but the agreement itself must meet local legal requirements and those must be left to the discretion of qualified attorneys.

7.6.5 Risk Allocation

All the other risks, liabilities and other elements which could not be defined and arranged by legislation, standardisation and agreement should in a best case scenario be covered by insurances. If insurance of IoT is possible than it realizes that IoT is a mature market and the IoT ecosystem is complete.

7.7 Conclusion and Recommendations

New technologies lead to change. Change is a catalyst that can be feared, but can also be embraced and used to optimise the current status quo of society and economy, and sometimes even leapfrog technologies that have already been improved. Especially the hyperconnected aspect of IoT technologies will have

quite some impact on the society and economy, and may raise certain ethical or legal discussions on new and existing topics.

As the IoT technologies, developments, combinations and deployments of IoT verticals and horizontals continue to evolve, the opportunities and challenges will evolve as well, including the legal and compliance consequences, challenges and opportunities, including privacy, security and other compliance by design and related automation thereof. Addressing and resolving these challenges are one the most important value creating and success factors of IoT. On privacy-by-design, the Article 29 Working Party worded it as follows in the Opinion 8/2014: 'Organisations which place privacy and data protection at the forefront of product development will be well placed to ensure that their goods and services respect the principles of privacy-by-design and are equipped with the privacy friendly defaults expected by EU citizens'.

As any relatively new market, also the IoT supply side and IoT demand side will need to find, understand an trust each other the coming period, and for that a principle-based ecosystem of IoT policy frameworks may facilitate of uptake of that market. As its hyperconnected, agile and hybrid nature, such policy framework ecosystem will need to be hyperconnected, agile and hybrid as well in order to have the positive impact it seeks. Principle-based mechanisms with a solid common ground of globally recognised definitions and principles will facilitate such agile framework ecosystem. Each policy framework will need to be hybrid, with all the tools and mechanisms available and newly developed, including for instance self-regulation, community frameworks, standardisation, where relevant current regulation and where necessary regulation, preferably Pan-European because of the borderless nature of technology. As per the extreme variety of actors, objects, markets, capabilities, Things and relationships, one single IoT framework seems difficult, hence the conclusion that an interoperable and durable ecosystem of IoT framework may be the way to facilitate and support the market and all related stakeholders in an efficient way. Such ecosystem will need to be based on open and transparent dialogues with a large variety of groups and stakeholders from a 3D multi-angle, both internally at the European Commission, as well as externally in the European Union and beyond.

With such hyperconnected multi-disciplinary brainpower and related combinatorics innovation, trust, usability and market update will have the best chances to succeed, and may result in multiplicity: a symbiotic combination of diverse groups of people working together with diverse groups of machines to make decisions and solve complex problems. As Commissioner Oettinger

put it on a human-centred IoT: 'The aim is to empower citizens rather than machines and corporations, thanks to high data protection and security standards.'[11]

With that, the IoT combined with the Internet of Humanity leads to the Internet of Human Prosperity.

[11] http://ec.europa.eu/commission/2014-2019/oettinger/announcements/keynote-speech-closing-plenary-session-net-futures-2016-brussels_en