D5.3 – Final Policy Whitepaper on IoT

IoT: Policies towards 2025

Editor:	Maarten Botterman, GNKS Consult BV	
Deliverable nature:	Report	
Dissemination level:	Public	
Contractual/actual delivery date:	M26	M26
Suggested readers:	Researchers, decision makers and policy makers, both business, public sector and civil society	
Version:	1.0	
Keywords:	Policy, trusted, ethical, IoT, privacy, data protection, security	

Abstract

Technology is deeply invading every aspect of society. “Being connected” to the Internet has become the norm in large parts of the world – whether by computer, tablet or smart phone, and this is now also increasingly true for “things”. The European Commission has been exploring and supporting innovation in this field in its research programmes and policy papers for more than a decade. In accordance with the principles of the treaties, the Commission aims to make sure that the development of the IoT does not compromise the fundamental values on which European society is based and helps address societal issues.

This Policy Whitepaper on IoT builds on the policy paper that was released as D5.2, and is updated with public comments on the D5.2 work which has been discussed in a number of forums, both at relevant conferences and workshops, and on-line, and recent relevant developments related to IoT and data. The recurring theme in this paper is "trusted IoT" and “human dignity” and includes reflections on topics such as big data / data protection, "security" and "ethical issues by design" that are crucial in this aspect.

Main conclusion of the dialogue so far is that an ethical way forward is the only way to ensure IoT development and deployment can happen in a sustainable way, supporting both society and business in the long run. The challenge for the coming year will be to determine what “ethical” means at a global level, and how such an approach can be realised, world-wide (governance aspect). The draft IoT Good Practice Declaration to the IGF expresses this and will function as a vehicle for further dialogue on this.

The Paper concludes with a number of concrete policy recommendations for IoT innovation to take place within a responsible and ethical framework, and at the same time will be stimulated to attract even more investment over the years to come. IoT should “go ethical” to be able to fulfil the promise it holds towards the future, globally: both for business, as for society as a whole!

With thanks to all those that provided feedback on the recommendations of the Policy report (D5.2), in particular people from the European IERC network and the global IGF DC IoT network. Special thanks to Prof.Dr. Wolfgang Kleinwaechter (Aarhus University, co-founder of IGF DC IoT); Prof.Dr. Jonathan A.K. Cave (Warwick University, also co-author to the RAND publication on IoT); Prof.Dr. Pedro Maron (Duisburg University, project manager of IERC projects GAMBAS, Smart-Action).

Disclaimer

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 609024.

Copyright notice

Table of Contents

List of Figures

Executive Summary

Digitalisation of our society is progressing at rapid pace. The Internet of Things, and its underlying data streams, currently shape an important part of that transformation by introducing more and more objects that are digitally connected in our lives, ranging from cars to smart tvs to smart homes, smart cities, smart wearables up to tsunami warning systems and air pollution sensors. Drivers for IoT are business opportunities (new markets, new business models), and increasingly also societal opportunities (e.g. smart cities, environmental monitoring, disaster warning, etc.). IoT comes also with challenges, ranging from privacy concerns to security and safety issues. All data generated and shared by objects connected through the Internet and combinable using smart algorithms lead to a world in which privacy is getting a new meaning, and choices in smart environments are increasingly made for us according to algorithms for acting and/or self-learning. With the massive uptake expected over the coming years IoT has become a real game changer.

During meetings over the last year, both within the European IoT research community and the more recent Alliance for Internet Of Things Innovation (AIOTI), as well as in global forums such as the Internet Governance Forum's Dynamic Coalition of the Internet of Things (IGF DC IoT) and EuroDIG, focused at policy aspects of IoT, the need to address these aspects are recognized, as is the need to ensure space for innovation and development of new IoT products and services within the current and developing legal frameworks. Whereas the IoT up to today is mainly driven by business opportunity considerations and technology push, time has come to involve consumers/citizens in order to make sure we are developing a "future we want" (i.e. the terms used by the United Nations when describing the aims of the Sustainable Development Goals as adopted in September 2015) with "respect for human dignity" as called for in the September 2015 Opinion from the EDPS pointing out that "*In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing*."

This Policy Paper on IoT towards 2015 focuses on specific policy issues that can assist or be assisted by the development of the IoT. IoT can be used for many different things by a wide range of stakeholders, and acceptance, experience and continuing innovation of those stakeholders will determine the impacts of the IoT more profoundly than its technological specifications alone, and needs to be "trusted IoT". This requires reflections on topics such as big data / data protection, "security" and "ethical approach" on a global level respecting human rights, and within Europe with a focus on human dignity and European legislation.

IoT develops within a wider policy context across different sectors ranging from health to agriculture, transport, logistics etc. and policy domains such as Internet governance, big data/analytics and cloud computing. It's specificities must be addressed to ensure we develop "trusted IoT" and dispel the more extreme hype and fears in order to fulfill its potential to alleviate societal challenges and encourage and reward entrepreneurs.

Following a series of dialogues within the European research and stakeholder community and at global level, a list of policy proposals has emerged that were widely seen as relevant. In particular we found a lot of support for the argument to put more attention on "going ethical" – and have stakeholders develop together how this exactly would look like – as with the current speed of

technology development we cannot continue to count on "adherence to the law". To quote the EDPS: "*there are deeper questions as to the impact of trends in data driven society on dignity, individual freedom and the functioning of democracy*."

In line with this we propose to "go ethical" and we present a number of concrete policy actions for stakeholders to underpin this.

***Policy action towards European industry**: Encourage innovators and providers to develop ethical technology in line with market and used needs. This could be an important way for businesses to add value to their brand, and would also allow consumers to determine which companies hold ethical principles in high regard. The objectives would be to foster a value-added strategy much like what has happened for green tech over the last decade.*

NB: The "Large Scale Framework projects", in which a series of "best of breed" demonstrators from different application areas could be hosted, should include some horizontal activities in support of an ethical way forward, taking into account practical aspects such as privacy and data protection, security, ethics, spectrum and standardisation protocols. Demonstrators should be set up in such a way that citizens are welcomed to see, participate and react, and such experiences across demonstrators should be assessed as one of the horizontal tasks. See also the AIOTI recommendations.

***Policy action towards developing a better understanding of what is needed:** develop a taxonomy for security of IoT applications per sector and type of application, thus ensuring a common understanding of what level of security is expected to be delivered by providers for specific applications; Develop a taxonomy for privacy sensitivity of IoT generated data collections, including recommendaed ways forward for collecting, sotring, protecting and sharing these data.*

***Policy action towards development of global context that considers EU values**: actively engage with and support the creation of a global ethical charter that would safeguard vital interests of consumers in IoT environments, offer guidance to developers of IoT environments and services (even ethical impact assessments before development). The development and implementation of such a charter is one potential consequence of a continuing programme[1] of research and debate on the ethical, legal, social and environmental aspects of ICT, specifically as regards the IoT.*

For the latter see also the EDPS opinion 4/2105 calling for "*an open and informed discussion in and outside the EU, involving civil society, designers, companies, academics, public authorities and regulators … to help define a new digital ethics, allowing to realise better the benefits of technology for society and the economy in ways which reinforce the rights and freedoms of individuals*."

In order to ensure a good understanding of what is expected from IoT objects, ecosystems and services to be "trusted", to be seen as "ethical" engagement with citizens/consumers is necessary – and a first step in that is making citizens/consumers aware. European level large scale pilots can play an important role here – and a dialogue up and beyond this will need to take place, at a multi-stakeholder level.

[1] Such a programme is recommended by the European Group of Ethic's Opinion 26 published in February 2012 and recent statements by Commissioner Kroes. These call for broad societal debate on trade-offs among comfort, security and privacy in order to promote a conscious development of an IoT world people would want to live in.

***Action proposal towards developing public awareness**: to actively stimulate and support reach out to the general public with information about IoT, and invite feedback, through IoT themed events for citizens and consumers, social media campaigns, etc., thus stimulating the emergence of a flywheel of awareness, mutual learning and feedback. See also the EDPS opinion (4/2015) and the DC IoT Good Practice declaration (2015).*

***Action proposal towards leveraging EU funding**: to require involvement/interaction with and active feedback from well informed citizens when there is European (co-) funding demonstrators and/or deployment projects.*

***Action proposal towards leveraging EU global influence:** to make IoT and underlying data streams and European values and legislation a key point in global diplomacy, whether in terms of trade, sustainability, privacy and data protection, internet governance, or on relevant sectoral platforms.*

Whereas much of the current drive is already coming from business opportunity, in particular IoT is very well suited for small and medium enterprises as well as startups. Creation of awareness on IoT opportunities and a healthy ecosystem for startup and growth of innovative companies is expected to have a strong impact on development of IoT.

***Action proposal towards raising awareness of entrepreneurs**: Continue to bring information about IoT developments and innovation opportunities into accelerator/ and innovator networks that foster entrepreneurship in SMEs. IoT can bring to those networks much inspiration, with abundant opportunities for innovation and startup business. At the same time, it is foreseeable that informing those networks of the IoT related opportunities will be like seeding in very fertile ground – a further boost of IoT related innovation can be expected when the right IoT innovation opportunity insights are shared with the right accelerator- and incubator networks.*

***Action proposal towards creating healthy ecosystem for startups**: for EU supported incubator and accelerator programmes to require contributions to relieving Europe's societal challenges (such as independent living, sustainability, etc.) by development of specific IoT based solutions – knowing that for the purely commercial initiatives, there is an increasing interest from commercial players to invest (thus European intervention for these type of developments are less needed).*

Whereas IoT is new in many respects, current legislation applies also to the IoT environment. However, this legislation was build prior to the emergence of IoT at large scale, and this is a game changer in many ways. In order to ensure that business invests in legally compliant applications of IoT without the threat of big fines or having to take out products or close down services, legal clarity should be provided on a number of issues.

Privacy and data protection

Action proposal leveraging EU funding towards better privacy and data protection*: to extend the obligation of carrying out Privacy Impact Assessments (PIAs) when developing IoT products, services and architectures. The PIA Framework in use for RFID following the requirements as spelled out in the European Commission's RFID Recommendation may provide good guidance for this. Require PIAs for products, services and architectures developed with EU funding.*

Action proposal on developing a global network on data protection and IoT*: to fund a network to develop solutions specifically allowing IoT developments to grow in a way that privacy concerns are addressed as well as possible, including development of a "global" code of conduct. As IoT is a global development, ideally this network would include partners from different regions in the world, including but not limited to China and USA.*

Consumer protection

Action proposal*: review European consumer legislation in the light of a new reality of "connected sensors and actuators" and the further move from "products" to "services" that is enabled by this.*

Competition regulation

Action proposal: *conduct open multistakeholder enquiries into the practice and effects of competition within the IoT and markets exposed to or reliant on its capabilities.*

Other domains relevant for IoT

Action proposal for developing a better understanding of what is needed: *stimulate an active dialogue between law and IoT developers to ensure the best possible understanding of what measures are necessary, and still allowing innovation of IoT to flourish and be applied in the interest of consumers and citizens. Note that this will require an ongoing dialogue for a number of years, as IoT is a fast moving area with a currently continuously changing landscape of applications.*

Action proposal ensure justified trust of citizens in IoT: *adopt a soft law framework to address the existing of gaps, duplications and inconsistencies in the framework of regulations affecting or affected by the IoT. (see also: Europe´s policy options for a dynamic and trustworthy development of the Internet of Things[30])*.

In line with these concrete policy recommendations, it may be useful to look at current engagements and stimulate European industry and in particular EU sponsored projects to actively participate in one or more of European and global multistakeholder platforms such as EuroDIG and IGF, where issues as trust, ethics and Human rights an inseparable part of the agenda when discussing technology progress in society. IoT is not just a technology issue: its emergence is a societal issue in which technology is merely just one of the perspectives.

-=(0)=-

1 Introduction

This Policy Paper on IoT Future Technologies focuses on specific policy issues that can assist or be assisted by the development of the IoT. In the full understanding that the IoT can be used for many different things by a wide range of stakeholders, and that acceptance, experience and continuing innovation of those stakeholders will determine the impacts of the IoT more profoundly than its technological specifications alone, the dominant theme in this paper is "trusted IoT", and includes reflections on topics such as big data / data protection, "security" and "ethical issues by design" that are crucial in this aspect.

The wider IoT policy context has been described in the paper "IoT and Society"[2] which contextualizes the IoT in relation to the Internet more generally[3]as a whole, big data, analytics and other ecosystem services connected to the floods of data unleashed by the IoT and cloud computing (as IoT devices are mostly part of a cloud and the resulting data are often stored, processed and shared via clouds). It is also recognized that the IoT forms an increasingly significant aspect of many different domains as well as constituting a domain in its own right. Nevertheless, its specificities must be addressed if it is to dispel the more extreme hype and fears and fulfill its potential to alleviate societal challenges and encourage and reward entrepreneurs.

In 2014, IoT became a major topic in every venue from the Board rooms of industry and the debating chambers of government to the halls of academe and the cafes where entrepreneurs seeing new opportunities gather. This is reflected in the position of the IoT at the top of the 2014 Gartner hype cycle.

[2] The Internet of Things and Society: paper Policy context for IoT towards 2020, deliverable D5.1 of the EU sponsored project Smart-Action, M. Botterman (2014)
[3]. Trends in connectivity technologies and their socio-economic impacts, for the European Commission DG Information society and Media. J. Cave, C. Van Oranje, R. Schindler, et al. (2009)

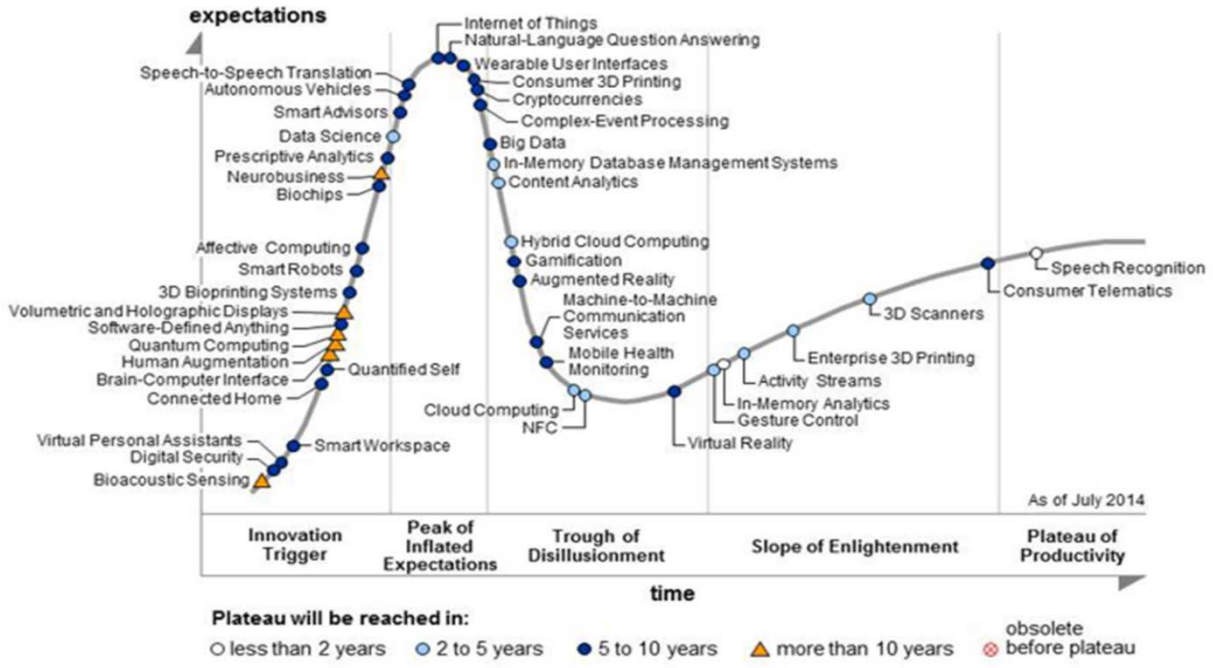

Figure 1: Gartner's 2014 Hype Cycle for Emerging Technologies[4]

IoT is both a necessity and a game changer. In order to help sustain the world, IoT will need to be accepted and adopted by the people whose needs it can serve. Chapter 2 explains the necessity of further IoT innovation and application for a sustainable world. Privacy is one of the key elements here, and both IoT and the underlying data streams have a major impact on availability of data that can be related to private persons. Security, safety and reliability are elements that greatly affect (justified) trust by users in the networks. And the Chapter makes extensive reference to the Sustainable Development Goals established by the United Nations in September 2015, which are derived from the UN Charter on Human Rights: aimed at creating "a Future we want".

The emergence of IoT is clear and - as a phenomenon - unstoppable. It is driven by societal needs and economic opportunities; by demand pull and supply push. It is enabled by many different strands of technology innovation application development in domains as varied as biotechnology, cognitive sciences and nano-technology. Instances are already seen in almost every area; the influence of IoT devices, services and architectures may rapidly become ubiquitous. These different forces inevitably produce transitory conflicts of interests, gaps and distortions for which trade-offs need to be made. Whether we as a society recognize and respond to the IoT as a "thing in itself" will greatly influence the effectiveness of our ability to exploit and eventually resolve these tensions. Chapter 3 illustrates this growing presence and thematic unity through examples of IoT applications already finding their way to the market. It is just "scratching the surface" and a chapter that can never expect to be fully up-to-date, as developments go incredibly fast. Some applications that we would have never thought of, two years ago, are already broadly used as examples in the field for some time.

[4] http://www.gartner.com/newsroom/id/2819918, retrieved 2015.01.03

Given this momentum and emergence, what role is there for policy? How can this development be assisted? To what opportunities and threats should society be exposed, and from which should it be protected? Whereas many aspects of European development are market driven, as a general rule there are significant 'market failures' – by which is meant the failure of markets to deliver efficiency, equity, innovation and quality of life improvements.

This is not new; many other aspects of European development are as strongly driven by politics and societal forces as by economic influences. Indeed, more than a few of the disruptive technological and business trends with which we struggle to cope have their origins neither in commercial nor political ambitions, but rather in curiosity, ethical and aesthetic urges. Each of these domains offers its own perspectives, often expressed in its own language.

In balancing and integrating them, markets play an additional critical role; monetization and trade enable values of all sorts to be created and captured, and the activities of widely disparate actors effectively coordinated. But markets do not inevitably run in this direction. They may drive towards fragmentation and monopoly, or lock-in and destructive externalities.

To operate effectively, the tendency towards concentrations of power must be kept in check and the operation of the system made more efficient (by facilitating exchange of information, reducing transactions costs, and by eliminating fragmentation and undue delays). These generic problems find particular realisation in the IoT; new actors (e.g. device designers or end-users) may have far more influence than current arrangements allow; the true functions and significance of specific devices and services may be diffuse or slow to be recognized; and the new ways of thinking and business process architectures and models necessary to nurture the IoT may be slower to develop (within Europe at least) than the technologies themselves or the business practices of global competitors.

In addition, both existing and novel societal issues may need to be addressed by society as a whole, or through new forms of public-private collaboration. Chapter 4 frames the most important policy challenges for the coming to address in order to help the IoT to develop optimally, and those (more general) policy challenges that this optimized IoT can help to tackle. The policy framework developed here is a response to the global challenges developing.

We conclude in Chapter 5 with concrete IoT policy action suggestions aimed at European stakeholders, for concrete consideration for action today. Next to initiatives that allow us to further develop IoT in a responsible way, while respecting the need for "permissionless innovation" other initiatives are more aimed at increasing the readiness of society – raising awareness, and growing an understanding what we talk about if we are aiming to develop together "a Future we want"[5] with a keen eye for "preserving human dignity"[6]

[5] The aim towards the future as expressed in the Sustainable Development Goals document from the UN
[6] The key priority as expressed by the EDPS in its Opinion on Data Ethics and Article 1, EU Charter of Fundamental Rights: 'Human dignity is inviolable. It must be respected and protected.'

2 Using IoT to help create "a future we want"

Recognising that IoT is upon us and will continue to become more pervasive, what aspects are crucial to consider when looking ahead towards a future of omniscience of IoT? It is clear: development and deployment of IoT is a global issue, and thus touches many different cultures and legislations. Global companies cannot find shelter for justification in one jurisdiction or culture if they want to sell products around the world, therefore companies with ambitions to supply IoT products and/or services in different parts of the worlds will need to find a way forward themselves that makes their products and services relevant, in the long run, in multiple markets around the world. Eric Schmidt, CEO of Google, says in an interview[7]:

"…Google believes we're organized around our end users. My general statement is that we've got lots of problems and regulations and rules and politics and issues and shareholders. But as long as we're on the side of the user, we've got a pretty good answer. That's always been true and it's allowed Google to get through a lot of stuff. We're not actually focused on the advertiser or the other competitors or so forth. We're focused on the user. Judge us based on that."

Several aspects are important here where basically all those consumers/citizens care about. And while understanding that values and habits vary around the world, a couple of those will be taken into account, simply because these are important to the current key markets (the major "old" markets as well as rapidly upcoming markets):

1. **Privacy and data protection** (even more so after the Snowden revelations in 2013, and as arguments related to this are "hot" in the current global political debate and have led to, amongst other things, a ruling from the European Court of Justice declaring the Safe Harbour Agreement between the EU and the USA invalid);
2. **Security, safety and reliability** (if a product is failing, leading to unsafe situations or even accidents, the world will know via social media and global news services, thus potentially dramatically affecting sales. If a product doesn't do what it promises, the world will know, too);
3. **Sustainable development** (globally recognised as a priority, it is recognised that for any development to be sustainable, environmental solutions can only work if they are also sustainable from a social and economic perspective. The Sustainable Development Goals that have been agreed by the UN General Assembly in September 2015 represent global norms, and include a clear call for connected technologies to contribute to achieving them. Please note that the SDGs also insist on "inclusive" use of connected resources).

These aspects are up and beyond the need for technical feasibility including standards (so that objects can interact, where necessary, and data can be shared, where possible), and spectrum availability.

[7] Eric Schmidt: 'How Google Works' Is All About the Customer Experience, Published on October 10, 2014 by Cory McNutt

In this Chapter, we will further discuss how these generally recognised values relate to IoT development and deployment, as a background against which effective policy measures can be developed in the full understanding that <1> IoT is global, and <2> the development and deployment of IoT is and only can be a multistakeholder issue.

2.1 Privacy and data protection

It is clear: in terms of pervasiveness, IoT has already contributed to the emergence of a society in which almost everything is or can be monitored, well beyond the descriptions as used by George Orwell in his book "1984"[8]. The novel is set in Airstrip One (formerly known as Great Britain), a province of the super state Oceania in a world of perpetual war, omnipresent government surveillance, and public manipulation, dictated by a political system euphemistically named English Socialism (or Ingsoc in the government's invented language, Newspeak) under the control of a privileged Inner Party elite that persecutes all individualism and independent thinking as "thought crimes". "Big Brother is watching you", and trust in society and freedom is sketched as very low. This book had a great influence of the thinking of a generation that grew up after World War 2 and reflects some of the thinking that is fundamental in the discussions about privacy.

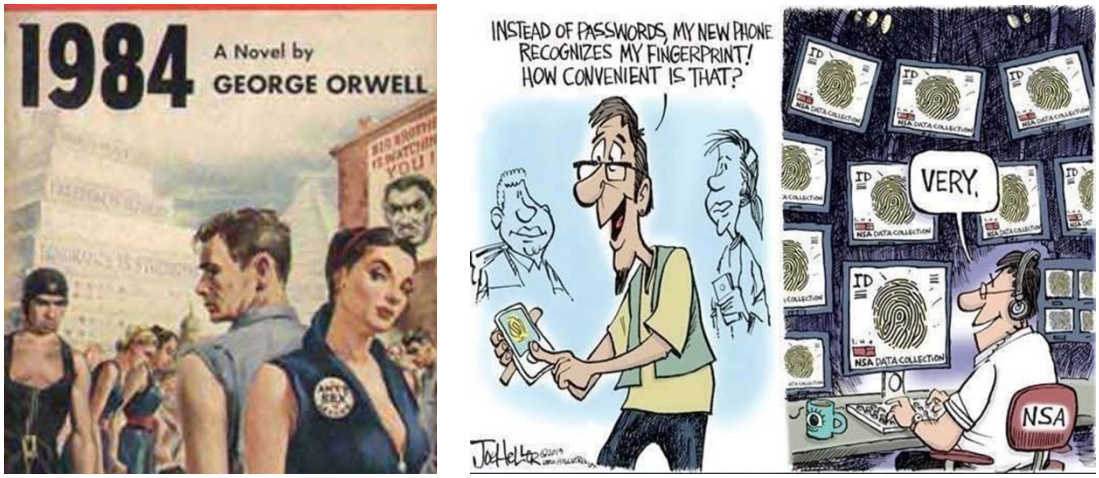

Figure 2: 1984, a society in which you can trust nobody – and "Big brother" sees it all … and a reality of pervasive monitoring by security forces in 2013[9]

Now: whereas the levels of monitoring are very high and well beyond the imagination of Orwell in terms of what technically is possible, in Europe trust in government and society has remained at a relatively high level. When Snowden revealed, starting in June 2013, some evidence reflecting the pervasiveness of monitoring through numerous global surveillance programs, many of them run by the NSA and the Five Eyes[10] with the cooperation of telecommunication companies and European governments, this resulted in widely expressed concern and even outrage by the general public, civil society and politicians.

[8] Orwell, George (1949). Nineteen Eighty-Four. A novel. London: Secker & Warburg.
[9] Gary Farvell, http://www.csmonitor.com/Commentary/Monitor-Political-Cartoons, retrieved 10 Jan. 2015
[10] "Five Eyes", often abbreviated as "FVEY", refer to an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States that was formed . These countries are bound by the multilateral Agreement, a treaty for joint cooperation in signals intelligence.

This led to a global discussion making clear that monitoring is a necessity, yet should be proportional, and not take place at all costs, and a balance is yet to be found. This results in a discussion that will continue to stretch over the decades to come.

Within this setting, the discussion in Europe about privacy and data protection is finding its way, moving from a Directive on Data protection and privacy towards European legislation. The reform is to strengthen individual rights and tackle the challenges of globalisation and new technologies, and "simplify" compliance by being applicable law in all EU member states, whereas the Data protection Directive originating from 1995 was applied by national governments in similar but not always the same way. In addition, the new General Data Protection Regulation (GDPR) offers Data Protection Officers to fine up to 5% of global revenue – and thus potentially impactful.

When the original Data Protection Directive was developed and agreed in 1995, the Internet was by far not as important as today, and nobody had even mentioned the term "Internet of Things" yet. The current reform has been under way since 2011 and culminated in a Proposal to Council and Parliament by the European Commission on 25 January 2012. This proposal was approved by the European Parliament in March 2014, and, although subject to amendment by the European Council, is expected to come into force in 2017. With this, it should be noted that the work has not been completed. When this law was set up in 2011, "big data" was not yet an issue widely recognised. Today, we know that big data, and big data analytics, fundamentally challenge the concept of "personal data" as through big data analytics data that in isolation do not relate to persons often can be related to persons when combined with other data.

The 2014 Opinion from WP29 on IoT recognises the value of IoT, as well as the potential intrusions it can generate to privacy. In this Opinion, statements are made that alarmed businesses around the world now asking for guidance to the European Data Protection Supervisor, as what is suggested may put a lock on many current developments in the field.

Business are looking for guidance on this, as big data is a subject of interest to many, and companies around the world are looking into the opportunities offered by big data, big data generation, collection, and analytics. IoT is a major driver in this, as "connected things" will generated endless streams of data that will be captured and used. According to the European Data Protection Supervisor Peter Hustinx[11]: "*If big data operators want to be successful, they should … invest in good privacy and data protection, preferably at the design stages of their projects*".

With this, he recognises the important of "soft law" at this point. Investing in good privacy and data protection should be core in the innovation, development and deployment of IoT, and probably a pre-condition for European (co-)sponsored research. A way forward could include the habit/obligation of a Privacy Impact Assessment in the design stage of new IoT products and services.

In his published Opinion[12] on Digital Ethics, the European Data Protection Supervisor (EDPS) refers to Article 1 of the EU Charter of Fundamental Rights: '*Human dignity is inviolable. It must be respected*

[11] Peter Hustinx according to Mark Say in the artcile "Big data needs big guidance" in FT, December 29, 2014. Retrieved http://www.ft.com/cms/s/0/fab4bae8-7f88-11e4-86ee-00144feabdc0.html#axzz3O8I1GAvc on 2015.01.07

[12] Opinion 4/2015, Towards a new digital ethics:Data, dignity and technology, EDPS, 11 September 2015

and protected.' From that position he further explains that: "*In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing*."

It is in line with this that some projects funded by the European Commission are looking very carefully at the issue of privacy protection and the idea of limiting the amount of information available to each entity. In general, the key issue to take into account while discussing privacy has to do with the integration of information from different sources. While a single stream of data might not contain enough information to invade the privacy of the user, the correlation and concurrence of information at an entity can lead to privacy considerations that were unthinkable only looking at the individual sources.

While the user is ultimately responsible for the data it allows to escape in the open, a modern individual that works and lives with current technologies cannot keep up with the types and amount of information being "leaked" by applications and websites. It is, therefore, for an individual virtually impossible to design privacy policies that are permissive enough to allow for services to work, while at the same time, restrictive enough that the privacy of the user is not compromised.

For this purpose, it is crucial that automated and self-configuring solutions are offered that analyze the type and amount of information given away for a specific user and configure the appropriate number of policies to ensure that the level of security and privacy desired by the user is kept untouched. This goes beyond mere regulatory actions and require robust and flexible technology solutions that work under very different conditions.

Of specific importance to the Internet of Things is also the ruling by the European Court of Justice in the case of Maximillian Schrems versus the Irish data protection commissioner regarding the right of Facebook to transfer data to servers located in the USA under the Safe Harbour scheme. On 6 October 2015, the Court declared the Safe Harbour Decision invalid, as the protections under the Safe Harbour scheme provided by the US Authorities had proven to be inadequate, in particular because "*the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements*" and because for non-US citizens there is no opportunity to redress: "*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection*".[13]

Currently, IoT providers such as the globally popular "Nest" smart meters and smoke detectors, owned by Google, still refer to "Safe Harbour Agreement" protection of personal data[14]. Whereas Nest explicitly commits to a number of privacy measures, it should be noted that today (2015) redress is thus not possible when a European citizen considers her or his privacy right to be violated. This is also true for companies such as Younqi (health bands) and many others that collect data and

[13] ECJ ruling in case C-362/14 Maximillian Schrems vs Data Protection Commissioner, 6 October 2015, see http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
[14] https://nest.com/legal/privacy-statement-for-nest-products-and-services/

store them on US servers. As these services are popular with many European citizens, solutions will need to be found.

It should be noted that negotiations on "Safe Harbour 2" are currently on their way, now including the intent to tackle the core issues that led to the ECJ declaring the Safe Harbour Agreement invalid. However, the fact that the new GDPR has not yet been finalised further complicates the completion of the negotiations between the European Commission and the US government.

Overall, it is noted also by the European Parliament that surveillance and collection of data should be proportional and justified, noting that new legislation is underway in multiple EU member states that would allow broad collection of data and tapping of internet communications: also including IoT.[15]

2.2 Security, safety and reliability

Security has been a high level concern of national states since the emergence of national states. However, as with environmental issues, over the last decades the world became even more aware of the need to work together on preventing damage to society through human mistakes, hostile attacks and/or natural disasters. IoT has played a major role in this, and vast innovations as well as roll-out of monitoring networks has taken place over the last decades, with clear "boosts" following the terrorist attacks to the Twin Towers and Pentagon in 2001 ("9/11") and the Tsunami disaster in 2004 (Indian ocean). Networks of increasingly density, with increasing in-build "intelligence", are rolled out to prevent disasters or provide at least early warnings.

Also in traffic, networks of sensors have been developed over recent years to provide warnings for fog, wind, changes in density and speed of vehicles, etc., and in-vehicle IoT systems are implemented at high speed to increase the safety of drivers and reliability of the vehicles – both on land, in the sea and in the air. The need for this is boosted by the increasingly intensive use of transport networks, and facilitated by the emergence of new technologies that make it possible to monitor and take preventive action in ways that were never possible before.

The Internet of Things was an explicit subject of the World Economic Forum's 2014 Global Risks Report[16]: "*First, the growth of the "Internet of Things" means that ever more devices are being connected online, touching many more parts of life and widening both the potential entry points for and impacts of disruption. Second, there is ever-deepening complexity of interactions among the many aspects of life that are dependent on connected devices, making those impacts potentially harder to predict.*".

The IoT takes the Internet to a new level of security risk. As the Global Risk report argues: "*In the past, cyberattacks typically had only a limited effect because they broke only ones and zeroes or things made of silicon. Organizations under attack might have a bad week, but after that they generally could execute business continuity plans, rebuild computers and use data from securely backed-up vaults. However, projects such as the Smart Grid – online connection of electrical power generation and transmission – are increasing the possibility of cyberattacks breaking things made of concrete and steel.*"

[15] NY Times, 27 October 2015: Europe is Spying on you: http://www.nytimes.com/2015/10/28/opinion/europe-is-spying-on-you-mass-surveillance.html?_r=0
[16] Global Risks 2014, report by the World Economic Forum, Geneva, 2014

In the 2015 Global Risk report[17], WEF repeats and further strengthens its warning: "*While the "Internet of Things" (IoT) will deliver innovations, it will also entail new risks. Analytics on large and disparate data sources can drive breakthrough insights but also raise questions about expectations of privacy and the fair and appropriate use of data about individuals. Security risks are also intensified. There are more devices to secure against hackers, and bigger downsides from failure: hacking the location data on a car is merely an invasion of privacy, whereas hacking the control system of a car would be a threat to life. The current Internet infrastructure was not developed with such security concerns in mind.*"

IoT is likely to disrupt business models and ecosystems across a range of industries. This may bring large scale disruptions to labour markets and financial markets, and a major public security failure could affect further development. In addition, the more dependent we become on our IoT supported environments, thus becoming part of our critical infrastructures, the more damage can be done to disrupt our societies. From this perspective, taking resilience into account when designing and developing IoT environments is crucial.

All data generated and stored in IoT environments are vulnerable to unauthorised use and/or abuse, and thus potentially subject to access control. The level of security will depend on the level of risk that is incurred when data are retrieved or IoT actuators are accessed by unauthorised systems or persons, and will vary. A well-argued risk assessment is crucial, including appropriate measures to mitigate the risks. Whereas there is already a lot of literature on "trusted ICT systems" IOT environments requires a specific risk classification due to their nature of connectedness.

Former US Vice President Dick Cheney's doctors disabled his pacemaker's wireless capabilities to thwart possible assassination attempts, said Cheney during an interview with CBS on Sunday 20 October 2013.[18] This is often referred to as "classical example" and it dates from a time that the capacity to do so was hardly present. Yet the Internet of Things progresses, and so do the vulnerabilities. An example of July 2015 that will be remembered for many years is the take-over of a Jeep Cherokee by two hackers, sitting at home. True, the car driver was forewarned, and happened to be a WIRED journalist. Yet they used a hacking technique—what the security industry calls a zero-day exploit—that can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles. Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.[19] Demonstrating this could be done to one car, shows that all vehicles that have wireless connections as such would be vulnerable to such attacks: whether on the highway, or maybe even in the air.

Next to clearly demonstrating that new developments (for instance: car makers tend to turn their cars more and more into "mobile phones" functionality) make society more and more vulnerable to attacks by hackers, it also shows that "connected things" (be it cars or otherwise) need to be protected in a way that the protection can be patched and/or upgraded, when necessary. In the case

[17] http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf, retrieved 2015.02.10
[18] Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking, Lisa Vaas in NakedSecurity, 22 October 2013, see https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/
[19] Hackers remotely kill a Jeep on a Highway; by Andy Greenberg, WIRED, 21 July 2015, see: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

of Chrysler, the patch has to be manually implemented via a USB stick or by a dealership mechanic. It is inevitable that ultimately all car manufacturers will follow the example that Tesla sets already today – updates will be transmitted wirelessly to all registered cars.

Next to different categories of IoT applications with different levels of vulnerability, ranging from protecting against unauthorised access to data collected and/or stored by the device to "connected actuators" that can be remotely influenced (for instance by uploading fake data) or even controlled (like the car), there is also the level or protection. The time that a security key could be baked in to a chip is past – and systems will no longer be reliable when many systems are protected by one and the same password – as cracking that password would make many more objects vulnerable than the one that was attacked. Security is a continuous race between those that attack and those that defend. This means that no system that would be considered "secure" today, can be deemed to stay secured, indefinitely. A clear warning regarding this can be found in the paper, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice[20]" in which authors claim that a massively resourced agency such as the NSA could build enough custom hardware that would crack the prime number used to derive an encryption key. Once enough information is known about the prime, breaking Diffie-Hellman connections that use that same prime is relatively trivial. They warn that breaking one code would thus lead to a great number of encryptions becoming decryptable. This means that new systems are to be designed with dynamic security connections, or at least to allow change of the security code when deemed necessary.

In terms of safety, IoT products are subject to general product safety legislations[21] that are often sector-related, and subject to sector regulation. Safety requirements can be much higher when IoT is applied in specific environments for specific purposes, such as in vehicles, in buildings, in medical equipment, etc. Hence, it is crucial that specific application areas are considered when a new product is developed for the purpose of these specific applications. Next to the security of access, there are thus also requirements re: the functioning (and testing of the fail-safe of the functioning).

Overall, it is fair to say that appropriate measures to ensure security, safety and dependability should be considered in early phases of the design process as to ensure that IoT can be deployed and used in a responsible way. In addition, there is a plea to ensure that systems are "open" thus subject to "public" scrutiny. "Public" is here between brackets, as some technical expertise will be required, yet the fact that others can check whether the statements made by the developer of the product are correct is generally believed to lead to better code, and to systems actually doing what they are mend to do, and not something else. The Volkswagen emissions scandal, though not precisely an Internet of Things issue, has exposed yet another issue with "smart" physical goods: the possibility of manufacturers embedding software in their products designed to skirt regulations. Another example is the mistrust of electronic voting machines– both systems were closed and not accessible for scrutiny. Openness allows uncovered terrifying vulnerabilities in products ranging from cars to garage doors to skateboards.[22]

[20] See https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf
[21] For instance Directive 2001/95/EC on general product safety, O.J. 2002/01/15
[22] VW's cheating proves we must open up the IoT, Klint Finley, WIRED, 24 September 2015

2.3 Sustainable development

Our world is under severe stress by the way we are using it, and life as such will not be sustainable in the long run, unless we find a way forward that is sustainable. According to the Brundtland Commission in their famous report to the UN General Assembly in 1987, "Sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their own needs"[23].

The three main pillars of sustainable development include economic growth, environmental protection, and social equality: it was recognised that there will be no sustainable development unless solutions found take all three pillars into account. A world cannot be sustainable, ecologically, if there is no economically viable solution. And even if a solution is ecologically right, and economically viable, but not addressing societal needs, this will lead to social unrest related to unfair distribution of wealth, choice and opportunities.

Since 1987, many policies have come in place to address the issue of sustainability: it is now a high priority item on the political agenda, globally, regionally, nationally and locally. Since 1987, the world population has risen to over 7 billion today, and projections by the UN towards 2050 very between 8.3 and 10.9 billion people in 2050[24]. The ecological footprint (i.e. the number of hectare necessary to sustain the current level of living without impeding the consumption by future generations) already exceeds for more than 40 years what our planet can replenish, according to the latest Living Planet report.[25]

Since it became widely available in the 1990s, the Internet has enabled new products and services, improved economic efficiency, transformed access to information, and facilitated greater collaboration between governments, businesses and citizens. Its growing impact has been central to the emerging Information Society and digital economy, affecting both developed and developing countries. As many as 40% of the world's people now use the Internet at least occasionally, a proportion that is growing every year.[26] Its development potential was emphasized in the World Summit on the Information Society (WSIS, 2003/2005) and will be further demonstrated when the UN reviews WSIS outcomes in December 2015.[27] ISOC engaged with the Sustainable Development Goals (SDG) process in particular to ensure the potential role of the Internet was well understood.[28]

---

[23] Our Common Future, Report of the World Commission on Environment and Development, World Commission on Environment and Development, 1987. Published as Annex to General Assembly document A/42/427, Development and International Cooperation: Environment August 2, 1987. Retrieved, 2015.02.01

[24] "World Population Prospects, the 2012 Revision – "Low variant" and "High variant" values". UN. 2012. Retrieved 2015.01.02

[25] Living planet report 2014, WWF and Global Footprint Network, Water Footprint Network, ISBN 978-2-940443-87-1 http://wwf.panda.org/about_our_earth/all_publications/living_planet_report/ecological_footprint/. Retrieved 2015.01.02

[26] ITU, 2014, p.15

[27] A comprehensive review of WSIS outcomes by the secretariat of the UN Commission for Science and Technology for Development can be found in UN CSTD, 2015.

[28] The Internet and Sustainable Development: an Internet Society contribution to the United Nations discussion on the Sustainable Development Goals and the 10-year Review of the World Summit on the Information Society, see: http://www.internetsociety.org/sites/default/files/ISOC-ICTs-SDGs-201506-1.pdf

Sustainable Development Goals and IoT

In the process, over time, the Internet became universally underlined as key for Sustainable Development. IoT application is a necessity in pursuit of some of the Sustainable Development Goals[29] that were established in September 2015 following the Millennium Summit of the United Nations in 2000, as an action plan upon Universal Declaration of Human rights[30]. IoT connected objects will be able to cover large areas for monitoring and collecting information that will help with early warnings for accidents and natural disasters, will help better understand what is needed for specific purposes by measuring, and will partly be able to handle autonomously when triggered to do so by measured values.

Figure 3: UN Millennium Development Goals and beyond 2015

[29] http://www.un.org/millenniumgoals/ Accessed 2015.01.04
[30] http://www.un.org/en/documents/udhr/ Accessed 2015.01.04

As such, ultimately all goals will be affected by the ongoing digitization of our societies. In particular, the Internet of Things will be of immediate value for contributing to the achievement of a good subset of the SDGs, which will be discussed, below:

- **Goal 2. End hunger, achieve food security and improved nutrition and promote sustainable agriculture:** sub-goal 2.3 By 2030, double the agricultural productivity and incomes of small-scale food producers, in particular women, indigenous peoples, family farmers, pastoralists and fishers, including through secure and equal access to land, other productive resources and inputs, knowledge, financial services, markets and opportunities for value addition and non-farm employment; sub-goal 2.4 By 2030, ensure sustainable food production systems and implement resilient agricultural practices that increase productivity and production, that help maintain ecosystems, that strengthen capacity for adaptation to climate change, extreme weather, drought, flooding and other disasters and that progressively improve land and soil quality

IoT will help manage crops, and resources that enable food production by providing insight in the state of the resources and the state of the crop (networks of sensors) and increasingly by taking action when needed (such as irrigation, fertilising, fighting diseases), either autonomously or by signalling farmers. In addition, it will help detect emerging natural disasters thus allowing measures to be taken to prevent or limited damage and prepare for recovery.

- **Goal 3. Ensure healthy lives and promote well-being for all at all ages:** sub-goal 3.6 By 2020, halve the number of global deaths and injuries from road traffic accidents; sub-goal 3.9 By 2030, substantially reduce the number of deaths and illnesses from hazardous chemicals and air, water and soil pollution and contamination

IoT can help with road quality and traffic management by signalling imminent dangers such as proximity, or deterioration of infrastructures. Networks of sensors can also be put in place to detect hazardous chemical and pollution, and extend warnings (or even act, for instance by closing a dam).

- **Goal 6. Ensure availability and sustainable management of water and sanitation for all:** sub-goal 6.3 By 2030, improve water quality by reducing pollution, eliminating dumping and minimizing release of hazardous chemicals and materials, halving the proportion of untreated wastewater and substantially increasing recycling and safe reuse globally; sub-goal 6.4 By 2030, substantially increase water-use efficiency across all sectors and ensure sustainable withdrawals and supply of freshwater to address water scarcity and substantially reduce the number of people suffering from water scarcity; sub-goal 6.5 By 2030, implement integrated water resources management at all levels, including through transboundary cooperation as appropriate; sub-goal 6.6 By 2020, protect and restore water-related ecosystems, including mountains, forests, wetlands, rivers, aquifers and lakes

In terms of water management, again both sensors and water management systems will be a crucial element of preventing dumping, and alerting in case of hazardous chemicals and materials in the water. It will also help in distributing water efficiently, in a sustainable way.

- **Goal 7. Ensure access to affordable, reliable, sustainable and modern energy for all:** sub-goal 7.2 By 2030, increase substantially the share of renewable energy in the global energy mix; sub-goal 7.3 By 2030, double the global rate of improvement in energy efficiency; sub-goal 7.b

By 2030, expand infrastructure and upgrade technology for supplying modern and sustainable energy services for all in developing countries, in particular least developed countries, small island developing States and landlocked developing countries, in accordance with their respective programmes of support

Infrastructures, including energy infrastructure, become much more effective and reliable thanks to integration with sensors and switches that manage it, detect failures, and increasingly also allow two-way energy streaming.

- **Goal 8. Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all:** sub-goal 8.2 Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors; sub-goal 8.3 Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalization and growth of micro-, small- and medium-sized enterprises, including through access to financial services

IoT is not only directly applicable in terms of sensors and actuators that are connected and can together perform services: it is also an opportunity, as it is very much scalable and distributed as a technology. With modest investments, first steps towards IoT enabled solutions become possible. This does not only allow entrepreneurship and startups to take place with minimal resources, it also potentially brings IoT applications to where solutions need to be provided.

- **Goal 9. Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation:** sub-goal 9.4 By 2030, upgrade infrastructure and retrofit industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies and industrial processes, with all countries taking action in accordance with their respective capabilities; sub-goal 9.c Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020

Sustainability comes with feedback loops, and IoT networks are very well suited to provide this feedback. Increasingly, knowledge will be embedded in systems that will act, and in order to not further widen the gap access to and implementation of these kind of technologies need to be included in the Goal 9 activities.

- **Goal 11. Make cities and human settlements inclusive, safe, resilient and sustainable:** sub-goal 11.4 Strengthen efforts to protect and safeguard the world's cultural and natural heritage; sub-goal 11.5 By 2030, significantly reduce the number of deaths and the number of people affected and substantially decrease the direct economic losses relative to global gross domestic product caused by disasters, including water-related disasters, with a focus on protecting the poor and people in vulnerable situations; sub-goal 11.6 By 2030, reduce the adverse per capita environmental impact of cities, including by paying special attention to air quality and municipal and other waste Management; sub-goal 11.7 By 2030, provide universal access to safe, inclusive and accessible, green and public spaces, in particular for women and children, older persons and persons with disabilities

Networks of monitoring systems and sensors will be able to detect natural disasters building up, such as the tsunami wave alert system, and systems developed to provide early warning in case of earthquakes, hurricanes, volcano eruptions, etc. Early warning will provide the opportunity to prevent or limit damage. Partly, autonomous protection systems can be build in (like closing dams). Monitoring also helps in keeping public spaces safer – as the introduction of CCTV in the UK has proven following the murder on the 2 year old James Bulger in 1993. Cities around the world have started to experiment with IoT applications in many ways, ranging from intelligent waste collection to smart lighting, city bikes on subscription basis to smart traffic management systems and alerts for unhealthy pollution levels.

- **Goal 12. Ensure sustainable consumption and production patterns:** sub-goal 12.5 By 2030, substantially reduce waste generation through prevention, reduction, recycling and reuse; sub-goal 12.6 Encourage companies, especially large and transnational companies, to adopt sustainable practices and to integrate sustainability information into their reporting cycle

This also benefits from feedback loops that become possible thanks to the use of tags and sensors in materials. In more and more cases maintenance will no longer be needed on a "regular" basis, but when needed, as indicated by the object that may require maintenance, such as cars, industrial machines, etc.

- **Goal 13. Take urgent action to combat climate change and its impacts:** sub-goal 13.1 Strengthen resilience and adaptive capacity to climate-related hazards and natural disasters in all countries

As indicated above, signalling systems, feedback loops and even actuators will help us taking the best possible measures.

- **Goal 14. Conserve and sustainably use the oceans, seas and marine resources for sustainable development:** sub-goal 14.a Increase scientific knowledge, develop research capacity and transfer marine technology, taking into account the Intergovernmental Oceanographic Commission Criteria and Guidelines on the Transfer of Marine Technology, in order to improve ocean health and to enhance the contribution of marine biodiversity to the development of developing countries, in particular small island developing States and least developed countries

With IoT, measuring a wealth of elements in a wide area has become possible that will help us understand what wasn't overseeable, before. Big and small data will help us combine information in ways that will allow us to learn much about what is going on, and what works to make things better.

- **Goal 15. Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss:** sub-goal 15.1 By 2020, ensure the conservation, restoration and sustainable use of terrestrial and inland freshwater ecosystems and their services, in particular forests, wetlands, mountains and drylands, in line with obligations under international agreements

As above.

- **Goal 17. Strengthen the means of implementation and revitalize the Global Partnership for Sustainable Development:** sub-goal 17.7 Promote the development, transfer, dissemination and diffusion of environmentally sound technologies to developing countries on favourable terms, including on concessional and preferential terms, as mutually agreed; sub-goal 17.8 Fully operationalize the technology bank and science, technology and innovation capacity-building mechanism for least developed countries by 2017 and enhance the use of enabling technology, in particular information and communications technology

As said: IoT helps to generate the data we need to better understand what is going on, and to learn. As it is scalable technology with a relatively low threshold to develop and deploy, people around the world can learn from each other and will be able to better address societal and practical challenges in their immediate environment.

It is thus clear that the tension on our ability to sustain our world for future generations needs to be addressed making use of connected, scalable technologies. Awareness raising on waste and usage of resources, active stimulation of more "clean" technologies and less material use, and other measures of ecological, economic and social policy nature are under way to address this. Technology is already noted to help: the 2014 Living Planet Report says: "Technological advances, agricultural inputs and irrigation have boosted the average yields per hectare of productive area, especially for cropland, raising the planet's total biocapacity from 9.9 to 12 billion global hectares between 1961 and 2010." It is clear that IoT is a necessary complement to help address the challenges ahead, both in terms of monitoring the environment (e.g. air quality) and taking preventive action (such as closing the pipe when the stream becomes too polluted, or indicating speed limits and highways in case of smog alert).

In order to be able to do so, it will be important to continue to innovate thus ensuring emergence of effective IoT technologies and IoT related services that are affordable and widely available. Current IoT developments already contribute considerably to a more sustainable world, and more will need to be done. When designing IoT products, waste, use of materials, and re-use of materials will be important considerations, taking into account the number of devices. A study on RFID and Waste concluded that the presence of passive RFID tags in waste streams does not necessarily raise major 'red flags' in terms of waste treatment. Active RFID tags (those with their own power source), fall under the WEEE Directive, and are expected to remain much less in number. Nevertheless, it was considered important and possible to even further reduce the impact of RFID on the yield of recycled materials (such as glass or plastic) from tagged objects, by design changes that ensure that RFID tags can be easily removed at the end of life (e.g. attaching them to lids or labels rather than the recyclable objects themselves) and ways to incorporate recyclability in the design phase of products and/or packaging[31].

Other aspects of sustainability strongly interrelate with security, as well. From a societal perspective, a major security failure could also prevent the IoT from becoming truly widespread (as was also recognised by the WEF 2015 Global Security report). Privacy and data protection issues can lead to

[31] RFID and Waste: Towards a Sustainable Solution, report on a workshop held on 12 July 2012, organised for the European Commission DG INFSO. Workshop report retrieved 2015.01.07 at http://www.gnksconsult.com/site/images/stories/rfid_and_waste_community_launch_workshop_report_final_v4.pdf

major setbacks, when not taken into account from the outset. And the additional challenge is that regulatory mechanisms to deal with IoT will ultimately need to be agreed upon at international and national levels.

Whereas "batteries" affect the environmental sustainability of IoT, it is also one of the examples where it directly affects the economic aspects. Whereas the development and proof of concept testing of IoT solutions can be done with batteries that provide power where necessary, in a widespread application of connected sensor (and actor) networks, replacing batteries may turn out to be economically expensive and possibly not viable in the long run. The same goes for identification of different nodes (allowing a change of service providers?) and upgrades of nodes (software/hardware).

In conclusion, IoT products and services are crucial in the race towards sustainability, and to avoid that IoT products and services become polluters in themselves, active attention needs to be given to the design of IoT products, in particular when in the need for an independent power source. As the Living planet report 2014 says: "We cannot conjure perpetual growth out of a closed system [i.e. the planet Earth] – but we can make the system work better".

Eradicate hunger in a world with a continuously growing population means that resources will need to be used more and more intensely, and in a way that it does not lead to depletion – otherwise the problem of "feeding the world" gets only bigger over time. In 2050, 9 billion people need to have access to good quality, safe food. Whereas there are many elements towards fighting hunger around the globe, it is clear that it will require more intense use of natural resources, and more intense production systems – as much as possible implementable locally, around the world, also building on the understanding of a changing environment re: climate and CO2. This is referred to as "Climate Smart Agriculture" and addresses both climate changes directly, and making best use of technology. Ultimately, this will require affordable connected systems and IoT to help monitor and manage environments and processes.

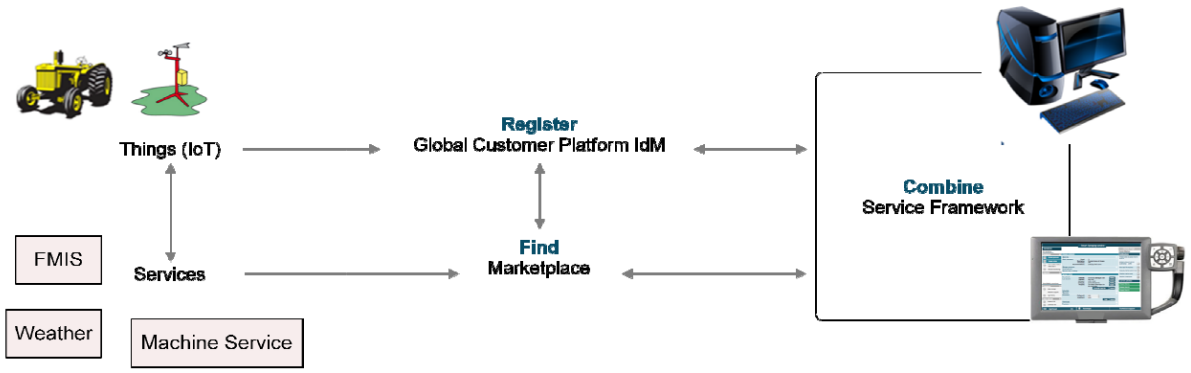

Figure 4: FI PPP Smart Agriculture framework of services

The European Commission sponsored within the Future Internet PPP (FIWARE PPP[32]), the SmartAgriFood projects focusing on sustainable food production. It argues that the intelligence,

[32] See http://www.fi-ppp.eu/

efficiency, sustainability and performance of the agri-food sector can be radically enhanced by using information & decision support systems that are tightly integrated with advanced internet-based networks & services. This project focuses on three sub systems of the sector – smart farming, focussing on sensors and traceability; smart agri-logistics, focusing on real-time virtualization, connectivity and logistics intelligence; and smart food awareness, focussing on transparency of data and knowledge representation. Using a user-centred methodology, the use case specification will be developed with a particular focus on transparency and interoperability of data and knowledge across the food supply chain.

Human rights can be affected, too, as was recognised by the stakeholder involved in the United Nations conference to agree on Sustainable Development Goals. On a global level, this has led to the creation of a Dynamic Coalition on Internet of Things in 2008, as part of the Internet Governance Forum[33]. In this coalition, stakeholders from different sectors gather to discuss the practical and societal aspects of IoT, to ensure a way forwards is found that is sustainable and in respect of Human rights. During the 10th IGF meeting in Joao Pessoa, it was recognised that IoT is a game changer that affects the ways in which we can address human rights. There was a call for developing further clarity on this.

[33] http://2014.intgovforum.org/event/c2879b04fc6b8839fc49947924b6efb8#.VAgd5mNQTO0 Accessed 2015.01.08

3 IoT addressing societal challenges today

By the time this report is published, the examples of IoT technologies addressing societal challenges below will already be overtaken by new developments – yet the overview as such helps us understand in more concrete terms how pervasive the difference can be that IoT makes towards our lives right now, and towards a more sustainable world in the longer term.

3.1 Environmental monitoring

A wide array of environmental monitoring devices has become available over the last couple of years. They vary from specific products to monitor large geographic areas in ways that otherwise would be impossible to local, personal devices that become part of a cloud of sensors that tell you about your immediate environment, and aggregates the data from multiple users often part of a service provision. Three examples ranging from air quality to animal location tracking are given below:

The **Air Quality Egg** (AQE) is presented as an Open source hardware Internet of Things platform and hobbyist device for crowdsourced citizen monitoring of airborne pollutants. It is a device that uses sensors to collect and share data about the air quality outside a person's home or office. While government agencies monitor pollutants daily from centralized locations, the Egg collects data in real time from its user's immediate environment. The base station relays the air quality data over the Internet where a website aggregates and displays data from every Egg in operation. This real-time data can be used to design and measure the impact of urban pollution policies and changes. It also encourages residents to learn more about their city and understand how their actions impact their community. Air Quality Eggs can be found across North America, Western Europe and East Asia and may eventually play a role in developing countries with the most rapid urban population growth and highest rates of pollution.

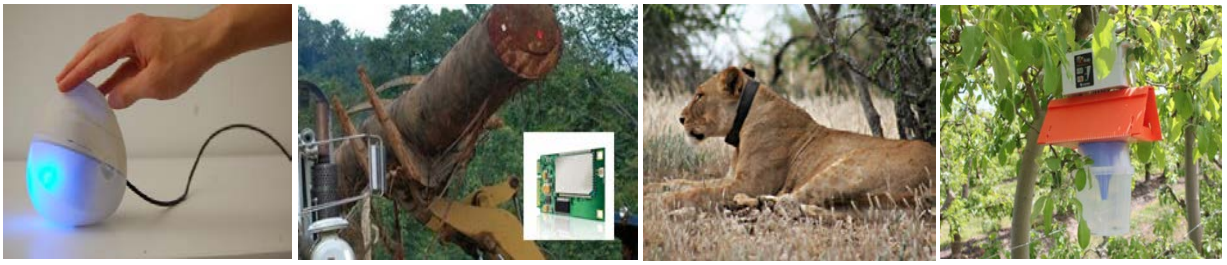

Figure 5: Environment monitoring: air quality, illegal logging, lion tracking and insect traps

Invisible Tracck is a small device covertly placed in trees in protected forest areas to help prevent illegal logging. The devices, which are smaller than a deck of cards, alert authorities when illegally harvested trees pass within range of a mobile network. It is designed to withstand the climate and can be detected up to 32 km beyond the usual range of the nearest mobile network. When illegal loggers collect timber in protected areas to take it to a mill, the hidden device sends location updates to law enforcement. It was developed by Cargo Tracck in response to a call to reduce illegal logging in the Brazilian rain forests. According to Greenpeace, illegal timber accounts to between 60/80% of all logging, and there was no effective way to address this.

Ground Lab´s open source **Lion Tracking collars** are to help conservationists protect the last 2000 lions living in the wild in Southern Kenya, and at the same time safeguard the Maasai herders cattle by warning the Masai for presence of lions in the area. The focus of the project is specifically on implementing techniques to reduce predator-livestock conflicts, by employing the Maasai warriors to conserve rather than kill.

Insect traps help to detect presence of insects in, for instance, agricultural areas. Z-Trap is an electronic insect trap that helps farmers remotely monitor an insect population and protect their crops from insect damage. In 2010, insects cost U.S. farmers around $20 billion in damaged crops and an additional $4.5 billion for insecticide. Z-Trap helps prevent crop damage by using pheromones to trap insects and then compile data on the number of different types of insects in the trap. Z-Trap wirelessly transmits the data, including its GPS coordinates, allowing farmers to view a map of the types of insects that have been detected. By remotely monitoring pests, farmers can place traps at a density dictated by specific needs, thereby saving time and money and minimizing the use of insecticides.

3.2 Natural disasters relief

Many means are already in use to get advance warning, in particular metrological networks of sensors, and satellite observation. Nowadays, weather forecast get much more refined and locally relevant because of the enormous growth of the number of sensors that are increasingly sharing data. Similar approaches are also used to enhance the warning time for natural disasters such as earthquakes, tsunamis, hurricanes and landslides.

Tsunami warning systems are high on the priority lists since the 2004 tsunami in the Indian ocean. In 2014, the U.S. federal National Oceanic and Atmospheric Administration (NOAA), completed the buoy network and bolstering the U.S. tsunami warning system. This vast network of 39 stations provides coastal communities in the Pacific, Atlantic, Caribbean and the Gulf of Mexico with faster and more accurate tsunami warnings. These final two deep-ocean assessment and reporting of tsunami (DART) stations, deployed off the Solomon Islands, will give NOAA forecasters real-time data about tsunamis that could potentially impact the U.S. Pacific coast, Hawaii and U.S. Pacific territories.

Figure 6: Monitoring and warning for tsunami, landslides, and weather changes

Slope failures worldwide result in many thousands of deaths each year, and for billions on damage to civil infrastructures. British Geological Survey developed a Landslide alarm system that is based on early observation of increased acoustic emission levels (high-frequency stress waves) due to inter-particle soil friction and displacement. For the system (called ALARMS – Assessment of Landslides using Acoustic Real-time Monitoring Systems) special “sensors” have been developed by

drilling holes and filling it with sand and gravel to make movement easier to detect. The sensors allow thus early detection which is expected to save lives and eventually take measures to avoid or limited damage.

Meteorological warning systems increase the number of nodes for measuring different elements of the weather, and connect them, thus being able to dramatically improve weather forecasts, and at a higher granulation. For instance, meteorological monitoring can be integrated in rail networks, city lighting, and many more objects and systems.

3.3 At home

In the home, IoT is expanding rapidly. Whereas only ten years ago most households had only one internet access point, if any, most have at least two, today (e.g. mobile and fixed line or cable). And whereas only the PC was on-line at that time, since then many households adapted smart phones, and smart tvs, and also smart meters, smart thermostats, camera´s and more are now rapidly coming on-line, all collecting data and providing services. When buying a new washing machine today, it may well be that it can be monitored and instructed from a smart phone, from any location in the world!

Smart meters provide real-time, two-way communication between customers and the utility and enable a number of benefits. Smart meters allow customers to receive granular detail about their electricity usage and to modify their energy consumption according to price signals. Dynamic pricing facilitates the use of renewable energy sources like wind and solar, which are highly variable. For example, cheaper rates incentivize customers to use these sources when the additional capacity is available. Smart meters also allow utilities to collect electricity usage information automatically, rather than manually sending someone to manually read the meter. Automatic detection of outages can also lead to faster repairs.

When the European Directive on energy end/use efficiency and energy services was adopted, it included an article on metering (art.13) in which existing meters, when replaced, would be replaced with smart meters (”if and when reasonable”). What was only discovered after this was that with those smart meters many data related to usage of electricity in the household could be deducted, including, by extension, which tv programme was watched at what time.

Figure 7: Smart thermostats, smart meters and smart lighting, just examples of IoT in the home

Thermostats can help homeowners consume less energy, savings paying back their initial investment cost in under two years. By now, a wide range of different types of sensors are available: activity sensors that detect whether someone is home, humidity sensors, weather sensors, and

temperature sensors that detect how quickly the temperature changes. Nest, for instance, collects data to learn the daily routine of users and their temperature preferences, and then combines this with outdoor weather data to tailor the home's heating and cooling settings based on the time of day and whether anyone is home. Users can often control their thermostat remotely from their smart phone or computer. Finally, Nest sends users a monthly energy report, as well as other alerts, such as when it is time to change air filters, which can reduce heating and cooling bills by 5 percent.

Lightning is now rapidly adopting sensor techniques, adding movement or ambient light sensors, and including internet nodes allowing communication has become easy and is expected to change the landscape of home lighting over the coming years. ON World predicts that LED wireless light bulbs will be one of the fastest growing IoT market over the next decade, forecasting that by 2020, more than 100 million wireless light bulbs and lamps with IP addressed will be installed, up from 2.4 million in 2014[34].

3.4 Personal care

With the ongoing miniaturization of devices and wireless connectors, sensors can now be seamlessly integrated in our household, our clothes, and even our body. The first medical aid object that was recognized to be part of the Internet of Things was the pacemaker from Dick Cheney, as it reached the world news that his doctor made sure his pace maker could no longer be " instructed" from the outside. Yet whereas integration of technology comes with new dangers, we find often that the benefits are greater.

One such examples is the CardioMEMS **Heart Sensor**. This is an implantable medical device for monitoring heart failure. Heart failure affects many people around the world and costs a fortune in health care services, medication, and lost productivity. The device, which is about the size of a paper clip, is implanted into a patient's pulmonary artery using a minimally-invasive technique and measures pulmonary arterial pressure. Data from the device is collected wirelessly and transmitted to a central database for the patient's health care providers to review. A rise in pulmonary arterial pressure is the clearest sign of a potential problem. In a randomized clinical trial, the CardioMEMS Heart Sensor resulted in a 30 percent reduction in hospitalization rates in heart failure patients after six months.

Figure 8: implantables, aids to enhance our health care, wearables that can measure, provide feedback and warn

Asthma has enormous negative impacts on children, resulting in 100 million missed school days and 10 million emergency room visits per year in the United States only. GeckoCap is a "smart" button that can be attached to any inhaler to remind children to use their inhaler and automatically

[34] Smart Wireless Lighting: a market dynamics report, ON world, Q4 2013 http://onworld.com/smartlighting/

record each time it is used. The data is automatically stored in the cloud, allowing parents and health care providers to view the usage history through an online interface as well as discover if the inhaler is running low. Parents can also use the online interface (app on smart phone or tablet) to set goals to encourage their children to develop healthy habits and provide them rewards for adhering to a medication regimen over time.

A similar system is developed to improve **medication adherence**. Diabetes patients with low levels of adherence have health care costs almost twice that of those with high levels of adherence. A smart pill bottle that reminds patients to take their medication helps. It even escalates reminders that include flashing lights, audio reminders, SMS messages, and phone calls. The pill bottle detects when a patient opens and closes the bottle and records that the patient has taken a dose. This information is transmitted over the mobile network. Patients can allow their doctors, family members, or other care givers access to their medication adherence reports.

The fridge that knows when to order a new pack of milk is one of the oldest examples of IoT, and still today it is not clear whether such an application will really reach the market at some point. However, if a fridge is left open for more than 5 minutes, it may be useful to alert the persons in the household that one may have forgotten to close it. For this, Lively is developed as a system composed of activity sensors placed on objects around the home that **monitors the daily behavior** of an individual living alone. Lively uses a pill box, and car keys to collect data on an individual's eating, medication, and sleep habits. The system unobtrusively learns a person's routine over time and then can alert family, friends, or caregivers of changes that may indicate a problem. Since many older adults lack Internet access, Lively transmits the data using mobile networks.

Wearables are coming in the market at high speed. Google glasses are widely known today. NIKES include now Bluetooth Smart sensors, enabling everyone from pro athletes to incidental runners to learn a lot more about their workouts and athletic performances. The information can be sent wirelessly to a Bluetooth hub device (in Nike's case, an iPhone or iPod Touch) and shared with friends via the Nike+ Training app, online or through social media. The Nuubo Smart Shirt is a sensor-equipped shirt that monitors a patient's vital signs and movement. The sensors in the shirt can take regular measures on items such as heart rate, blood pressure, and body temperature. In addition, it can conduct an electrocardiogram (ECG). The shirt sends data wirelessly to a server for data analysis where, for example, software can detect anomalies in the ECG. Since the shirt allows people to move around, it has potential applications for patients in hospitals, low-risk patients at home, and athletes in training. The shirt also includes a GPS so health care providers can locate patients in the event of an emergency.

3.5 In the City

City environments are intensively used, and IoT can help improve the experience of city life in many ways and help respond to major societal challenges such as climate change, ageing populations, the move to online retail and micro-deliveries, etc. So-called "smart cities" use digital technologies to improve on performance of the public services and wellbeing of the citizens, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens. Key 'smart' sectors in city environments include transport, energy, health care, water and waste. It supports the ability for citizens to more directly participate in governance and maintenance of the city.

More and more cities are seeking ways towards "becoming smarter", often triggered from one domain, such as "city lighting", energy delivery, or dynamic traffic (and parking) management, using this as an access point to further unlocking of the potential of connected, communicating sensors and actuators that generate and share data.

Figure 9: smart waste-bins, smart lighting, bike sharing

Waste is a major issue in city agglomerations, and multiple cities have addressed this by setting up smarter ways of collecting waste, both in terms of having citizens to bring it to collection points near the house (in some cities with electronic access cards to the waste bin, for "locals only") and smarter planning of collection of waste by signaling of waste levels per bin and smart routing for waste trucks. The picture above is from Barcelona. These compact drop-off containers have a subterranean vacuum network through the pipes, sucking up trash below the ground. This automated waste collection system decreases noise pollution made by trash trucks and keeps the public space and stench clear. Where this wasn't possible, sensors on rubbish and recycling bins have also been tested. Through radio frequency and WiFi, the sensor gives data to a central system, detecting the trash level. Sanitation workers can then plan the optimal route and times to collect it.

Smart lighting is the starting point for the city of Eindhoven to start development of a smart infrastructure with data sharing. Via public procurement, suppliers are sought that not only ensure there is enough light ("to the satisfaction of citizens") but also an infrastructure that can support data sharing from sensors and actuators, enabling a wealth of new and smart services for citizens to develop, either driven by the city or by local entrepreneurs, making best use of the emerging smart infrastructure. Success is measured in terms of "satisfied citizens" that are to be actively involved in all development, as well as local entrepreneurs, scientific institutions and the City of Eindhoven itself.

Carbon footprint is an important element of "quality of life" in cities. Use of bikes in cities is becoming a high issue on the political agenda, both in terms of provision of safe pathways for people on bikes as in terms of making bikes available. Bike sharing systems are now available in many European cities, and arrangements range from subscription cards that allow you to loan a bike from a bike station to full "pay per use" solutions, with GPS tracked and alarm secured hardware. The picture above is from the City of Antwerp, using the same bikes that are also supplied by Clear Channel in Barcelona, Caen, Dijon, Milano, Stockholm, Zaragoza and Oslo.

3.6 And much more

Above, just a couple of initiatives enables by IoT have been mentioned, that truly all in themselves contribute to a landslide in the quality of services that we can now afford, and for which the quality improves by the day because of the growing number of nodes connecting to the Internet and

sharing information. With the rapid adoption of smart phones, hundreds of millions and soon billions of people will have access to services reflecting information that is based on networks of IoT devices: those we carry, those in our homes, on the streets, and wherever they are installed to make a difference. And with the rapid development of “connected wearables” including smart health bands etc. data are truly connected on a very granular, personal level. With cars, smart phone apps and wearables increasingly keeping track of geo-location it becomes increasing difficult to keep your whereabouts private.

All these sensors generate data that potentially are used for a realm of applications. By not being deterministic about this (“only for this purpose, and otherwise not”) innovation in services becomes possible beyond our imagination. Like every development that enables new applications, we need to accept that there will also be attempts for non-authorised and even criminal use. At the same time that should not stop us from benefiting from the wealth of possibilities that is generated today.

4 IoT policy context towards 2025

Within the wider policy context in which IoT developments are embedded, there is a clear need to address those issues that can lead to unsustainable outcomes when not taken into account in further development of IoT. As argued above, it is clear that IoT is needed, and its progress, inside and outside of Europe, unavoidable. Many solutions find their way to the market already, and there is a global call for continued investments in technologies that help us deal with the increasingly intensive use of the world's global resources, including energy, materials, clean air, sweet water and space. At the same time there is a need for IoT to be trusted, which includes tackling issues related to data protection, and security. In short: we need to move forward, yet in a "ethical" way (i.e. taking into account ethical considerations that are the result of legislation, culture, habits and individual choice) thus to ensure both economic and social sustainability.

So: what can we do to ensure that the investments made in IoT are paying off, in economic sense (to those that invest), and address the societal needs that need to be addressed, and all this in a long term perspective? In this chapter we frame the policy context to provide a background for concrete policy actions.

4.1 The call to action

The Internet of Things poses profound policy challenges. Many come from the ways in which it is likely to affect and even disrupt areas either of settled policy or those that are already struggling to cope with other related technology clusters such as cloud computing and data analytics.

In addition, there are policy challenges arising from the Internet of Things itself. Some of are familiar from the experience of other emergent technologies, especially those with the potential to transform public services and industrial structures as well as Europe's commercial fortunes. These include the need for suitable forms of finance, access to skills and fair and efficient market access. They also include human capital requirements, in particular for business, entrepreneurial, technological and societal knowledge available to new and existing enterprises moving into this area or building new businesses with the aid of Internet of Things capabilities. Beyond this, the enterprises behind such potentially disruptive technology-led developments need organisational capital in the form of value network linkages, partnership opportunities and an appropriate mixture of competitive and cooperative contacts among businesses at different points in the value chain, officials and civil society actors. Underpinning these is the need for a stable, transparent and proportionate legal and regulatory framework capable of providing the right mix of certainty and flexibility.

These are not simply European problems; the global nature of the Internet itself has already taught us that such issues need to be understood globally, even when they can be tackled at European or Member State level. This is partially a matter of bounding the market and binding the players; European regulations and laws apply directly to European economic actors (including in some cases foreign entities directly active in European markets) but may be less effective in influencing the behaviour of outside players. This may complicate policy aimed at protecting European citizens (e.g.

the need for the Safe Harbour Agreement in relation to personal data protection and the difficulties it is currently experiencing).

The globalisation question may have commercial ramifications, providing non- or minimally-compliant global actors with powerful cost advantages in global markets and thus weakening European firms' competitiveness. For the Internet as a whole, this tends to be limited to overseas markets because many of the most important issues subject to government limits are controlled by regulated entities; for the Internet of Things, it may not be so easy to identify the source of particular problems or to control e.g. global producers of Internet of Things-enabled devices while retaining open protocols for interoperability and composition. This not only affects current competitiveness; it also affects the direction and pace of technological development, which may be stronger elsewhere, or go in directions that do not meet the needs of applications of specific European public and general interest such as eHealth) or which magnify the impact of areas in which Europe has tended to underperform such as service model and business model innovation.

On 4 February 2015, the Alliance for Internet of Things Innovation (AIOTI) was initiated by the European Commission in order to develop and support the dialogue and interaction among the Internet of Things (IoT) various players in Europe. The overall goal of the establishment of the AIOTI is the creation of a dynamic European IoT ecosystem to unleash the potentials of the IoT, and the focus is on assisting the European Commission in designing of IoT Large Scale Pilots that will be funded by the Horizon 2020 Research and Innovation program.[35] One of the working groups (AIOTI WG4) is specifically focusing on policy aspects, and has produced a report on barriers that might restrict take-up of IoT in the context of the Digital Single Market, including in relation to privacy, security and liability.[36]

In this section, we recap some of the sources of regulatory and policy challenges analysed above. Then we identify some important areas of current uncertainty that should be clarified in order to develop suitably supportive – and not unnecessarily non-distorting – policy actions in relation to the Internet of Things. And where relevant, we will make reference to the view of the AIOTI WG04 report on policy.

4.2 What needs to be achieved?

Rather than taking policy action to determine "what will be done", it is important to create the circumstances that support IoT innovation and deployment to happen in a healthy way. For this, the following starting points are important:

4.2.1 Create an IoT environment that encourages investments

Crucial for innovation and progress is ensuring that capital finds its way to IoT innovations and IoT inspired innovations. For this, it is important that an environment develops that takes away unnecessary uncertainties related to legality of specific technical solutions, stimulates interoperability (Standardization, inter-domain connections, flexibility, innovation, openness), and ensures a fair competition landscape (transparency and accountability).

[35] See https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti
[36] AIOTI WG04 Report on Policy issues, dd. 26 october 2015

Active stimulation of knowledge sharing (awareness of opportunities and risks, and sharing pre-competitive insights re: how IoT can serve the market, best), and access to investment capital (European research funds, seed funds from risk capital networks, etc.) will for sure make a difference here. The use of open standards that allow interoperability of IoT elements and environments will not only help interoperability but also increase transparency.

Making sure data collection, storage, and sharing mechanisms are set up in such a way that robust protection against privacy infringements is enabled will help make sure that systems will be acceptable, even if legislation on these issues is (continues to be) subject to change.

Ensuring availability of bandwidth for communications between connected objects is another crucial factor. When taking into account the predicted growth towards as much as 50 billion communicating devices in 2020 (as CISCO, Ericson and other predicted), it will be crucial to be smart with the way these devices connect. Partly, this will be by design of architectures and use of different ways of communications, ranging from fixed wire (fiber) to NFC, Zigbee, WiFi, WiMAX, and 3G, 4G or 5G and other standards for wireless communications.

Last, but not least: it would be good if people know what is necessary, and what is available, as knowledgeable consumers in a free market situation will drive towards a better understanding of what consumers (people!) want, and faster effective deployment of IoT as people will invest in it where needed

4.2.2 Ensure emergence of a trusted IoT environment

Uptake of IoT in the mass market will stand or fall with people being willing to use it. Basically, this will be subject to a trade-off made by people based on their understanding and trust in IoT products and services ("*Do I trust it to do what it says?*"), their ability to hedge the risks ("*If things go wrong, how do I get compensated*?"), and the ability of the industry to meet expectations in terms of security, safety, and availability. User experience is key. Do IoT objects or services work according to what is promised, are they safe to be used, and do they share data that can be related to me or the people around me, or not?

Legislation related to consumer protection, ranging from product safety, to product reliability, product information reliability and personal data protection, should reflect an understanding of the sensitivity of data in a big data and big data analytics context. From an environmental protection perspective, it should take into account that IoT tags will be everywhere, and in the case of active tags with independent power sources, real choices should be made to avoid potentially severe damage to our environment. From an economic perspective, systems should be set up in such a way that maintenance is doable, whether in the home by the (amateur) home owner, in professional workspace (by trained personnel) or in the field/air/sea (wide space to be covered). Systems that cannot be kept up will deteriorate and lead to loss of trust.

Key in this is transparency, security, and accountability. Well explained terms and conditions, easy to use installations, appropriate security fitting to the sensitivity of the specific IoT application – and to the data generated (Encryption, key registration, verification, authentication, QoE, QoS) are crucial in this.

In addition, code should be open (to public scrutiny), and/or to independent expert scrutiny. Today, the vast majority of smart home gadgets, connected cars, wearable devices, and other Internet of Things inhabitants are profoundly closed. Independent researchers can't inspect the code that makes them run. You can't wipe the factory-loaded software and load alternative software instead. In many cases you can't even connect them to other devices unless the manufacturers of each product have worked out a deal with each other.

While some issues, as the above, can and already should be tackled today, it is clear that new trust issues may come up that may require new measures, as this area is rapidly evolving. Therefore, there is a call of active monitoring and continuous evaluation, as well as knowledge sharing.

4.2.3 Use IoT to addresses societal challenges

While much can be left to markets, we also concluded that there is an urgent need for developing IoT in response to specific societal challenges, such as healthcare; assisting independent living; a secure and safe society; environmental sustainability and dealing with increasing complexities in networks and infrastructures. For these challenges, it is important concerted actions are stimulated to take place, drawing upon all stakeholders involved, as no stakeholder will be able to address these challenges alone. Addressing societal challenges using IoT is multidisciplinary from the outset – as a deep understanding of the specific societal challenge themselves is central to any IoT solution.

Next to specific societal challenges, cities that are actively pursuing innovation through implementation of connected objects to better serve their citizens provide excellent development opportunities, as public authorities that take responsibility for protecting the public interest work directly with industry to provide those facilities. In many projects currently rolling out, science is actively involved, as well as the citizens concerned that participate to public panels etc. Several business cases already show that the innovation itself can pay for the investment in connected objects and – services. Partly because certain tasks can be provided more effectively, measure made (for instance: streetlights that shine brighter when necessary, and dim when possible thus using less energy) to generation of new business opportunities such as services related to the data collected and shared via public infrastructures.[37]

4.2.4 Address specific regulatory and policy challenges

Many of the regulatory and policy challenges are familiar both from other Internet-related contexts and from prior assessments of the specific needs of the Internet of Things. These include such familiar issues as privacy, security and innovation. These have a special character in relation to the Internet of Things; though of course the response – particularly where it involves legal or regulatory change – must take into account other affected areas and the principles of technological and economic neutrality. Many of these special characteristics have already been considered above, but we draw attention to a few specially-relevant aspects.

[37] See for instance: Smart city Eindhoven launches citybeacons (http://eindhoven365.nl/smart-city-eindhoven-lanceert-citybeacons/?lang=en) or Eindhoven as living lab for intelligent lighting (http://www.eindhoven.nl/inwonersplein/leefomgeving/slim-licht/Eindhoven-as-living-lab-for-intelligent-lighting-1.htm)

With regard to privacy, this includes the way privacy concerns are heightened by the invisibility and substitutability of many of the sensors involved in collecting potentially personally identifiable information, the difficulty of finding the entities involved and fitting them into existing data processor and/or data controller roles and the fact that many potentially concerning profiles could arise from the concatenation of large amounts of individually-insignificant observations.

In terms of security, the possibility that individual sensors or actuators may be compromised goes well below the granularity of most conventional organisational, physical and informational security policies.

Finally, the potential for Internet of Things devices to be repurposed or to be composed in ways that offer new functionalities vastly increases the scope for innovation (including bottom-up innovation by those able to hack such devices or their interfaces) but at the same time weakens the connections between the parties whose interests are affected and goes beyond conventional IPR protection frameworks.

In addition to these – rather negative – challenges, there are more positive and exciting possibilities evident in relation to Europe's Grand Challenges – these are areas where there is a need for considerable advance, but also areas where the scope of the issue allows it potentially to serve as a platform for novel forms of challenge led collective endeavour to tackle intractable and urgent problems in such areas as the environment, health, and the ageing society.

Specific technical aspects of the Internet of Things that potentially justify policy intervention arise from its novel ICT aspects, including the importance of new organisational forms running form designed autonomous systems to self-organising swarm robotics. They also come from the potential of the Internet of Things to create data floods with their own dynamics and potential for advances in terms of ownership, governance, curation, access, processing and exploitation. Moreover, the Internet of Things is closely clinked to other ICT-related hot topics like Big Data and Cloud computing.

4.3 What is to be taken into account?

4.3.1 Overarching issues

When taking policy action with regards to IoT, it is crucial that all involved in the policy process understand the wider context. This means there needs to be a solid understanding of the following:

Governance: in terms of "how do we get things organised?." Dealing with governance issues relating to IoT, which is per definition a global technology, in a world that is very diverse in its state of use of Internet and technology, and in its appreciation of "values" means that there is not one "fit for all": by definition, IoT will need to be set up in a way that allows adoption in different cultures, within different legislations and the accompanying cultural values. In this world change is the only constant.

Big Data and IoT: data continue to boom – and "connected things" heavily contribute to that. Currently, there is little transparency on which data are collected and shared. Potentially, all data can be related to individuals, which means that privacy considerations need to be addressed from the outset. What principles to apply on collection, storage, access, and usage of data? Whereas

intended use of data at the point of collection is can be assessed, its potential use in combination with other data not identified yet at the point of collection, cannot be predicted nor assessed.

Security in IoT applications: How do we make sure data will not end up in the wrong hands (access)? And how do we deal with applications with different degrees of "sensitivity" to system failure, and/or system tampering? Do we need a taxonomy for IoT, and how would that look like? In this we need to consider security in context: is it about access to data, resilience, reliability, safety?

Ethical, by design: how can we build in ethical use, from the outset? Is "privacy by design" sufficient, or is more needed? And how would we know what ethical standards to apply for European products in a global market? Like under "governance", it is clear that ethical values are under constant change, influenced by law and culture. Yet whereas "law" is codified, ethics are more of an attitude than a "letter".

Last, but not least: **spectrum**. What if all these 50 billion objects in 2020 want to communicate, constantly? Would that work? What will be the effect of 5G, and the introduction of LoRa networks? It will take some time before connectivity becomes an issue, and at that point it will be much more difficult to introduce and apply new standards. We may be able to prevent ending up in a gridlock if we take spectrum considerations into account from the outset.

4.3.2 The problem of fragmentation

Fragmentation operates at many levels, briefly discussed below. We do not argue that all fragmentation is bad; far from it, variation to reflect specific needs or to explore potential innovations is essential if the Internet of Things is to survive, just as a dynamic balance between competition and collaboration is required. But our ability to separate appropriate variation from damaging fragmentation may be improved if we describe some of its more significant dimensions.

Perhaps the most obvious type, arising from the open nature of the Internet of Things, is fragmentation at the device level. Appropriate variation is addressed by interoperability frameworks, data-sharing rules and protocols and the evaluation is supported by considerations of extensive vs. intensive competition, lock-in and similar elements of the economics of innovation[38].

Closely related to this is service and application fragmentation, or the tension between the tendency of large platform operators to create walled gardens of carefully integrated services vs the more self-organised composition of independent and autonomous services to create flexible capabilities that can keep pace with end users' changing requirements and discoveries.

A second area of potential fragmentation, where the Internet of Things makes contact with other communication and interaction technology clusters, concerns access to and rights to use the electromagnetic spectrum. Spectrum demands vary in in space, power and time, and both the availability of suitable spectrum resources for Internet of Things development and the opportunity cost in terms of competing uses must be considered in relation to current spectrum licensing regimes and to proposed and existing provision for 'unlicensed' spectrum use for experimentation and for delivery of e.g. low-power services.

[38] Cave, Jonathan, Prisoners of Our Own Device – An Evolutionary Perspective on Lock-In, Technology Clusters and Telecom Regulation (August 15, 2009). TPRC 2009. Available at SSRN: http://ssrn.com/abstract=1995551.

A third issue concerns the relation between the Internet of Things and the Internet *sensu strictu*. There are a range of policies and market developments constraining the development of the Internet, but the Internet of Things is not limited to this infrastructure; it can also make use of non-Internet (mobile, ad hoc, weightless radio, etc.) networks. This potential for bypass will alter the degree to which incumbent powerful Internet entities can harness or restrict the power of the Internet of Things.

More obviously, in both this and other contexts, is the scope of regulatory and policy fragmentation and for measures to alleviate it running from shared policy formulation through information sharing and coordinated action (shared responsibility).

On the self-regulating end of the scale, earlier work on the subject as well as this report has warned of the dangers of fragmentation of protocols for e.g. information exchange, interoperability, response to actuator signals, federation or concatenation of individual units, spectrum sharing, payment handling and even for the operation of 'smart agents' for negotiating privacy issues. The problem of fragmentation is not simply a matter of competing and non-interoperable rival protocols but also the risk that protocols are defined at too granular or microscopic levels to permit them to internalise operational and functional complementarities and the possibility of shared services and capabilities.

Finally, we draw attention to the very specific risks created by fragmentation of security approaches – especially attack signature identification and sharing, coordinated response arrangements and the ability of the Internet of Things ecosystem to identify and react to complex emergent risks and problems.

4.3.3 Mapping the issues

In order to refine and build consensus around the recommendations described below, and to identify the interested parties, it is useful to classify potential areas for intervention according to how they present themselves and play out in the policy arena.

To begin, we may usefully divide regulatory issues into three broad categories[39]:

- Existing regulatory issues that the Internet of Things makes harder e.g. protection against automated processing and decision making;
- Existing regulatory issues that the Internet of Things makes easier or obsolete e.g. type approval not needed for assemblages of items, where it can be handled by protocols or negotiated changes, traffic regulation etc.; and
- New regulatory issues – e.g. assigning liability for the delegated actions of autonomous systems or for the collective action of systems that interact in ways beyond the control or monitoring capability of their fragmented 'owners' and 'controllers'.

A further classification element that is not limited to regulation is the degree to which issues are or should, stretch across boundaries and thus the possibility that the assessment of the need for action – let alone the action itself may involve realignment or linkage of issues across regulatory or

[39] This schema was pioneered in Cave, J., Robinson, N., Schindler, H. and S. Kobzar (2015-forthcoming) "Understanding Regulatory and Consumer Interest in the Cloud" Boston: MIT Press.

ministerial boundaries. An example is the potential need to unify or coordinate DG CNECT and DG ENER approaches to Internet of Things-enabled Smart Grids. This might ultimately result in transfer of responsibility from an organisation historically responsible for an area to another better-placed to address the problem once it has migrated to the Internet of Things or to control a 'technical' solution in which Internet of Things-enabled capabilities replace traditional ICT or even non-ICT approaches.

In addressing this aspect of an issue or group of related problems, it is useful to scope the potential and need for cross-organisational cooperation in policy development by means of some or all of the following activities:

- Sharing information;
- Joint problem analysis;
- Coordinating policy opportunities (e.g. recrafting Directives or implementing in Work Programmes);
- Identifying common and coordinated objectives (especially at specific and implementation levels);
- Formulating crosscutting and coordinated policy options (including extension and withdrawal of existing initiatives and measures);
- Integrated impact assessment and stakeholder engagement to handle
    - Internet of Things-specific and ICT-specific entities;
    - providers of services and platforms for the Internet of Things;
    - commercial and other entities offering Internet of Things-enhanced services to other parts of the value chain; and
    - providers of complementary services such as data controllers and processors, cloud and repository providers, transaction support, privacy, security and assurance-as-a-service, analytics services, etc.
- Assessing spill over implications for other policy domains such as energy, transport, health, and competition;
- Coordinated monitoring and evaluation strategies – including enforcement of obligations and legal measures to allocate costs and benefits.
- Analysis of the understanding of and institutional appetite for questioning foundational assumptions regarding consent, autonomous systems and policy stance towards cybernetic (complex, mixed human/machine) systems[40].

4.4 What is the opportunity?

Europe has a long tradition in telecommunications, and in services. In the race for global leadership on IoT it is not the front runner anymore on many aspects, yet still has its strengths to build on. The support programmes managed by the European Commission can help European industry to find its way forward towards new innovation and growth with global impact when it manages to address the key needs of the world. The work done by the IoT European Reseach Community (IERC), now integrated in the AIOTI initiative, helps European stakeholders to find each other and work together

[40] this includes exploring new forms of service contract, consent certification, privacy and security attestation and frameworks for their federation across jurisdiction, sectoral, product type and use type boundaries.

under conditions overseen by the European Commission, i.e. requiring attention for European legislation and values.

Europe needs to position its investments in technology and innovation that are addressing Europe's societal needs, such as addressing the challenges of increasing average age of its citizens, increasing tensions in geopolitical sense that affect the safety of citizens, increasing scarcity of goods and materials, and intensity of use of our natural habitat. And European developments need to take into account Europe's values, such as privacy and data protection, safety, respect for the environment, etc.

Within a global context with a wide variety of priorities and values, and with the full understanding that IoT development and deployment is a global issue, Europe can truly step up and play its important role as a leading market with very specific priorities and values, such as these related to privacy and data protection, consumer protection, and product safety.

An important step in this is the ECs focus on better IoT governance in the global debate, insisting on increased transparency and accountability in multistakeholder context. Two kinds of issues exist: technical matters, to make sure all the infrastructure and devices that constitute IoT can talk to each other; and overarching matters, to address cybercrime, Net neutrality, privacy and data protection, and freedom of expression.

The EC can also play a leading role in development of a "security ontology" for IoT "things" and services, and development of a "privacy sensitivity ontology" thus reflecting a good understanding of risks and trust. And furthermore, the Commission can play an important role in stimulation of a (global?) broad awareness raising and societal debate about ethical aspects regarding the trade-offs that come with IoT, and proportionality of measures to be taken.

5 Suggestions for policy action

Building on the policy frame presented, there are ample opportunities for action supported by the European Commission through the instruments that are available to her. Actions range from demonstration and monitoring, from legal action to empowerment of consumers and citizens by awareness raising, and support of innovation and deployment by improving access to knowledge and investment funds for entrepreneurs. The initiative to set up the Alliance for IoT Innovation is an important step in creation of an IoT ecosystem. In the following paragraphs we will make concrete action proposals related to those domains, starting with the concrete support with experimenting and development in real user environments, followed by awareness raising and education, through legal reviews and clarity to the "soft law backend": promoting an ethical approach, across borders and stakeholder groups.

5.1 Large Scale Framework Pilot for IoT

For 2016 – 2017, the European Commission considers to call for European IoT Large Scale Projects. Large Scale Pilots should provide the opportunity to demonstrate actual IoT solutions in real-life settings and make it possible for providers to test business models and integration modalities through direct experimentation with users. This could also help clarify the need for complementary actions around notably standardisation, interoperability and other policies like trust and security, and provide an environment where to test data analytics tools at scale. In order to set scope and ambition, the European Commission organized a consultation on this at the end of 2014.

Traditionally, many elements of the pilots are already defined in the tender phase. Specifically for a fast moving area as IoT it is important that specific projects contributing to the Pilot are not defined beforehand, but that the "best of breed" demonstrators are selected that are available at that time.

This is also the approach supported by the AIOTI initiative. In its report, WG04 (policy) suggests that Large Scale Pilots should develop IoT applications with privacy compliance in mind, considering if and when a Privacy Impact Assessment is necessary in the context of the IoT, and develop a standardised approach to performing such assessments, in accordance with Privacy by Design best practice. It is also recognised to be vital that Security issues are addressed as part of the design and development phase. As the Large Scale Pilots address a variety of industry sectors, each should tailor security requirements according to their sector, to fulfil the adequate prerequisites, and balance the security risks to cost, throughout their life cycle.

WG03 (standards) suggests a high level architecture in her report, at functional level consisting of a network layer, an IoT layer, and an application layer. Following the High Level Architecture will help partners to work together in Large Scale projects.

Action proposal: *The "Large Scale Framework projects", in which a series of "best of breed" demonstrators from different application areas could be hosted, should include some horizontal activities in support of an ethical way forward, taking into account practical aspects such as privacy and data protection, security, ethics, spectrum and standardisation protocols. Demonstrators should be set up in such a way that citizens are welcomed to see, participate and react, and such experiences across demonstrators should be assessed as one of the horizontal tasks. See also the AIOTI recommendations.*

The bigger such a Large Scale Framework would be, ideally representing a full value chain, linking activities between various regions, various countries, and various industries/sectors, the better, as in the end IoT environments become mostly part of one interlinked network, thus allowing cross-sectoral and cross-jurisdiction evaluations. The feedback from such a pilot would be useful to guide further IoT developments, and would possibly generate input to legislator reviews and considerations to ensure the legal framework serves a society that is underpinned by networks of interconnected objects.

5.2 Awareness raising and societal debate on IoT issues

IoT is pervasive, and will become even more pervasive over time. Yet in order to guide future innovations and applications, it will be important to better understand what people want. A better understanding will ensure more targeted investments and inform policy makers when to take action, if issues come up that cannot be left to markets alone[41]. As AIOTI WG04 recognises that certain IoT applications may prompt a wider societal debate, starting with but also up and beyond to privacy, on ethical issues, it is important to ensure that debate takes place before IoT has developed in ways that make citizens loose trust in the digital connected environment. Rather than just a technology and market push, it will be useful to also create a solutions pull from citizens and consumers. The EDPS calls in his Opinion (2015) for a deeper discussion: "*Data protection principles have proven capable of safeguarding individuals and their privacy from the risks of irresponsible data processing. But today's trends may require a completely fresh approach. So we are opening a new debate to what extent the application of the principles such as fairness and legitimacy is sufficient*." He calls for all stakeholders ("Policy makers, technology developers, business developers and all of us") to consider "*if and how we want to influence the development of technology and its application*".[42]

It will be important that people better understand the changes in our environment. What does it mean to have a smart meter in your home? Who will have access to the data that your smart wearables are reporting on your smart phone app with regards to your health? What possibilities and rights do you have with regards to data generated in IoT environments that relate to you? What does it mean if a US IoT provider commits to a privacy policy "for personal data"? Why is the "Safe Harbour" ruling by the European Court of Justice so important? Many questions get asked, and many answers are given – so the debate has begun, and it is important to make sure politicians, citizens and consumers are well informed in this.

With all this it is also important to better understand the trade-offs. Whereas almost anybody would say "no" when asked to give up their privacy, the answer mostly completely changes if something is offered in return, such as convenience, safety, or wealth. Where the trade-offs lay for people in society can be determined by people "who think they know" or by people "who know how it should be": in reality, the proof of the pudding is in the eating. Therefore a combination with informing people about, and involving people in IoT environments will be an important element to enable a productive and grounded societal debate.

[41] http://www.pewinternet.org/2014/05/14/internet-of-things/ The Internet of Things will thrive by 2025, Pew Research Center, May 2014, retrieved 2015.01.06
[42] Opinion 4/2015 EDPS

In this, it should also be understood that this is not a debate for which the end date can be set, already. Trade-off choices are made within a societal context, and are subject to change depending on events, time, culture and location.

It is in the interest of both public and private sector players to involve citizens/consumers in this debate, in which outcomes will be found within legal frameworks and following consumer choices based on commercial offerings and public IoT environments responding to societal needs.

The European Commission could play a useful role in stimulating and facilitating such a debate within the European Union, and calling for a wider debate around the world. Business and civil society will play their part in informing citizens and consumers, as it is also in their interest to understand what people want. For sure, it could contribute to some of the platforms that already entertain a multistakeholder dialogue today, such as EuroDIG and the Internet Governance Forum. For the global debate, it is important that Europe participates in full recognition of IoT being a global technology, with data potentially streaming across many borders. What is developed in Europe, will be used around the world. And what is developed in other parts of the world will be used, here. Whether it is in eHealth, or just a "connected" (smart) TV, smart car, health band, smart meter, or industrial tags, sensors and/or actuators.

From an innovation and deployment perspective, it will be important to design products and services in such a way that they can continue to serve (local?) society even if values and choices are different in different markets, and/or change over time.

***Action proposal**: to actively stimulate and support reach out to the general public with information about IoT, and invite feedback, through IoT themed events for citizens and consumers, social media campaigns, etc., thus stimulating emergence of a flywheel of awareness, mutual learning and feedback.*

***Action proposal**: to require involvement/interaction with and active feedback from well informed citizens when there is European (co-) funding demonstrators and/or deployment projects.*

***Action proposal:** to make IoT and underlying data streams and the European values regarding those a key point in global diplomacy, whether in terms of trade, sustainability, privacy and data protection, internet governance, or on relevant sectoral platforms.*

5.3 Awareness raising on business opportunities in IoT to entrepreneurs and startups

In order to foster and further stimulate innovation and entrepreneurship, there is a need for knowledge transfer and inspiration, complemented with incentives. In answer to that, the European Commission addresses specifically startups and SMEs with specific instruments. The current phase of development, innovation opportunities and market potential of IoT products and services are very well suited for this as initial ideas do not necessarily immediately need big investments.

It is widely recognized that small and medium-sized enterprises (SMEs) and entrepreneurs are crucial for tracing new paths to more sustainable and inclusive growth, thanks to their role in developing and diffusing innovation and providing employment. Availability of and access to knowledge about IoT is an important element that leads to development of new ideas on IoT products and services by these companies.

It is recognized that access to finance represents one of the most significant challenges for these firms, a problem that became even more apparent with the recent financial and economic crisis, according to a recent OECD publication[43]. The European Commission has extended explicit support to SMEs in general for many years, and these instruments are currently further strengthened. A specific focus is now emerging towards startups. In fact, startups often start as S(M)E, yet it is noted that there is a clear difference between those that start small and aim to grow, and those that choose to stay small (or medium) in terms of business size.

For this, ecosystems are currently emerging to support innovation by ensuring access to knowledge on technology and business, and access to finance and generally available tools and support platforms, and testbeds.

Particularly aimed at supporting the emergence and interconnection of such ecosystems is the Startup Europe Initiative[44] of the European Commission. It aims at improving framework conditions for tech startups in Europe, and in particular the business environment for web and ICT entrepreneurs so that their ideas and business can start and grow in the EU. Networks with business accelerators are contracted and build, knowledge transfer is facilitated and attention is given to specific opportunities, role models are put in the spotlights.

Other funding opportunities include the Horizon 2020's[45] SME instrument actively supports SMEs by providing both direct financial support, and indirect support to increase their innovation capacity by providing grants to help develop ideas, build and develop prototypes, get their products validated, demonstrated, and help with commercialization (500 million EUR in 2014/2015). The Horizon 2020 FET Open call is to support a large set of early stage, high risk visionary science and technology collaborative research projects (150 million in 2014/2015). 'Innovation in SMEs' aims at creating a bridge between the core of the framework programme - support to research, development and innovation projects - and the creation of a favourable ecosystem for SME innovation and growth[46]. COSME[47] is the EU programme for the Competitiveness of Enterprises and SMEs, running from 2014 to 2020, with a budget of €2.3billion. It supports SMEs by facilitating access to finance; supporting internationalisation and access to markets; creating an environment favourable to competitiveness; and encouraging an entrepreneurial culture. Eurostars is a programme that supports research performing SMEs that develop innovative products, processes and services, to gain competitive advantages (1.14 billion EUR up to 2020).

In summary: there is a wealth of instruments available to help startups in their endeavors to innovate and conquer new markets. Yet it is clear that not many potential entrepreneurs find their way to these instruments, either because they are not aware, or because of requirements that are unnecessarily limiting the approach of the entrepreneur, and (still today) sometimes cause too much administrative overhead, which is not the core business nor favorite activity for most entrepreneurs. Recent experience shows that creation and partnering with networks of accelerators

[43] Financing SMEs and Entrepreneurs 2014: An OECD Scoreboard, see http://www.oecd.org/cfe/smes/financing-smes-scoreboard-2014.htm
[44] http://ec.europa.eu/digital-agenda/startupeurope
[45] http://ec.europa.eu/programmes/horizon2020/en/
[46] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/innovation-smes
[47] http://ec.europa.eu/small-business/links/cosme_en.htm

and incubators can help ensure the money is spend in the most effective ways. Good examples include the Future Internet PPP (FI PPP), and Startup Europe projects such as the Startup Scaleup project, the Welcome project, etc.

Next to the European initiatives, there are already more than 150 accelerators active in Europe that attract startups by offering bootcamps and based on selection processes to pick out the most promising ideas and teams to help them find access to money and knowledge. These accelerators, such as Startupbootcamp, are taking their initiative with a focus on commercial outcomes, whereas the European Union supported programmes also take societal contributions into account, yet in many ways both commercial and EU sponsored accelerator activities seem to strengthen and inform each other.

***Action proposal**: Continue to bring information about IoT developments and innovation opportunities into accelerator/ and innovator networks that foster entrepreneurship in SMEs. IoT can bring to those networks much inspiration, with abundant opportunities for innovation and startup business. At the same time, it is foreseeable that informing those networks of the IoT related opportunities will be like seeding in very fertile ground – a further boost of IoT related innovation can be expected when the right IoT innovation opportunity insights are shared with the right accelerator- and incubator networks.*

***Action proposal**: for EU supported incubator and accelerator programmes to require contributions to relieving Europe's societal challenges (such as independent living, sustainability, etc.) by development of specific IoT based solutions – knowing that for the purely commercial initiatives, there is an increasing interest from commercial players to invest (thus European intervention for these type of developments are less needed).*

5.4 Ensure legal clarity and adapt legal framework to serve in a new reality

IoT is a fast (and vast) moving area, and can in many respects be seen as a "horizontal element" in a specific application … i.e. part of something bigger. This means that the legislation related to this "something bigger" also extends its power to the IoT "contribution to the whole". For now, the good news is that no IoT legislation as such is needed, as law in general is not technology specific. However, for being able to apply the law, work may need to be done.

As with any complex technological evolution, lawyers cannot apply laws, negotiate contracts or assess risk or the consequences for privacy without a proper understanding of the complex ecosystem we're applying these concepts to. Legal consequences cannot be assessed in isolation and without considering how the devices, technology and data actually interact. The IoT badge means nothing legally and probably conveys little factual information around "how" something works. Therefore it is crucial lawyers understand what they talk about.[48]

Next to domain specific legislation for a fast evolving number of domains where IoT is used, attention needs to be given to privacy and data protection, and consumer protection.

[48] Cutting through the Internet of Things hyperbole, Mark Webber, 15 October, 2014, on http://privacylawblog.fieldfisher.com/2014/part-1-cutting-through-the-internet-of-things-hyperbole

5.4.1 Privacy and data protection

While adoption of the new Privacy and Data protection legislation in Europe is waiting for the opinion of the Council, the Article 29 Data Protection Working Party[49] about how the law should be applied adopted and opinion on Internet of Things on 16 September 2014. IoT is recognized as a major game changer. In its opinion, WP29 expresses its appreciation of the potential societal value offered by IoT application, yet at the same time focuses in this initial opinion on "*everything that might and could go wrong*".[50]

Staying "on the safe side" of privacy and data protection (following the "precautionary principle") is an understandable stance for experts that gather with the task to ensure the best possible privacy and data protection. Yet the challenge will be to find a way forward that encourages behaviours that protect privacy without stifling innovation and impeding the development of the IoT. Guidance has been provided by the EDPS by September 2015, pointing out the importance that a balance is made with the societal interest in deploying IoT, and calling for "*preservation of human dignity*". Let alone that legislation that is too intrusive will lead to many finding their way around it when no reasonable way forward can be found.

As IoT in combination with big data analytics brings a paradigm shift in ways that data can be related to people, it will take a number of years to come to a better understanding on how to deal with this. Current legislation is based on protection of "data related to persons". A good example to sketch the challenge was given by Patrick Tague[51], below: "

"A good example of [the challenge to protect privacy as we used to do] is location privacy. We have all these location tracking devices now. If I decide to reveal my location to the world I may also reveal the fact I happen to be in the same physical environment as you are so I'm also betraying your location privacy. I can do that without your consent and even without your knowledge. This general problem of data sharing and privacy will be accentuated by IoT and we need a completely different conceptualization of privacy to deal with it. So not only will existing tools not be adequate for the job, but existing models of privacy are going to be inadequate in this world of very aggressive and pervasive data sharing".

The big challenge in this increasingly connected environment is that it will become more and more difficult to determine who is going to "own" specific data, who has control of it. And how individuals can opt out if all these different devices are collecting different data elements, or can have awareness and control on where it goes. It is clear that most current commercial IoT developers are more driven by the rush to the market to take advantage of the opportunities than spending more time on getting security and privacy protections to a higher level, so, if any, that often gets bolted on, later.

[49] This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. Website: http://ec.europa.eu/justice/data-protection/index_en.htm

[50] Opinion 8/2014 on the Recent Developments on the Internet of Things, adopted on 16 September, Article 29 WP, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[51] The security implications of IoT: A roundtable discussion with four experts, John Dix, Network World, Feb 10, 2015

AIOTI WG04 (Policy) suggests to explore the usefulness of Privacy Impact Assessments (PIA)[52], as is foreseen in the GDPR as well. Whereas this is generally seen as a useful way forward, it is recognized that it is most effective to assess the intended impact of a specific IoT object or IoT enabled service. However, it will not be able to catch unintended (or, in the case of "backdoors", undeclared) use. And the impact of combining data with other data at some point in the future is entirely out of scope of a "proportional" PIA – thus PIA's should be extended beyond the IoT devices and services domain to the level of data: which data are collected, how they are stored, protected and shared.[53] As in these cases a PIA will not be sufficient, calls for conduct should help to ensure privacy by default, and by design.

***Action proposal**: to extend the obligation of carrying out Privacy Impact Assessments (PIAs) when developing IoT products, services and architectures. The PIA Framework in use for RFID following the requirements as spelled out in the European Commission's RFID Recommendation may provide good guidance for this. Require PIAs for products, services and architectures developed with EU funding.*

The PIA framework was produced by industry in January 2011, endorsed by Art 29 data protection working party in February 2011, and signed by key stakeholders and Neelie Kroes on 6 April 2011[54]. Today the Privacy Impact Assessment process has expanded to other new privacy-related areas like the certification of smart meters. It is due to be mandatory under new EU Data protection rules. The European Norms on RFID and the RFID Recommendation are based on the existing EC 95/46 data protection directive and the article 29 working party interpretation of it.

***Action proposal**: to fund a network to develop solutions specifically allowing IoT developments to grow in a way that privacy concerns are addressed as well as possible, including development of a "global" code of conduct. As IoT is a global development, ideally this network would include partners from different regions in the world, including but not limited to China and USA.*

Solutions need to work, and be usable (otherwise it will not be used!). The EDPS sees this as "*a good opportunity to involve the data protection community, as they can play a new role using existing tools like prior checks and authorisations - because no other bodies are equipped to scrutinise the new data processing*". Possibly not a lot of new technology but new trust architectures including a new use of current technology such as (but not limited to) PET, PEM, hardware roots of trust for (virtual?) servers, etc. A specific concern is the recent ruling of the European Court of Justice (ECJ) in the case Max Schrems vs. the Irish Data Protection Authority, declaring the "Safe Harbour Agreement" to be invalid as non-USA citizens that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection.[55]

Whereas there was already a situation of relative uncertainty, based on recognition of some of the weaknesses of the current Safe Harbour agreement, and negotiations were under way to improve

[52] AIOTI WG04 Report on Policy issues page 8
[53] See results DC IoT meeting in Dresden, 25 and 26 July 2015
[54] See speech Vice-President Kroes at http://europa.eu/rapid/press-release_SPEECH-11-236_en.htm
[55] Judgment of the Court 6 October 2015 in case C-362/14, Maximillian Schrems vs. Irish Data Protection Commissioner

on this, while at the same time the European Privacy and Data Protection Legislation is about to move from a Directive to Law, at some point next year, the ruling brings a lot of uncertainty on legalities of localization for services related to IoT applications that include analysis of data, and collection of data in other regions than those under EU jurisdiction. NB: it should also be noted that the European Parliament has expressed her concerns about the activities of multiple member states relating to surveillance, as expressed in the resolution against mass surveillance passed on 29 October 2015.[56] Uncertainties with regards to data protection and privacy legislation are affecting the willingness of companies to invest in new products and services that may turn out to be "illegal". With penalties going up to 5% of global revenue this has become a real threshold for offering services.

5.4.2 Consumer protection

General consumer protection law is also applicable to IoT products and services. Up and above national and regional legislations designed to ensure the rights of consumers, the United Nations General Assembly adopted Guidelines for Consumer Protection in 1985, and was expanded to include "sustainable consumption" in 1999[57]. Shortfalls currently exist in the IoT context, as was noted during the 2014 meeting of the Dynamic Coalition on IoT (DC IoT)[58] in Istanbul. At the heart of product liability law in Europe is the "no-fault" liability regime introduced by Directive 85/374/EC (the "Product Liability Directive"). This imposes liability for damages caused by a defective product on the "producer" of that product. Generally, the "producer" is either the manufacturer or the EU-importer. With the move from products to services, "arises the question of whether it is appropriate to extend a "no fault" liability regime to technologies that are more in the nature of a service than a product".[59] In this the "voice of industry" warns against regulation/consumer protection that "stifles beneficial innovation or lead to unwanted competitive disadvantages". How "beneficial" is determined is not further explained, and is to be explored. With regards to "unwanted" competitive disadvantages both it needs to be clear whether stakeholders agree (when is it "unwanted"?) and whether over time "disadvantages" may also provide sustainable advantages, as vision may lead to a way forward beyond the near horizon.

There has been considerable international activity, not least the US FTC Report[60] laying out a range of consumer protection issues for raised by the IoT including consumer-relevant security risks[61] and

[56] See http://www.europarl.europa.eu/news/en/news-room/content/20151022IPR98818/html/Mass-surveillance-EU-citizens'-rights-still-in-danger-says-Parliament

[57] United Nations Guidelines for Consumer Protection, New York and Geneva, 2001, retrieved 2015.01.05, http://unctad.org/en/Docs/poditcclpm21.en.pdf

[58] Narelle Clark during the Meeting report Dynamic coalition on the Internet of Things, 4 September 2014, retrieved 2014.12.20, http://2014.intgovforum.org/event/c2879b04fc6b8839fc49947924b6efb8#.VAgd5mNQTO0

[59] AIOTI WG04: Policy report, page 23.

[60] US FTC (2013) "The Internet of Things: Privacy and Security in a Connected World" available at: http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[61] Unauthorised access to and misuse of personal information; facilitating attacks on other (larger, aggregated) systems; and risks to personal safety.

consumer privacy issues[62]. It recommends a range of measures concentrating on: i) "security by design"; ii) data minimisation[63]; and iii) "increasing transparency and providing consumers with notice and choice for unexpected data uses including mandatory actions to prevent harmful access."

However, the targeting of such recommendations and their actual costs and benefits were not wholly clear, and the report has been extensively criticized, even by its own Commissioners[64]. This activity is not limited to recommendations and to IoT-specific measures; there are clear signs in the growing use of general, technology-neutral laws to regulate the IoT. For example, the FTC has used its general consumer protection powers[65] to act against "unfair or deceptive acts or practices" to prosecute privacy and security violations, such as the recent order against Trendnet[66] for failing to prevent unauthorised access to sensitive consumer information carried in audio and video feeds from home security cameras.

The range of potential consumer protection issues goes well beyond these tentative beginnings. Consumer protection law is generally implemented as a complement to competition law on the assumption that protected consumers force firms to compete and that effective competition for the business of informed consumers is the best way to protect their interests. As such, it is predicated on the notion that individual consumers are best placed to identify their interests, evaluate the offers before them and choose accordingly. However: i) this assumption may not hold up across all IoT-enabled contexts; ii) those bound by or made liable under consumer protection law may not be able to detect, let alone mitigate consumer harms effectively in the IoT; and iii) some risks to consumers that are or will be raised by the IoT that go well beyond those that can be handled by retail market incentives.

On the first point – the ability of consumers to manage their risks – we note that many interactions in which devices act on or on behalf of consumers are too fast, too remote, too complex or too fine-grained for effective scrutiny and meaningful consent. To take one example, the growing use of NFC-enabled payment devices has already led to situations where consumers have been subject to charges of which they were not aware. As we move into a world in which 'our' devices interact with others in ways that require a sequence of micro-transactions and automated micro-payments, this situation can be expected to accelerate. More generally, the Internet itself raises related issues including the complexity and remoteness (in time, attention location or probability) of many significant consumer risks. The granularity of the IoT and the autonomous automated and often-silent operation of its devices and systems raises both the likelihood and potential costs of consumer inattention. Even if they could know these details, the costs of managing this flood of decisions are likely to exceed the expected benefits on a per-transaction basis, and policies (as has been shown with privacy policies) provide only coarse-grained protection. Without informed, rational and mobile consumers, the incentives on firms to minimize harms and improve services are weakened, distorted or even reversed.

[62] Including the potential ability of third parties to gain access to or control of devices, data or networks.
[63] In the hope that this would eliminate the 'attractive target' represented by large data stores and that it would limit the possibilities that data controllers would be used in ways that consumers do not expect.
[64] See e.g. http://techfreedom.org/post/109234568019/josh-wright-blasts-ftcs-internet-of-things-report.
[65] Federal Trade Commission Act, 15 U.S.C. § 45(a).
[66] See http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

On the second point – the ability of IoT players to detect and manage consumer risks – we note that many of the adverse consequences to which documents like the EEU Guidelines and the FTC Report draw attention arise not from individual devices but from their interaction or composition with others or from the system itself. As such, they may be as invisible to device and local service providers as to consumers, and little is to be gained by making them bear contractual or legal liability. This is particularly true in cases where consumers' expectations depend on network performance, or on interactions with devices and services through open interfaces, in the absence of certification or responsibility-sharing arrangements at the right level. Indeed, in cases of physical safety and the provision of emergency services, the purely financial liabilities likely to be imposed on device manufacturers will not provide adequate incentives, and may lead to protective or hedging innovations that weaken overall performance by shifting rather than mitigating risk.

On the third point, we simply note that consumer protection also reflects considerations of citizen safety. In this regard, even if the market eventually moves away from unsafe or dangerous IoT devices and services, the damage will have been done. This may be especially important for actuators such as medical devices that can do significant harm if hacked or misled by inaccurate information. The very different protective standards applied in areas such as health and finance as compared to entertainment or transport mean that rules operating at the device or service level (which often cut across these domains) run the risk of being ineffective or disproportionate or both.

As a final note, we would like to point out that these considerations do not in themselves argue for more extensive or intrusive consumer protection rules, binding on ever more parties. The foregoing discussion makes clear that there is no point in placing responsibility on parties who are unable to bear it or to respond in useful ways. Beyond that, it may be that the Internet of Things – if properly developed – can reduce the need for consumer protection by giving consumers more consistent and effective control over the way their interests are served for instance by allowing them to collect and analyse information on their preferences and options more effectively or by equipping them with tools to automate complex or burdensome decisions without giving up ultimate control. This aligns with recent work in behavioural economics on the importance of attention budgets and the impacts of cognitive limits; which suggests that suitably structured and informed decisions can help consumers to learn or identify and to express their preferences. Moreover, the operation of such 'protective devices' can create a far better evidence base than currently exists for understanding how consumer interests may be threatened or advanced and therefore what shape (if any) new forms of consumer protection should take.

***Action proposal**: review European consumer legislation in the light of a new reality of "connected sensors and actuators" and the further move from "products" to "services" that is enabled by this.*

5.4.3 Competition regulation

As noted in the previous section, competition works together with consumer protection to identify and promote efficient outcomes. But competition does not always have these effects. In the case of telecommunications and then for the Internet, specialised bodies of legislation and specialised institutional forms had to be devised to deal with the specificities of sectors dealing with extended and complex value chains, highly diverse business models, rapid technological progress, pervasive infrastructural effects across the economy and a competitive dynamic that favoured concentration, monopoly and collusion. It was originally thought that these arrangements (specialist regulators)

were merely transitional, and that their powers would eventually revert to competition authorities as markets matured and the intricacies of network and platform competition were understood. However, the opposite has proved to be the case, and the scope of their activities has tended to increase, with more and more new regulatory responsibilities (e.g. from the Internet) and an increasing tendency to act directly as competition authorities[67]. This has specific implications for the Internet of Things, due to its critical importance, strong interactivity and inherent flexibility. New players, such as device providers and those whose formerly-controlled goods and services are increasingly (in effect) outsourced to the IoT must be regulated or protected. Overall, the structure and dynamics of new markets within the IoT value chain itself must be better understood before effective competition policy is implemented. To indicate why, we note that competition does not always promote efficiency and may not be viable (for example in the presence of large fixed costs, critical infrastructure dependencies or strong network externalities. In such cases, utility regulation or consumer protection (often by informational remedies) are likely to be more effective. Knowing whether this is the case, deciding whether particular market structure or conducts are likely to be harmful and devising effective remedies are especially challenging in the IoT.

Beyond competition in the IoT itself, there are potentially profound risks (alluded to in the previous section) that information generated or collected by the IoT may itself facilitate market failure in those sectors that operate 'over' the IoT. We have already seen in e.g. smart transport and smart energy applications how the use of IoT devices allows operators and service providers to collect and correlate vast amounts of data that can be sold on to third parties, used to lock in customers or employed to facilitate collusive arrangements via enhanced monitoring.

Action proposal: *conduct open multistakeholder enquiries into the practice and effects of competition within the IoT and markets exposed to or reliant on its capabilities.*

5.4.4 Other domains relevant for IoT

Currently many rights are not being taken into account due to a lack of standardisation, information, compliance and the disposable nature of many devices. From a consumer protection point of view, control of the IoT environment should be with the users, especially the rights to safety, information and redress and clear rights on use of data on individuals. In order to exercise all rights, consumers will need to be alert and aware, and there need to be ways to identify who to complain to, or eventually: who would be liable for specific use.

It should be noted that IoT has specific elements that mark it as a domain in itself, but its purpose is to serve other domains, such as transport, aviation, farming and food, health, manufacturing, etc. This is well understood by AIOTI WG 4 (policy), as is clear from the picture below. The organisations in the picture have been identified and briefly described in the AIOTI WG3 report[68]. Currently there are many organisations and platform active, both in the "horizontal" IoT domains as in the specific sectors.

[67] See e.g. van Oranje, Constantijn and Cave, Jonathan and van der Mandele, Martijn and Schindler, Helen Rebecca and Hong, S.Y. and Iliev, Daniel I. and Vogelsang, Ingo, Responding to Convergence: Different Approaches for Telecommunication Regulators (September 30, 2008). Available at SSRN: http://ssrn.com/abstract=2142015 or http://dx.doi.org/10.2139/ssrn.2142015.

[68] AIOTI WG03 Standardisation AIOTI WG3 report. on IoT LSP Standard Framework concepts

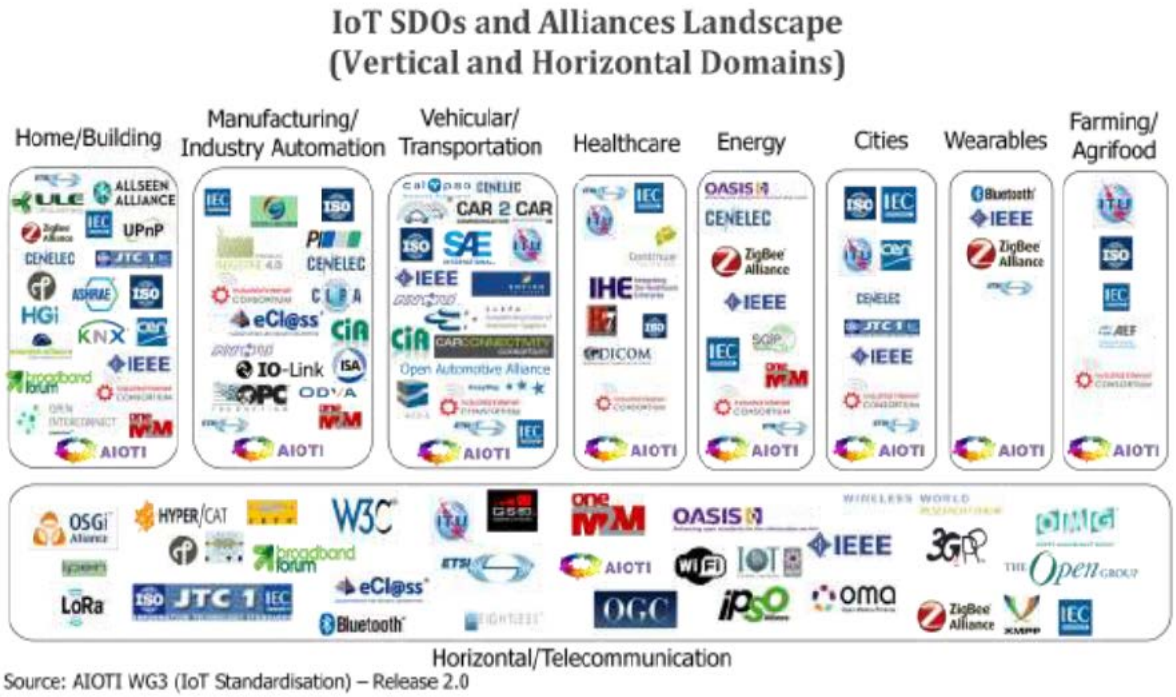

Figure 10: IoT SDO and Alliance initiative projection on vertical and horizontal domains

Other domains that have been mentioned in earlier research include[69]: equipment approval and compliance certification; data retention and lawful interception; human dignity, reputation, and freedom of expression; universal service and e-inclusion; cybercrime; and cyber security.

Action proposal: *stimulate an active dialogue between law and IoT developers to ensure the best possible understanding of what measures are necessary, and still allowing innovation of IoT to flourish and be applied in the interest of consumers and citizens. Note that this will require an ongoing dialogue for a number of years, as IoT is a fast moving area with a currently continuously changing landscape of applications.*

Action proposal: *adopt a soft law framework to address the existing of gaps, duplications and inconsistencies in the framework of regulations affecting or affected by the IoT. (see also: Europe´s policy options for a dynamic and trustworthy development of the Internet of Things[30]).*

5.5 "Going Ethical" with EU supported IoT

From above, it is clear that IoT is still very much in the rapid developing phase, and new applications continue to find their way from innovations to markets. Legal clarity isn't here, in many perspectives, even if it is clear that current law also applies to IoT applications. Current legal debates (e.g. WP29) threaten to take legal action "to stay on the safe side" which in itself is a threat to innovation as investors don't like investing into something that may be declared "illegal" at some point in the

[69] Europe's policy options for a dynamic and trustworthy development of the Internet of Things (SMART 2012/0053),
Schindler HR, Cave J, Robinson N, Horvath V, Hackett P, Gunashekar S, Botterman M, Forge S, Graux H, prepared for the European Commission, DG Communications Networks, Content and Technology (CONNECT', Brussels, 31st May 2013

future. Markets are adopting new IoT products and services as we speak, contributing to an increasing amount of data that is combinable and subject to new algorithms ("big data analytics"), yet consumers do not have an expressed opinion of what they think is "important" or even "acceptable" … as most consumers have no idea about the potentially wider impact of usage of specific IoT products and services on their privacy.

AIOTI WG4 (Policy) focuses on barriers that might restrict take-up of IoT in the context of the Digital Single Market, including in relation to privacy, security and liability, yet also recognizes that certain IoT applications may prompt a wider societal debate. As WG4 notes in this report, the "ethical" implications of certain potential IoT innovations that involve automated decision making (such as autonomous cars) are in the news, and it believes that it is society that will ultimately determine whether such innovations take hold or not.[70] As the EDPS is mentioning in his Opinion (4/2015): "*In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing. The EU's regulatory framework already allows room for flexible, case-by-case, decisions and safeguards when handling personal information. The reform of the regulatory framework will be a good step forward. But there are deeper questions as to the impact of trends in data driven society on dignity, individual freedom and the functioning of democracy*."

Thus whereas privacy is a key element of an ethical approach, security a necessary condition (both in terms of access to data as in terms of access to devices), and liability important in order to ensure accountability, and redress when things go wrong, it is clear that ultimately we will need to respond to wider ethical issues, as society will be confronted with the impact of an increasingly present "connected digital environment." – even if the norms are not clear, today. For instance, IoT technology is increasingly able to replace decision-making functions that were previously only capable of being made through human judgement. The "ethical" implication of this is a common topic among academics and in the popular press. One of the emerging questions is whether there should be a legal or regulatory response to these ethical challenges.[71]

Finding ones way in this uncertainty as a decision maker is not easy: it is clear that there are no clear external references, yet. As such that is the nature of entrepreneurship: acting in uncertainty and taking risk, when justified by expected return. In this there are two challenges:

1. How can business deploying IoT reduce the risk of legal breaches, or of investing in a market that turns away for ethical reasons;
2. How can governments (and civil society) ensure that societal challenges that require relief by deployment of IoT are addressed, in particular when the market would fail without intervention.

With the EDPS the conclusion is: "going ethical", with a keen eye on human dignity. Explicitly embracing the aim to make the best ethical choice in every moment may bring a number of advantages: a) it reduces businesses reduce risks for investments in products and services from a legal perspective, b) it supports businesses in a long term relationship with consumers who want to buy ethical and are willing to use the products and services that support their needs best; c) it helps

[70] AIOTI WG04: Report on Policy issues, page 5.
[71] AIOTI WG04: Report on Policy issues, page 22.

create a society in which people feel good and have a relatively high level of trust, thus keeping "transaction costs" overall at relatively low level.

Even more so: the "future capital" emerging from IoT environments will be largely in the data that are usable, thus also this concept (how to benefit in a legal and ethical way from data generated through our IoT products and services) will lead to even more solid data access with no (or little) drive for people to want to "opt out".

Thus if Europe wants to benefit from the emerging opportunities arising with IoT, "going ethical" can bring us new growth and innovation and helps us creating a world we want our children to live in, respecting European values. We will need to act responsibly and with high ethical standards. Responsibly because we have to realize that by adding sensors everywhere and tracking everything we are opening the door to potential hacks, security intrusions and breach in our users privacy. The law cannot do it all for us, it is our own standards and ethic that will transform the world. Guidelines to keep in mind when building IoT products in an ethical way include[72]:

- **Transparency to users**: understandable and clear terms of use, including an overview what is tracked, and why, and how that information is shared. Multiple legal terms pages don't help. Transparency also includes "usability" as it doesn't help to have options if you do not know how to use those. A clear example here is the Facebook privacy settings, that are not very well understood or used by most Facebook users, today;
- **Ability to turn off individual tracking**: where and when possible, in the highest level of granulation as practically possible. "All or nothing" does not fit here. In addition, it is clear that unless all people and objects around turn off tracking, "collateral tracking" may still happen;
- **Give the ability to delete historic data**: or at least makes sure that historic data are no longer related to individual accounts ("the right to be forgotten" in practice – and data can still be used for business process innovation etc.) Here, the Google case shows how complex this can get, as for instance the availability of online records and news articles as such is not challenged – newspapers continue to have a right to share information with the public. At the same time, retrospective correction of data that turn out not to be correct is a challenge;
- **Security**: when dealing with user´s data, make sure access is well secured. When falling in the wrong hands, this cannot be corrected – just compensated. Currently, data breaches need to be reported in some jurisdictions, and help make sure both private and public organisations pay more attention to avoiding breaches. The big issue is with data that are not apparently connected to persons (but may be when combined with other data), and data that are stored in the cloud of objects where access is not always clear;
- **Ethical behavior** is a cultural thing: it needs to be embraced, lived, in every aspect of the business. Needs to be talked about, to be an explicit value. Ethics is a living thing and can only thrive when welcomed and constantly encouraged.

It should be recognized that tensions exist between the technical measures for individual privacy enhancement and the business opportunities for digital-related commercial activities that correlate

[72] *Considerations for ethical standards in IoT*, blog by apassemard d.d. November 5, 2014, accessed 2015.01.06 at https://entrepreneurshiptalk.wordpress.com/2014/11/05/ethics-in-iot/

different sets of data collected from IoT devices, with the intent to monetize them. This opportunity to monetize data using data analytics is one of the reasons why the market success of Privacy Enhancing Technologies (PET) and the application of Privacy Enhancing Measures (PEM) remains limited[73]. In other words, the reasons for the business failure of PET and PEM in today market or for privacy protection solutions in general may not only be related to technical reasons or lack of knowledge, but also (and maybe more so) from misplaced incentives from an economic point of view[74]. This is also a common issue for the economics of information security[75].

Similarly to other areas of the "ethical market"—such as ethical funds, cruelty free foods and cosmetics, and fair trade items—"ethically oriented" (or ethically friendly), ICT may be seen as a new desirable feature for digital life[76]. The concept of ethical design in IoT products and services is in particular related to the ability of users to control and protect their personal data. This means that users are enabled to establish and freely shape value-based choices in their interactions with IoT. In order to be able to address changing preferences (geographically, and in time) values should not be imposed or pre-identified, but remain open to individuals' choice in ethical options. So in the design phase, those aspects that would be subject to values will be opened to ethical choice.

An important element of Ethical Design consists of its supporting mutual trust amongst all the components of IoT ecosystems: human, devices, applications, and business entities. Trust is boosted by a recognition of personal needs; by transparency in how things are organized—namely in a way that clearly shows that relevant measures have been taken to meet those needs—; and by accountability in ensuring that responsibilities are clear, and if someone responsible (person or organization) fails to live up to what is promised/required, they will be made accountable[77].

Stepwise in the lifecycle of design and development of new IoT products and services, we are looking at the following stages[78]:

1. Understanding the need for and value of trust;
2. Translating these needs and values into an Ethical Design of IoT products and services;
3. Demonstrating that these needs and values are taken into account;
4. Establishment of a clear framework for transparency and accountability.

The first stage is about creating awareness about this need, thus about creating a preparedness to invest in it. Unfortunately, it is likely that breaches of trust will happen that will help raising this awareness and preparedness, over time. So in order to be ready for this, it will be important to already engage in the following stages, starting with involvement of the user in the design phase in a

[73] *Does It Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy*, Cave, J. et al., final report, European Parliament, 2011
[74] *Privacy and security of personal information*, Acquisti, Alessandro in Economics of Information Security. Springer US, 2004
[75] *Guest Editors' Introduction: Economics of Information Security*, Anderson, R.; Schneier, B., Security & Privacy, IEEE , vol.3, no.1, pp.12,13, Jan.-Feb. 2005
[76] *The Ethical Consumer*, Harrison R., Newholm T., Shaw D. (eds), SAGE, London, 2005
[77] *Building Trust in the Human Internet of Things Relationship*, Kounelis, I.; Baldini, G.; Neisse, R.; Steri, G.; Tallacchini, M.; Guimaraes Pereira, A., in Technology and Society Magazine, IEEE , vol.33, no.4, pp.73,80, 2014
[78] *Ethical Design in the Internet of Things*, Gianmarco Baldini, Member, IEEE, Maarten Botterman, Ricardo Neisse, and Mariachiara Tallacchini, draft publication for IEEE, 2015

way that goes beyond usability, alone – it will be about "user experience design" in the widest sense, including aspects such as trust and comfort, and explicitly including awareness of relevant value-laden choices. Third stage in the development is demonstrating this in the eyes of the user, allowing further feedback to ensure both usability, usefulness *and* trust and comfort. And in order to ensure long term relevance of the products and services under development, it will be key to establish a clear framework for transparency and accountability, with respect for current legislation and pre-empting the evolution of the regulatory framework reflecting the changes in values and needs of citizens.

During the IGF 2015 session in Joao Pessoa, Brazil, attention will be given towards a global ethical approach, as suggested by the IGF Dynamic Coaltion on the Internet of Things. It proposes an Internet of Things Good Practice Principle:

> *"Internet of Things Good Practice aims at developing IoT products, ecosystems and services taking ethical considerations into account from the outset, both in the development, deployment and use phases of the life cycle, thus to find an ethical, sustainable way ahead using IoT helping to create a free, secure and enabling rights environment: a world we would like our children to live in."* [79]

This charter is the result of discussions at a number of meetings this year, including Lisbon (IoT week), Sofia (EuroDIG), Dresden (DC IoT), and Washington DC (IGF USA), and builds on the work done by DC IoT since the IGF in Hydrabad (2008).[80] Basically, the paper is building on 5 core ideas that are now subject to scrutiny of the wider global IGF multistakeholder community:

1. In order to develop the Internet of Things in a sustainable way developers and deployers need to commit to an ethical approach, taking into consideration that the IoT is really about people and how it affects people;
2. Good practice in IoT products, ecosystems and services require meaningful transparency to users and user control of data produced by or associated with an application, ensuring security and privacy;
3. Products that can be connected to the Internet should come with a clear indication on the data that gets collected, where the data are stored, and what the conditions for access are;
4. Stakeholders should work together to ensure consumers/citizens have choice when wanting to obtain current/popular services;
5. In order to establish a long term relevance of IoT products and services it will be key to establish a clear framework on transparency and accountability, with respect for current legislation and pre-empting changes in values and needs of citizens.

These ideas will be discussed during the IGF in Joao Pessoa, both during the DC IoT session and the IGF Plenary session on 12 November 2015. Aim is to develop in Joao Pessoa and over the coming year a better understanding on what an ethical way forward looks like, on a global level, working with a technology that is global, by definition – and on how such an ethical approach can be ensured.

---

[79] Internet of Things Good Practice policies, by IGF Dynamic Coalition on Internet of Things, dd. 30 July 2015, see http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/
[80] See for the work of the DC IoT: http://www.iot-dynamic-coalition.org/

Ultimately, the combination of technologies applied should lead to products and services that are transparent for the user in terms of how they collect, store and share information ("open" systems, or at least subject to scrutiny by independent experts), that give real choice to the user in terms of adapting that to his or her appreciation of local values (and legislation), and for which accountability for usages (and failure) is clear and redress is possible. It will require industry to commit to ethical standards, up and beyond privacy, government to lay its role in championing the public interest and legal protection of users, and independent researchers and civil society to continue to follow up and address the issues, by preference before they arise but for sure shortly after.

***Policy action**: Encourage innovators and providers to develop ethical technology in line with market and used needs (for instance following the guidelines above). This could be an important way for businesses to add value to their brand, and would also allow consumers to determine which companies hold ethical principles in high regard. The objectives would be to foster a value-added strategy much like what has happened for green tech over the last decade.*

Furthermore it should be noted that protection of IoT related applications and services and the information they generate is necessary to ensure sustainable trust in IoT environments[81]. Media reports of security failures associated with IoT applications show that the public's perception of security issues associated with IoT applications have brought attention to security in IoT and highlighted the importance of adequate security support. "Ethical" also means putting the right protections in place: as needed.

***Policy action:** develop a taxonomy for security of IoT applications per sector and type of application, thus ensuring a common understanding of what level of security is expected to be delivered by providers for specific applications; Develop a taxonomy for privacy sensitivity of IoT generated data collections, including recommendaed ways forward for collecting, storing, protecting and sharing these data.*

Whereas the complexities are far reaching and will require a longer debate, and operationalising in different sectors, it would be useful to create one global ethical charter, in interaction with stakeholders from all over the world: governments, industry, research and civil society.

***Policy action**: actively engage with and support the creation of a global ethical charter that would safeguard vital interests of consumers in IoT environments, offer guidance to developers of IoT environments and services (even ethical impact assessments before development). The development and implementation of such a charter is one potential consequence of a continuing programme[82] of research and debate on the ethical, legal, social and environmental aspects of ICT, specifically as regards the IoT.*

In line with these concrete policy recommendations, it may be useful to look at current engagements and stimulate European industry and in particular EU sponsored projects to actively participate in one or more of European and global multistakeholder platforms such as EuroDIG and IGF, where issues as trust, ethics and Human rights an inseparable part of the agenda when

[81] AIOITI WG04 Policy report, page 16

[82] Such a programme is recommended by the European Group of Ethic's Opinion 26 published in February 2012 and recent statements by Commissioner Kroes. These call for broad societal debate on trade-offs among comfort, security and privacy in order to promote a conscious development of an IoT world people would want to live in.

discussing technology progress in society. IoT is not just a technology issue: its emergence is a societal issue in which technology is merely just one of the perspectives.

6 List of Acronyms

AIOTI	Alliance for Internet Of Things Innovation
DC IoT	Dynamic Coalition for the Internet of Things within the IGF framework
EC	European Commission
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EuroDIG	European Dialogue on Internet Governance
FI PPP	Future Internet Public Private Partnership
GDPR	General Data Protection Regulation
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute for Electrical and Electronics Engineers
IERC	IoT European Research Cluster
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IoE	Internet of Everything
IoT	Internet of Things
ISOC	Information Society
ITU	International Communication Union
ITU-T SG20	ITU – Telecommunications standards related Study Group on IoT
MDG	Millennium Development Goals
PEM	Privacy Enhancing Methodologies
PET	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
RFID	Radio Frequency Identification
SDG	Sustainable Development Goals, following the MDGs
QoE	Quality of (customer) Experience
QoS	Quality of Service

UN	United Nations
WP29	Europe's Article 29 Data Protection Working Party
WSIS	World Summit on Information Society