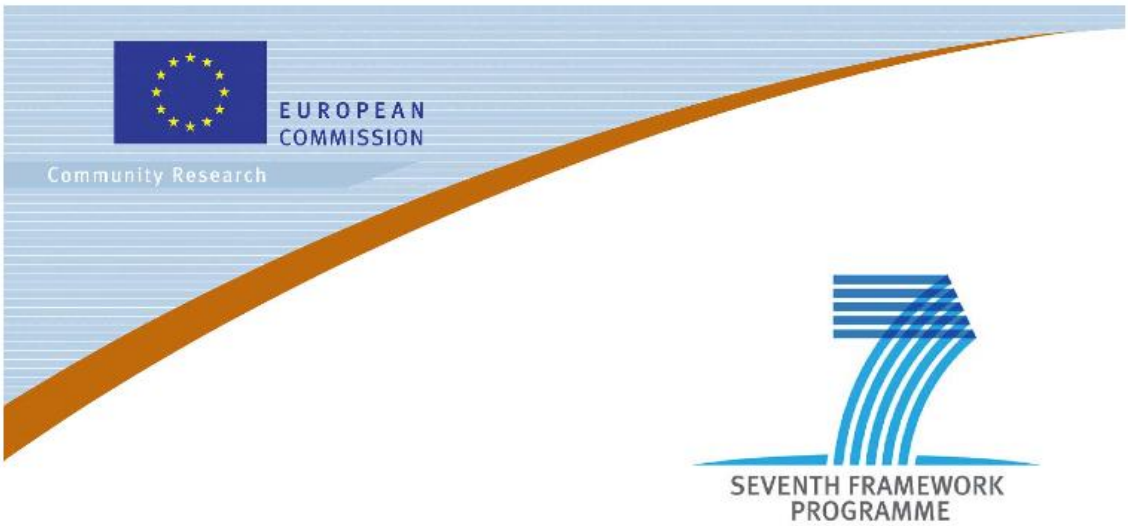

Private Public Partnership Project (PPP)

Large-scale Integrated Project (IP)

D.11.3.3: FIWARE Market and Policy Regulation Awareness

Project acronym: FIWARE

Project full title: Future Internet Core Platform

Contract No.: 285248

Strategic Objective: FI.ICT-2011.1.7 Technology foundation: Future Internet Core Platform

Project Document Number: ICT-2012-FI-285248-WP11-D.11.3.3

Project Document Date: 2014-02-16

Deliverable Type and Security: PP (Private)

Author: Juan Bareño

Contributors: FIWARE Consortium

1.1 Executive Summary

The objective of this task is dual, on one side it is about **establishing channels that could be a useful tool to promote business and innovation concepts coined by FIWARE** and to obtain feedback from external communities and on the other side it is to identify barriers at policy and regulatory level that could **prevent FIWARE from a successful exploitation and to define how Europe is working to overcome them.**

The key to the success will be a focus on the value created for the end users, new collaborative business models and ecosystems where all participants can be successful. Additionally, the FIWARE platform´s main objective **to promote a shared vision for harmonised European-scale technology** platforms and their implementation, as well **as the integration and harmonisation of the relevant policy, legal, political and regulatory frameworks**

The Future Internet gives rise to a wide range of new challenges regarding policy, regulation and governance. Making the Future Internet, to a success requires on the one hand the **removal of policy and regulatory bottlenecks** (for example those that hinder innovation), and on the other hand the creation of new policies and regulatory frameworks as well. Especially at the European level there is opportunity and need for **restructured policy and regulatory frameworks.**

Therefore we **analyze the European Context to the expansion of the service economy within the EC**, main European policies, regarding Future Internet, involvement of SMEs and entrepreneurs, Smart Cities…as well as the main regulatory barriers to overcome. The main objective of this analysis is to **present the landscape of such issues and challenges and define the advances so far and formulate the concrete activities** to be undertaken next years.

1.2 About this Document

This document is an on-going work aiming to complement the analysis carried out in WP11 under the tasks 11.1 Market and Competition Analysis and 11.2 Exploitation Strategy, FI-WARE sustainability and IPR Management. While the mentioned documents focus on the analysis of the external environment of FI-WARE from a market point of view and the definition of the FI-WARE Exploitation Strategy as such respectively, this specific report will keep an eye on those opportunities that could help FI-WARE to increase its impact in the market and/or alternatively identify those barriers that may prevent FI-WARE from being successfully exploited. We will pay special attention to those elements that fall under the categories of legal and regulatory barriers.

1.3 Intended Audience

As this deliverable contributes to defined FI-PPP Programme level activities the perspective and needs of FI-WARE and the FI-WARE consortium and related stakeholders are the addressed audience. As the dissemination level is "PP" (FI-PPP private) there is no plan to release this document to external parties.

1.4 Context of Chapter WP11 Exploitation

This work package focuses on a series of activities that identifies, create and work towards the exploitation and standardization opportunities of the FI-WARE project results. This work package approaches exploitation of the FI-WARE results from the point of view of the partners of the FI-WARE consortium, both individually and as a project. It does not intend to replace or overlap exploitation activities at the Future Internet Public Private Partnership Programme level, but to complement in a synergetic way the work that

other projects within Usage Areas will do in terms of take up of the generic enablers provided by FI-WARE., therefore complementing the perspectives of the partners of this project and the related stakeholders in the ecosystems they represent.

The exploitation of FI-WARE results is not based on a purely technological approach (technology push) but on the needs and requirements of the future "customers" and "users" of FI-WARE enablers. As a result, both supply and demand are meet within this WP.

With that in mind the project's exploitation activities have as main objectives the:

- Definition of project outcomes from an exploitation point of view, including identification of stakeholders and different typologies of users that will make use of FI-WARE
- Systematic analysis and continuous monitoring of market situation and trends
- Definition of overall and individual exploitation plans
- Definition of a framework for IPR and licensing management
- Definition of a Sustainability Plan for FI-WARE results
- Policy and Regulation Considerations
- Feedback of adjustments to project plan if necessary and promotion of the FI-WARE Testbed as an Open Innovation Lab
- Business oriented communication and training activities to increase market awareness and impact
- Definition and implementation of a standardization strategy that will enable adoption and achievement of the project goals and ambitions
- Definition of impact indicators and management of those along the project duration

This WP also supports and runs the project-level Standardization Committee that is in charge of the overall strategy, planning and execution of the Standardization activities.

1.5 Acknowledgements

The current document has been elaborated using a number of collaborative tools, with the participation of Working Package Leaders and as well as those industrial partners business people in their teams they have decided to involve.

1.6 Keyword list

Market awareness, exploitation, regulation, marketing, barriers, deployment, policy, privacy and data protection, net neutrality, open access to interfaces

1.7 Changes History

Release	Major changes description	Date	Editor
0.0	Table of contents	5/03/2014	Juan Bareño (Atos)
0.1	First draft	24/04/2014	Juan Bareño (Atos)
0.2	Contribution from Leaving Partners	15/05/2014	Contribution from Leaving Partners
0.3	Third Version	15/07/2014	Juan Bareño (Atos)
0.4	Fourth Version	15/10/2014	Juan Bareño (Atos)
0.5	Fifth Version	15/12/2014	Juan Bareño (Atos)
0.6	Sixth Version	03/02/2015	Juan Bareño (Atos)
0.7	Seventh Version	09/02/2015	Juan Bareño (Atos)
0.6	Review	12/02/2015	Juan Bareño (Atos)
0.7	Final	16/02/2015	Juan Bareño (Atos)

1.8 Table of Contents

1.9 Table of Figures

1.10 Table of Tables

2 Introduction and Background

The objective of this task is dual, on one side it is about **establishing channels that could be a useful tool to promote business and innovation concepts coined by FIWARE** and to obtain feedback from external communities and on the other side it is to identify barriers at policy and regulatory level that could **prevent FIWARE from a successful exploitation and to define how Europe is working to overcome them.**

The key to the success will be a focus on the value created for the end users, new collaborative business models and ecosystems where all participants can be successful. Additionally, the FIWARE platform´s main objective **to promote a shared vision for harmonised European-scale technology** platforms and their implementation, as well **as the integration and harmonisation of the relevant policy, legal, political and regulatory frameworks**

The objectives are the following:

- Establishing Market Awareness
    - **FIWARE aims to achieve a great impact on the Internet community, mainly targeting third party developers** and relevant actors as Smart Cities and Large Companies willing to exploit its Future Internet core-platform through the **FIWARE Lab** enabling entrepreneurs to develop and test Future Internet applications with FIWARE technologies
    - **The involvement of European cities, Industry**, as potential ecosystems, –and other communities (SMEs, entrepreneurs...) in the experiments will be crucial
    - One essential factor that can determine **the successful adoption of FIWARE by customers and** is the **establishment of FIWARE as a standard in any given sector of application**.
    - To identify the **reference use cases highlighting the positive impact achieved by using the FIWARE platform.**
    - To promote the **adoption of FIWARE in Europe and other regions** where the take-up of Internet innovation can occur quickly and impact local markets FIWARE Mundus
- Analysing the **Policy and Regulation context**, and when possible, contributing to shape it in a way that is beneficial for FIWARE deployment and exploitation
    - **The heterogeneity of legislation across Europe** covering security, privacy, trust, and digital rights is a barrier to entry for ICT SME. **Europe needs to reform and forge a true digital single market.**
    - In addition to the reappraisal of regulatory frameworks and practices that the rise of platforms in ICT markets invites, **FIWARE have identified the main regulatory challenges from the technical chapters and those non-technical aspects that could influence** FI-WARE exploitation in one way or another.
    - **Developing a comprehensive approach towards regulatory and policy issues** such as interoperability, openness, standards, data security and privacy within the context of the Future Internet complex and 'smart' usage scenarios

Regarding FIWARE progress in Market Awareness, we started to build a strong value proposition around FIWARE. This value proposition has shown to be particularly **strong in the vertical domain of Smart Cities and also in the IoT (Internet of Things) space.** FIWARE is actually experiencing a great momentum in both areas.

- In the case **of Smart Cities**, rumours say that the EC may soon publish a series of recommendations and best practices in which FIWARE would be explicitly mentioned.
- In the case of IoT, **discussions are taking place within EIRC (**European Research Cluster on Internet of Things) community to adopt **FIWARE as common foundation for an IoT platform**. We have also started promotion of **FIWARE results in GSMA.**

One of the unique selling points in our value proposition is the FIWARE Lab. 2014 has not only been the year at which **expansion in Europe** has started but also when **countries beyond Europe have arrive to us willing to join and expand the footprint of FIWARE Lab in their countries**.

- **Relevant to mention is the recent incorporation of Mexico**. Interestingly enough, some organizations are starting to approach us showing their interest to join the FIWARE Lab by contributing their resources (without that requiring funding from FIWARE). The experience demonstrates that there is a lot of potential to engage other countries/regions.

The FIWARE Acceleration Programme was launched last September. This was cornerstone in the now called FIWARE PPP (formerly known as Future Internet PPP). Thanks to the active role of FIWARE Accelerator projects, but also the support provided by the FIWARE partners, particularly through the series of **Start-up Weekend FIWARE special edition events,** FIWARE has raised a lot of interest among entrepreneurs in Europe.

- The results of the first Open Calls launched by the FIWARE Accelerator Projects have gone beyond the initial expectations.
- This means there will be soon hundreds of SMEs/start-ups working with FIWARE technologies, many of them experimenting on the FIWARE Lab. We have to provide them the necessary training, coaching and support has to be one of our first priorities!

All 2014 were sprinkled with our presence in many events. We have to be able to **combine both global relevant events as well as events focused locally in each country in 2015.**

- **Regarding events focused locally,** I would like to share with you the experience with the multi-site event co-organized with the Ministry of Industry in Spain. This event was instrumental in gaining a strong endorsement of the Government in Spain but also reaching a high awareness among Spanish Entrepreneurs (as a proof of this, it happened that a rather large number of SMEs/start-ups from Spain submitted their applications to the FIWARE Acceleration Programme). **We should seek for similar events in other countries in Europe. At least in Germany, France, Italy and Finland, Israel as well.** I encourage partners in those countries to come up with the design of a local-focused event.

Regarding Policy and Regulation context, Apps, by their very nature, work across borders, networks and devices and thus contribute to a single market. To support continued growth of the apps ecosystem and the role of apps in relation to the European single market consumers must be able to access and use apps (i.e. apps must not be subject to blocking or anti-competitive discrimination). **Europe needs to reform and forge a true digital single market**. This will give European entrepreneurs, who have all the right building blocks, the **incentive to invest and the ability to achieve global scale** at greater speed. Significant political will needs to be mustered to support these changes and **ensure Europe's startups succeed**.

The plan of the Commission is to develop "a truly connected digital single market" in Europe through swift and ambitious legislative steps in the areas of data protection, telecoms regulation and by modernizing and simplifying copyright and consumer rules for online and digital purchases.

If Europe's single market becomes truly and thoroughly digital, the macroeconomic benefits would be enormous. **Europe's digital businesses no longer would have to get individual licenses to operate in 28**

different countries. If regulatory barriers are removed, start-ups could directly access half a billion European consumers, a market that's larger than the US, where technology companies have the ability to achieve scale before they expand internationally**.**

FIWARE platform´s main objective **to promote a shared vision for harmonised European-scale technology** platforms and their implementation, as well **as the integration and harmonisation of the relevant policy, legal, political and regulatory frameworks.**

Imagine if this vibrant European entrepreneurial scene could benefit from a digital single market, which would end the need for obtaining different national licenses and reduce regulatory red tape. High-growth firms and technology-intensive start-ups suddenly could scale-up and **compete more vigorously in the global marketplace.**

3 Market Awareness

FIWARE aims to achieve a great impact on the Internet community, mainly targeting third party developers and companies willing to exploit its Future Internet core-platform through the **Open Innovation Lab** enabling entrepreneurs to develop and test Future Internet applications with FI-WARE technologies and that will be launched at the end of July with a huge official event in September (as part of the Campus Party; London, first week of September). For the Open Innovation Lab success **is key the fact of fostering developer communities**.

FIWARE (http://fiware.org) is an open initiative targeted to create a sustainable ecosystem where European companies, and companies in other regions who wish to join Europe in this endeavour, will be able to capture the opportunities that will emerge with the new wave of digitalisation brought by combining the Internet of Things with information and Big Data services on the Cloud.

The value proposition of this target ecosystem is built around four major pillars:

- **The FIWARE Open Platform**: The FIWARE platform provides a rather simple yet powerful set of APIs (Application Programming Interfaces) that ease the development of IoT and Smart City Applications. The specifications of these **APIs are public and royalty-free**. Besides, an **open source reference implementation of FIWARE components is publicly available** so that multiple FIWARE providers can emerge faster in the market with a low-cost proposition.
- **The FIWARE Lab**: The FIWARE Lab, launched on 6 September 2013, is a non-commercial sandbox environment where innovation and experimentation based on FIWARE technologies takes place. Entrepreneurs and individuals can make **"hands on" the technology** as well as **test and showcase** their applications on The FIWARE Lab, **exploiting open data published by cities and other organizations**. Several cities are already connected or are currently working on setting up a connection to the FIWARE Lab in order to export their open data in this environment. To be close to its adopters the FIWARE Lab is deployed over a geographically distributed network of federated nodes. Their operation is powered by the FIWARE Ops suite of tools.
- **The FIWARE Acceleration programme**: The FIWARE Acceleration programme is aiming at promoting the take up of FIWARE technologies among solution integrators and application developers, with special focus on SMEs and start-ups. As an example, the EU launched an ambitious campaign in September 2014 mobilizing 100M€ to support SMEs and entrepreneurs who will develop innovative applications based on FIWARE.
- **The FIWARE Mundus programme**: Despite born in Europe, FIWARE is designed with a global ambition, aiming at expanding to other regions. The FIWARE mundus programme is designed to bring coverage to this effort engaging local ICT players and domain stakeholders, and eventually liaising with local governments. As a first achievement, partners in several countries of Latin America (**Mexico, Brazil, Chile**) with support of their local government are embracing FIWARE, working on the setup of FIWARE Lab nodes in their countries and promoting FIWARE locally. Opportunities also clearly exist in other regions like **Africa** and **Asia**

The success of the FIWARE concept will depend very much on the use of the adequate technological solutions and its ability to engage small and medium developers to use the different tools FIWARE is going to provide. In the end, FIWARE success will depend on the success of the applications that are going to be developed on top. FIWARE will succeed if the developers using FIWARE succeed.

In this context we have defined the following tasks and within them the according actions:

- **Identifying the target audience**
    - Involve SMEs, Web developers and other Open Source Communities to create the developers community around FI-WARE
    - Involve Relevant Actors, as Smart Cities and Large sectorial companies, as promoters of innovation ecosystems
- **Designing relevant business messages**
    - Elaborate marketing material for business impact
    - Validate FI-WARE messages
- **Selecting communication channels and activities to create Ecosystem**
    - Business events are a suitable tool to raise awareness and to obtain feedback from participants
    - Promote FIWARE Lab
    - FIWARE mundus: FIWARE extending its reach
    - Trainings
    - 3rd Call: Organization of Hackathons
    - Apps Developers feedback (i.e. Foodloop y Smart Taxi)

One essential factor that can determine the successful adoption of FIWARE by customers and the creation of a market-pull, and ultimately the proliferation of ecosystems is the establishment of FIWARE as a standard in any given sector of application.

- **Public policies may have a big impact on the establishment of a standard**. If well it's true that publicly endorsed initiatives get wider attention by the community, there are potential issues that need to be taken into consideration.
- **Lack of coordination within policy makers could result in several incompatible approaches**. In the case of Smart Cities, for example, each municipality could endorse FIWARE as a standard for its current, concrete needs, but other applications and systems would then have to be reviewed afterwards to leverage and profit from the FIWARE ecosystem.
- **Lacking a holistic view of the FIWARE initiative** in all of its extension, could eventually lead to barriers. Dissemination of FIWARE and its adoption is essential to unleash its full pot

3.1 Identifying the target audience

FIWARE aims to achieve a great impact on the Internet community, mainly targeting third party developers and companies willing to exploit its Future Internet core-platform. The experiments and use trials, and the **involvement of European cities, Industry, as potential ecosystems, –and other communities (SMEs, entrepreneurs...)** in the experiments will be crucial

Action 1 ⇨ Involve SMEs, Web developers and Open Source Communities to create the developers community around FI-WARE

Since **SMEs, web developers and other ICT companies are important for the purpose of creating the developers community around FIWARE GE**. As it was anticipated in the strategy, FIWARE will need the experience, contact and involvement of other associations that can act as interface to a big base of potential users/clients. These organizations will have additional elements of value to present to their communities, and FIWARE will get access to them, resulting in a win-win situation.

The FIWARE Acceleration programme is aiming at promoting the take up of FIWARE technologies among solution integrators and application developers, with special focus on SMEs and start-ups. As an example, the EU launched an ambitious campaign in September 2014 mobilizing 100M€ to support SMEs and entrepreneurs who will develop innovative applications based on FIWARE

Through open calls, the third phase calls for SMEs and Web entrepreneurs to develop highly innovative services and applications. The 16 selected "accelerator projects" will publish Open Calls for the distribution of grants to SMEs and Web entrepreneurs as of September 2014. SMEs and Web entrepreneurs may submit proposals to one (or perhaps more) of these Open Calls, in accordance with the requirements defined by the projects launching the Open Calls

Other communities that have been approached in the last period are, for example, ICT Labs (for the purpose of extending technical works and mainly because of its potential for development of entrepreneurship initiatives around FI-WARE and future academic programmes), clusters of researchers with close elements to those of FI-WARE (ex. The IERC cluster working in IoT) and actors in the context of Smart Cities, as previously described**.**

Despite born in Europe, FIWARE is designed with a global ambition, aiming at expanding to other regions. The FIWARE Mundus programme is designed to bring coverage to this effort engaging local ICT players and domain stakeholders, and eventually liaising with local governments. As a first achievement, partners in several countries of Latin America (**Mexico, Brazil, Chile**) with support of their local government are embracing FIWARE, working on the setup of FIWARE Lab nodes in their countries and promoting FIWARE locally. Opportunities also clearly exist in other regions like **Africa** and **Asia**.

Practical case: The EIT ICT Labs

FIWARE has given support to the setting up of the so called Internet Innovation Hubs.

An Internet Innovation Hub refers to a physical place/infrastructure with real people and office space that brings together the needed actors and resources to deliver new business on Internet economy. Specifically it will bring together web entrepreneurs, mentors, investors, students, academia, public sectors, innovators and industry.

FIWARE has also collaborated with ICT Labs in the provision of training on FIWARE technologies (e.g. the FIWARE workshop recently held in Paris, one of the nodes of ICT Labs). The main intention of such

collaboration is **the extension of the number of experts and ambassadors on FIWARE technologies** (training of trainers) so that our training network scales to the extent needed by the programme as well as by the adoption strategy by other parties and potential customers.

Action 2 ⇨ Involve Relevant Actors, as Smart Cities and Large sectorial companies, as promoters of innovation ecosystems

Next Generation of Internet Based Services, business-enabling platforms are one trigger for this new kind of collaboration. Motivating market players to **collaborate on a common platform** is the foundation for the next generation of Internet-based services. As this Internet application and service revolution continues, successful multi-purpose transactional platforms can unlock long term and sustainable revenue streams yet to be identified.

Recently many companies **have adopted the strategy of using a platform to attract a mass following of software developers** as well as end-users, building entire "software ecosystems". **Therefore, the actual level of competition should be between ecosystems.** For this purpose of potential innovation ecosystems promotion, FIWARE has carried put the following actions:

- **As Smart Cities are considered as open innovation ecosystems** and playgrounds to exploit the opportunities of the Future Internet, several **European cities** have been informed, within the current dynamic of the project, about FI-WARE platform availability
- **Continuation of fostering the interaction between the European industries, ICT and sectors** through the Use Cases mainly:

FIWARE as an open platform, developed with the contribution of hundreds of developers across Europe and supported by reference industrial players, universities and research institutions the FIWARE platform **may play a key role in the cities of the future**. Its massive adoption may help to speed up the replication of key components for setting up and consolidating the smart city ecosystem. However, for succeeding in such an endeavor it is of utmost relevance to **be aware of the potential limitations of the present platform** with the aim of identifying a set of actions for overcoming them. For this purpose we will define the following action plan:

- Identify the **needs, which are or not yet fulfilled by the platform**, in terms of the ecosystem requirements. This study will rely on the feedback provided directly by some of the cities through a questionnaire circulated by the European Commission as well as any other valid source.
- In the case of cities already using FIWARE, to **identify the key features which need to be improved** from a technical and commercial perspective to ease their adoption.
- To identify the **reference use cases highlighting the positive impact achieved by using the FIWARE platform in the city context.**

Plans for standardisation activities based on the assumption that most EU cities will manage their Smart Cities by means of a shared platform (be it FIWARE or another platform) would benefit from being supplemented by a market analysis of who the main global suppliers in the Smart Cities sector are, what financial investment they have in the field and whether the existence of standards is consistent with their commercial interests and ability to deliver and sustain proprietary applications.

City Platforms will require building the relevant Generic Enablers for Internet of Things Service Enablement, in order for things to become citizens of the Internet – available, searchable, accessible, and

usable – and for the City Platforms services to create value from real-world interaction enabled by the ubiquity of heterogeneous and resource-constrained devices.

- **The Internet-of-Things (IoT) will be an integral component of the Future Internet** (FI) and therefore should be smoothly integrated within FI service delivery models and the emerging utility based cloud computing paradigms. To-date several researchers have described the benefits of a pervasive (sensor-based) distributed computing infrastructure without however providing a systematic and structured solution to the formulation and management of utility based IoT environments.
- **IoT is a major component of smart city infrastructures.** It is subject of the development of architectural models (e.g. ITU), several are competing at this stage. Europe has moved forward with FI-PPP and **open IoT, and smart city is a good umbrella to further secure European developments in this field**.
- **The standardisation of IoT is still a subject of studies**, and of choice. The recently launched **exercise with ETSI will** provide outputs not only related to implementation, of vertical siloes, but also making possible cross use case capabilities. **TC M2M is the forum of choice to progress the issue in Europe.**

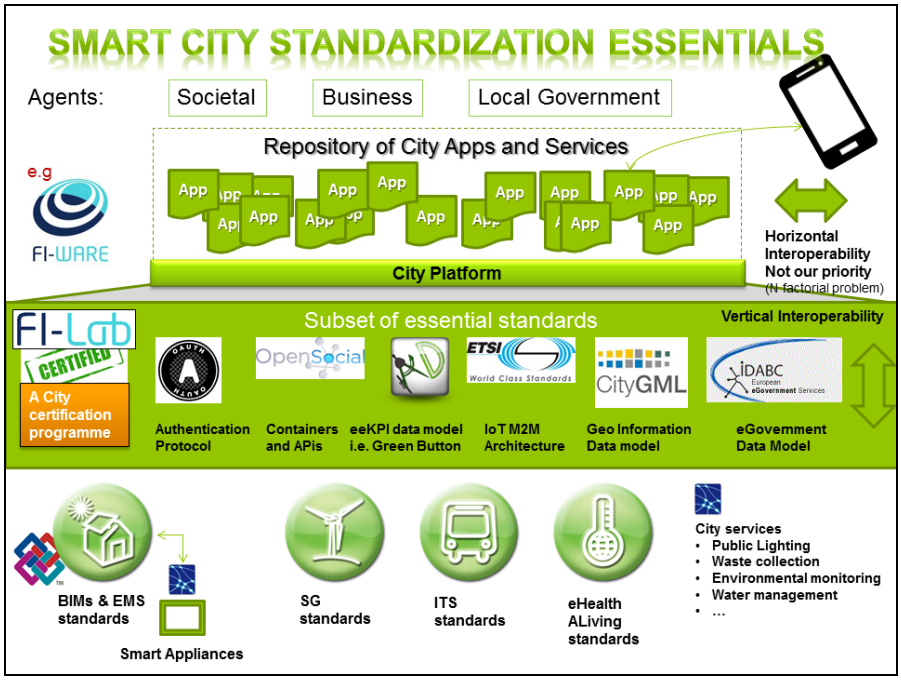

Figure 1: FIWARE Smart City Standardization Essentials

Smart City Applications on FIWARE

In this context, **cities will experiment a profound transformation**. Life in cities is still very similar to how it looked like 15 or 20 years ago. The Internet of Things, Cloud, BigData and the support of Open Data policies, all together in a smooth and seamless manner cooperation will create the conditions for a new period of intense transformation of cities into smart cities. However, the concept of "Smart City" is also under (re)volution, since it will not just be focused on providing more efficient services but becoming a digital platform being the fuel for a new economic boost, fostering growth and the creation of new jobs

through the enabling of development of innovative citizen services open to all. In contrast with the "Home", because of different city stakeholders, levels of regional development and local regulations, **cities are an ideal environment for telecom operators, ICT solution integrators** and other relevant providers of key city services (electricity, water, infrastructures…).

The initiative is **intended to help build healthy ecosystems** and ensure that the Internet of Things is **not controlled by a small number of large companies**. For example:

- **Cities will be able to publish their open data on the online FIWARE sandbox**, FIWARE-Lab, so developers can create smart applications using this data and standard FIWARE APIs.
- **Smart city applications developed and tested in one city can be replicated and amended in other cities**, creating scale opportunities for developers. In fact, there are several cities already working to deliver their Open Data (both historic and real-time) on FIWARE-Lab. This includes Lisbon (Portugal), Trento and Torino (Italy), Espoo (Finland), Santander, Seville, Malaga, Valencia, Las Palmas de Gran Canaria, and Sabadell (Spain).

In this context, the m**ajority of Smart City applications were developed using a mix of the following three types of approaches:** deploying datasets through the **open data platform, based on CKAN [CKAN**]; integrating city **sensors with the FIWARE IoT platform** and their **consumption through the NGSI context API** (Next Generation Service Interfaces - FIWARE Open RESTFul API Specification); and finally, integrating dynamic and/or structured information through the context API. The current status of this work is summarized in the table below.

City	Country	IoT	Open Data	Context	Prototype
Amsterdam	Netherlands		✔	✔	
Barcelona	Spain		✔		
Espoo	Finland			✔	Energy consumption dashboard
Helsinki	Finland			✔	Participation dashboard (CitySDK-Open311)
Las Palmas	Spain		✔	✔	Port management dashboard
Lisbon	Portugal		✔		Mobility and social networks
Lleida	Spain		✔	✔	Public transport and accessibility
Logroño	Spain		✔	✔	Smart watering, City App
Malaga	Spain	✔	✔	✔	Citizen as a sensor
Rotterdam	Netherlands		✔		
Santander	Spain	✔		✔	Big Data / Open Data publication of IoT
Seville	Spain	✔	✔	✔	Fountain water management, Crowd detection
Torino	Italy		✔		Security & participation

Trento	Italy		✔		TBC
Valencia	Spain		✔	✔	Smart Taxi
Vigo	Spain		✔	✔	City App
Porto	Portugal	✔	✔		Environment, Open Data on Tourism and Smart Metering Water

Table 1 Smart City Applications on FIWARE

Regarding Smart Cities, It depends very much on the city, but what we typically face when we start a conversation with a **city that wants to connect with FIWARE AND FIWARE-Lab is:**

- First, we find out (and encourage) that they **publish a large number of open data.**
- The second scenario is when a city is **already managing a sensor-based system**, for example, public transport buses may be collecting data that is valuable that we would like to make available in real-time. So what we are doing with them is creating adaptors for the data sources and sensor technologies that the city already has in place. Then they can inject that **data into a context broker, and that context broker component will offer standard APIs** to allow anyone to consume real-time data. **Previously, there was no standard API to manage real-time data for cities**.
- Third, we look to cities who have some **sensor networks** and we help them make those available on the FIWARE platform

While many connected objects are already deployed in European Cities, **the proprietary solutions are dedicated to process or cost optimization without the required openness to support service creation** involving all actors: cities, citizen, business players and social actors.

Definition of standard APIs (Application Programming Interfaces) becomes crucial in the development of a competitive market **supported by Open Innovation and a sustainable ecosystem around IoT-based solutions and services.**

The support of a common set of standard APIs and the collaboration with domain stakeholders in the development of **standard data models will accelerate innovation in Smart Cities** environment, taking advantage of seamless connectivity and open data resources. Taking full advantage of this market opportunity, **many start-ups and small enterprises will create new services using innovative devices and improve Quality of Life for citizens in urban areas.**

This is a value proposition that several cities in Europe have welcomed so they have started experimenting with FIWARE, making their open data available for experimentation on the FIWARE Lab. Helsinki and Espoo in Finland, Rome, Trento and Torino in Italy, Lisbon in Portugal, Amsterdam in the Netherlands, Valencia, Seville, Málaga, Santander, Barcelona and several other cities in Spain are just the first examples, but new cities everyday are showing their interest and joining the initiative every day

European Industries

Increase **the industrial competitiveness of business sectors in Europe whose impact in the economy is relevant enoug**h so that we ensure that they do not lack behind other competitors, and furthermore that they go beyond them. The way the FI PPP will contribute to that is by bringing the technology to its adoption in those sectors.

This revolution is also coming to our homes. The **Digital Home** is still a promise and an aspiration, but leveraging on the adoption of the smartphone and their ability to connect to smart sensors and actuators in a plug&play fashion, it may now become a reality. Competing with those companies who are dominating

the ecosystems around smartphones and tablets, manufacturers of high-quality smart objects (e.g., electrical appliances), Telecom Service operators and solution integrators can still play a role in this domain.

Next steps may address relevant application domains like the **Digital Car**, **e-Health**, **Smart Manufacturing**, etc. will experience a relevant development as a result of combining the Internet of Things with information and BigData services on the Cloud.

FIWARE, as derived from this, is a crucial piece in this puzzle, and the collaboration with all the other projects of the FI PPP in this phase and the next ones is as important as the construction of the technology foundation itself.

The largest amount of efforts in collaboration so far have been invested in cooperation with the projects within the FI-PPP, **Use cases,** in order **to fine-tune the strategy towards exploitable platform components in actual scenarios in different domains such as environmental care, transportation logistics of goods and people**.

3.2 Designing relevant business messages

Translating technical messages into business language (marketing material). **Our family of brands, marketing material and website experienced** an evolution towards a more professional, market and product oriented image thanks to Ogilvy.

3.2.1 Evolution of brands, marketing material and website for business impact

Promotional material like flyers, brochures and merchandising are often a good tool to disseminate and improve the project presence, always allocating a reasonable amount of efforts for these tasks.

Action 3 ⇨ Elaborate marketing material for business impact

Promotional material like flyers, brochures and merchandising are often a good tool to disseminate and improve the project presence, always allocating a reasonable amount of efforts for these tasks.

In the last six months, **FI-WARE has produced a new poster explaining the overall vision**, towards a more professional, market and product oriented image thanks to Ogilvy.

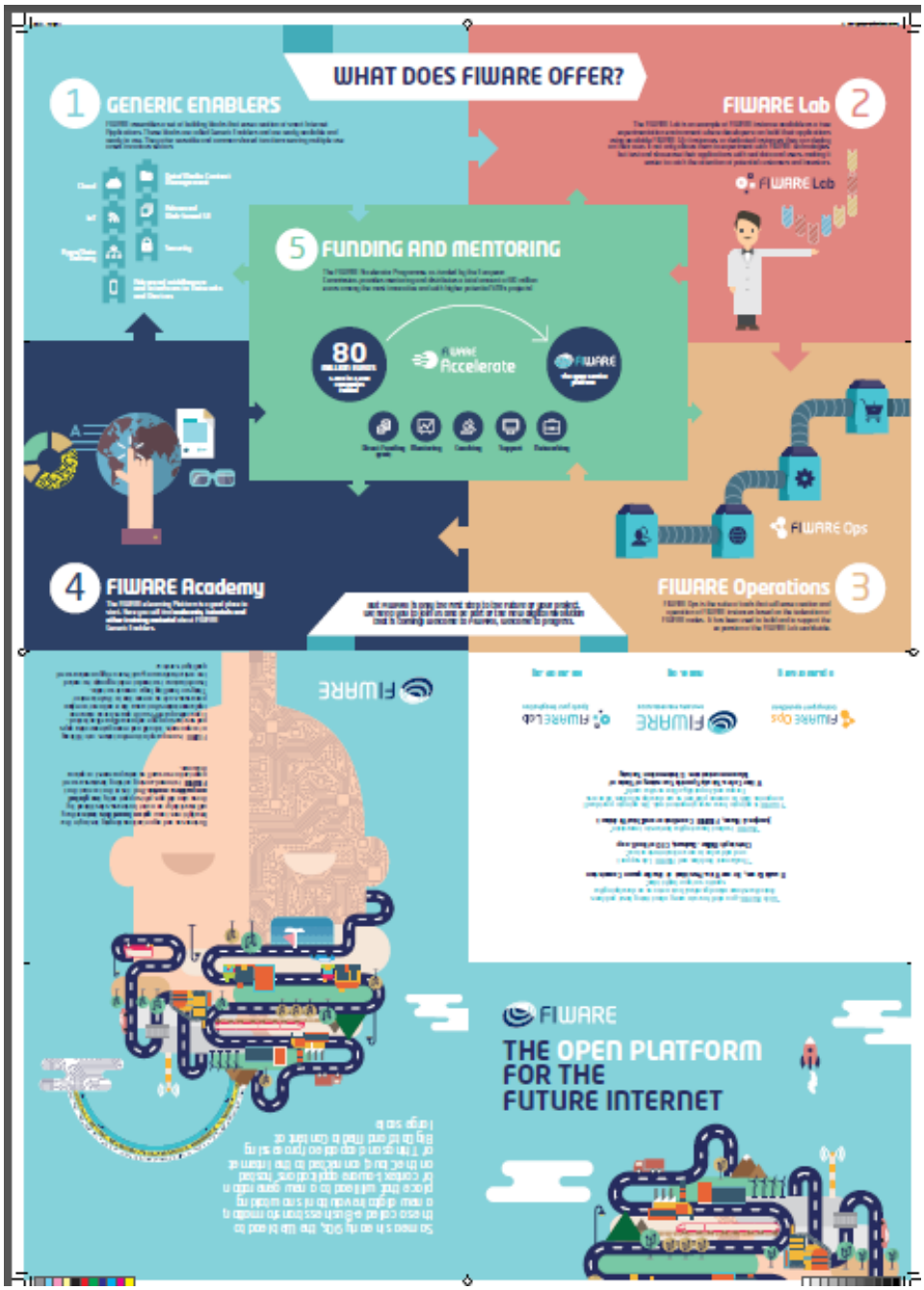

Figure 2: What does FIWARE offer?

Action 4 ⇨ New FIWARE developers web page and home for the catalogue – evolution of the catalogue

A new http://www.fiware.org/developers/ web page served from fiware.org (WordPress) which will be basically structured in the following sections:

- "What's FIWARE?
- Section which provides a link to the Quick FIWARE Tour Guide for developers page
- "FIWARE on the road" section which helps to discover next events linked to bootcamps, workshops, hackathons, challenges, etc and info from previous events.
- FIWARE Live Demos, examples and use cases on how to use FIWARE.

A new http://www.fiware.org/developers/guide web page served from fiware.org (WordPress) which will work as table of contents with icons-titles corresponding to each of the subsections of the "Quick FIWARE Tour Guide for developers. Each of these icons will link to the different stories and how to's of the FIWARE technical white paper.

A new homepage for the Catalogue. Structured in the following sections:

- Link to the quick FIWARE tour guide for developers
- Alternative implementations of FIWARE GEs: products that claim to be compliant with FIWARE GE specifications.
- FIWARE academy
- Bundles: as it is now it links to the list of Bundles
- Tools: as it is now it links to the list of Tools

3.2.2 Validate Messages

The objective is to extract **conclusions for the work carried out by Use Cases and SMEs** in the implementation of a working pilot using Generic Enablers of the FI WARE Platform.

- To analyse those GE that Use Case projects are planning to use in their pilots and trials
- Future internet generic enablers for SME- technical and business analysis from the TIC pilot implementation activities within Smart Agrifood project-ARIADNA Case

Action 4 ⇨ Validate FI-WARE messages

Defining FIWARE as a product

A clear communication plan For SMEs and Entrepreneurs to define how FIWARE will be offered, who will provide it. What FIWARE as a product is for?

- For SW developers
- For SMEs and Entrepreneurs: same. To become a business case
- User industries: focus on cities & the public sector and smart manufacturing, agro-food and energy.
- For SW and service providers.
- FIWARE infrastructure providers

3.3 Selecting communication channels and activities to create Ecosystem

With the potential market identified and business messages clarified it is now the time to select some of the relevant activities and events where the project could expand its influence, get new potential users/customers and present its main contents to make relevant communities aware of it.

- Business events are a suitable tool to raise awareness and to obtain feedback from participants
- Promote FIWARE Lab
- FIWARE mundus: FIWARE extending its reach
- Trainings
- 3rd Call: Organization of Hackathons
- Apps Developers feedback (i.e. Foodloop y Smart Taxi)

3.3.1 Business presentations and events

FI-WARE dissemination activities aim to **influence the broader community and foster the adoption of FI-WARE results by participating in relevant industrial events such as conferences, workshops, symposiums** or Code Camps or in events organized by the EU. Specific effort will be made to inform Open Source communities through participation at relevant events.

Business events are a suitable tool to raise awareness and to obtain feedback from participants. In order to provide a homogeneous vision of the project and facilitate the replication of the sessions (this has proven to be useful to minimize efforts and maximize the representation of the project), a typical session has been designed. See the structure below.

Organize International Events

During the latest month, **the most relevant activities have been**:

- **At the very beginning of the year, FIWARE was present at Campus Party Brazil**, where the awards of both the Smart City and Smart Business Challenges were given, while also new challenges for developers were launched: the Smart Society Challenge, which promoted initiatives pursuing benefits for today's society, and the FIWARE Excellence Challenge, which promoted those apps making the most of the FIWARE technology. As for the first challenges, the best apps received a total amount of 290,000 €, the winners of the first prizes being FI-Guardian and Foodloop. Campus Party Brazil was but the first evidence of the great wave of innovation that FIWARE was about to bring, making new space for development and entrepreneurship, as the founder of Girls in Tech said.

- **But, apart from attending international events such as CeBIT 2014**, this year has been the year of the FIWARE expansion, with the creation of FIWARE nodes all around the world and the setting of nodes in cities like Seville, Málaga, Santander, Las Palmas de Gran Canaria, Valencia, Trento, Torino, Espoo or Lisbon. But this effort went beyond the European boundaries, and soon countries from other continents announced their implementation of FIWARE nodes, such as Mexico or Brazil

Organize National Events

- FIWARE has actively worked in the organization of the Spanish workshop held in Madrid (20 June). Juanjo Hierro, made an overall presentation on FI-WARE and I tried to provide a view on how to use FI-WARE to get business value
- A Multisite event which was held in three different Spanish cities at a time, Seville, Valencia and Las Palmas de Gran Canarias. In this multisite event, a total amount of 190,000 € was delivered among the best apps using FIWARE; Cares was chosen as the best solution for today's society, while both FI-Guardian and Fonesense were chosen as the apps making the best use of FIWARE technologies.

However, if 2014 was the year of something, it was the year of the FIWARE Accelerator Programme. This European initiative was also presented at international events such as the **European Conference on Future Internet and Smart City Expo 2014, the latter taking place in Barcelona.**

And although FIWARE reached many countries through events, start-up weekends, challenges and workshops, it is not the only growth that we have witnessed. T**he FIWARE community keeps growing all around the world**. More than 1,300 people have joined our Facebook page since the beginning of the year, while in Twitter, that amount climbs up to 3,885

3.3.2 Promote FIWARE Lab

The second major breakthrough of FIWARE Lab was the expansion to a European network of federated nodes thanks to the **XIFI project**. FIWARE is twinned with this project that focuses on the uptake, deployment and federation of instances of FIWARE facilities. This is achieved via one of their major results, **FIWARE Ops**, a collection of tools that ease the deployment, set-up and operation of FIWARE nodes expanding an existing FIWARE instance such as the FIWARE Lab, or the creation of new FIWARE instances.

FIWARE Lab has turned into a truly pan-European **network of federated nodes** that keeps on growing to multiple locations (expected to reach 3000+ cores, 16TB+ Ram, 750TB+ HD soon). Users can decide on what location/node to deploy their service. All of the nodes are accessible by **a single user portal** and work in the same way, no matter where you are! Putting together current nodes and future incorporations, we already have many nodes: Spain, Trento, Lannion, Waterford, Berlin, Mexico, Zurich, Budapest, C4I, Karlskrona, Gent, Prague, two locations in the Athens area, Volos, Stockholm, Poznan, Crete

Action 5 ⇨ Promote the FIWARE LAB

FIWARE Lab is an open meeting point, where entrepreneurs take their ideas and find customers and investors who want to bet on the applications they developed. Campuse.ro, network geek knowledge of

Campus Party, acts as a channel for dissemination of FI-WARE / FIWARE Lab between the geek communities and centralizes FI-WARE challenges.

3.3.3 FIWARE extending its reach: FIWARE Mundus

As recently announced via the FIWARE Portal, **an important set of promotional activities aiming at paving the way towards a Global Future Internet Ecosystem** has been formally presented as the FIWARE Mundus offering.

The FIWARE Mundus Programme establishes a number of worldwide and regional links with a twofold purpose:

- On the one hand, FIWARE Mundus promotes the **adoption of FIWARE in Europe and other regions** where the take-up of Internet innovation can occur quickly and impact local markets.
- On the other hand, FIWARE Mundus **defines a long-term vision for FIWARE technologies** and business models taking into account equivalent research and innovation schemes in the US, Japan, Canada, Korea and beyond.

The FIWARE Mundus Programme organizes conferences and workshops to facilitate the identification of new European and international stakeholder groups and support the exchange of knowledge and best practices between FIWARE and the larger Future Internet community.

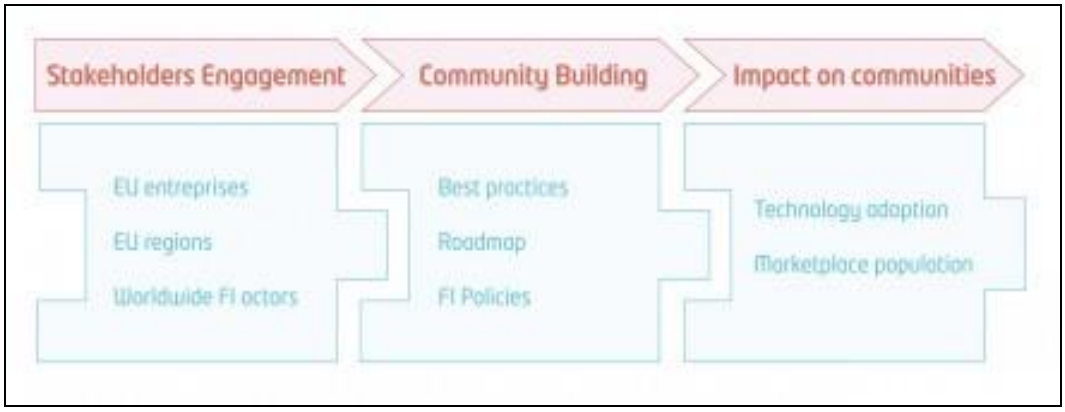

Figure 3: What does FIWARE offer?

The FIWARE Mundus Programme plays a crucial role in benefiting emerging Future Internet communities, such as South America or Africa, and allowing them to join an innovative and open source platform for the creation of Future Internet solutions and applications based on FIWARE in their countries.

FIWARE Mundus is developing a comprehensive Roadmap of the technical and business directions of the Future Internet research and innovation and the road ahead:

- **Benchmarking the quality of FIWARE technologies** and business models against similar research and innovation schemes in the international domain.
- **Promoting the establishment of a shared medium**- (2020) and long-term (2030) vision for Future Internet technologies.

FIWARE Mundus is looking at expanding the FIWARE ecosystem in European regions and at international level. At this stage 13 European regions have been "pre-selected" as the most likely candidates for the "FIWARE Regions" label: Helsinki (Uusimaa, Finland); Brittany, PACA, and Paris Ile de France (France); Berlin and Baden-Wurttemberg (Germany); South East Ireland; Lombardy and Emilia-Romagna (Italy); Wielkopolska (Greater Poland); Porto (Portugal); Catalonia and Canary Islands (Spain). In addition, other regions being considered include South Moravia (Czech Republic); Copenhagen region (Denmark); Picardie (France); Basque country (Spain); and Stockholm region (Sweden). "FIWARE Regions" are defined as those regions willing to set up a sustainable FIWARE ecosystem in the medium to long term, with support from regional public authorities and other relevant players in the regional Future Internet ecosystem.

Some of those FIWARE Regions will work hand in hand with the "innovation hubs" recently selected by FIWARE. All together they will form the FIWARE European ecosystem under the FIWARE Mundus umbrella. FIWARE Mundus is also looking at international expansion and cooperation. **A FIWARE node and ecosystem is currently being set up in Mexico** and should be operational in Q1 2015; contacts have been established with other Latin American countries, in **particular Chile and Brazil**, and with other parts of the world.

3.3.4 3rd Call: Organization of Hackathons

Hackathons are powerful tools to attract developers around the project and will serve as mechanism to assess, among other aspects, how attractive and easy-to-use the FI-WARE technology is.

Action 9 ⇨ Organize a Hackathon

Going forward, the biggest challenge FIWARE faces will be the uptake of its platform. To this end, it is **running hackathon challenges** with some serious prize money to encourage developers to join the emerging ecosystem. The platform has also outlined its future intentions to provide monetization opportunities for app makers and entrepreneurs who use the open source tools and initiatives like **FIWARE Lab** and the **forthcoming FIWARE Academy** may provide other opportunities for developers to identify viable business models, if needed.

3.3.5 Training Sessions

Action 5 ⇨ Training Sessions

Training sessions at ECFI Munich on 18 September 2014

The European Conference on the Future Internet (ECFI) in Munich from 17 to 18 September 2014 offers a dedicated training day for SMEs on 18 September. Within this training day at the Research Center Garching

of the Technical University Munich, the XIFI project will organise two introductory training sessions on the FI-WARE Open Ecosystem for SMEs.

The first introductory training session on 18 September from 10:00 to 12:00 aims particularly at SMEs and web-entrepreneurs who want to use the FI-WARE Open Ecosystem to run their experiments of Internet-based services and applications.

In this training session, SME representatives and web-entrepreneurs planning to submit a proposal in the open calls of the Future Internet PPP's third phase will get a better understanding of the FI-WARE Open Ecosystem, which will help them prepare a good proposal.

July 3, 2014 FI-PPP Day Trentino attracted SMEs and start-ups

Under the umbrella of the FI-PPP Liaison initiative, CREATE-NET and Engineering organized the first FI-PPP Day Trentino in Trento, Italy, on 4th June 2014. The FI-PPP Liaison initiative is an activity promoted by the EIT ICT Labs to cross-fertilize the FI-PPP ecosystem with the EIT ITC Labs ecosystems.

The purpose of this event was to inform SMEs and start-ups located in the Trentino region about the various opportunities for funding and innovation related to the FI-PPP Liaison initiative and the upcoming FI-PPP Phase III accelerators. The event provided the opportunity for the FI-PPP to ensure the engagement of new players on local level in the Trentino region.

Around 50 participants took part in the event and received an introduction about the FI-PPP, FI-WARE and FIWARE Lab, the 5 accelerators with links with the Trentino region, and the FI-WARE Trentino Challenge.

The FI-WARE Trentino Challenge is a prize for 2 SMEs, sponsored by EIT ICT Labs, for the development of a solution based on FI-WARE technology and related to OpenData or IoT of value for the Trentino region. More details about the Open Call, which will close on the 16th July, can be found on the FI-WARE Trentino Challenge Website.

The FI-PPP Day Trentino was very lively, with many question by the participants related to access to the funding, ability to use the software beyond the end of FI-PPP programme, and commercial support of the offering. This has shown that there is still important work ahead to be done in ensuring a long-lasting road for the FI-PPP efforts, but also that the hype, the interest and concrete need exist, and the work the FI-PPP is pursuing is going in the right direction!

Further information, including videos, is available on the FI-PPP Day Trentino Website.

3.3.6 App Developers Feedback

Action 5 ⇨ App Developers Feedback

Foodloop - food & supply chain.

Customers (supermarkets) can automatically commercialize high-quality fresh products, in real time and with lower prices as expiration dates approach so they can avoid waste and reduce costs. Consumers get offers directly to their mobile phones and the FoodLoop entrepreneurs maximize sales revenue through generating additional reach through cross-channel marketing, while minimizing the loss of perishable

products, and provide more affordable fresh food by offering discounts, special offers, clearance sales, all linked to the ERP of the individual store availability.

The designers of FoodLoop: "We made use of the Cosmos & memory database Generic Enabler that enabled us to analyze and filter the data in real-time and process it automatically. Basically a huge amount of files needs to be filtered in order to assign the right products to the people based on their location and product interest. Watch Food Loop's CEO Christoph Müller-Dechent talks about his start up and their experience with FIWARE and FIWARE Lab.

SmarTaxi - FIWARE technology analyzed by the developer

SmarTaxi collects data about the location and condition of a vehicle in real time. The data is stored, processed and reaches the driver through Internet. This way the driver is able to access and view a "heat map" with colors that indicate areas of greatest concentration of potential customers. The only requirement is that the driver has a smartphone or tablet with Internet connection.

From a developers point of view the transition to use FIWARE technology went smoothly. Using the Object Storage Generic Enabler (instead of Amazon S3) enabled them to store all the processed data in one platform so it's easy to access for the clients.

Additionally the Generic Enablers are ready to use, which allows us to focus on the product

4 European ICT Industry towards a Digital Single Market

Today, Information and Communication Technologies (ICT) are the driving force of economic globalisation and change in societies. ICT can drive productivity and growth in all sectors of the economy, companies large and small, in particular by improving access to markets, reducing costs and promoting cross-industry innovation, and is essential to the modernisation of public administration. Europe needs to keep up with global competitors such as the US, Japan and South Korea, which are rapidly expanding the digitalisation of their economies. Effective use of ICT is central to labour productivity and the EU's international competitiveness

However, the EU is losing ground in almost every segment of the ICT industry. The Digital Single Market should be a clear political priority. Highly fragmented markets hamper the capacity of private sector investment in high-speed fixed and mobile networks. Market consolidation is needed to invest in new and state-of-the art communication and broadband infrastructure which is capital intensive. Innovative digital services, such as cloud computing, also require a Single Market to ensure their cost-effective development and uptake.

- **Increase investments in digital infrastructure through a roadmap for deregulation of the telecom** sector, facilitation of market consolidation and the creation of a genuine telecommunications Single Market.
- **Adopt a Single Market approach to digital services, including cloud-based services**, to ensure the cost-effective development and uptake of innovative services.
- **Establish an appropriate and consistent EU Data protection framework that reduces administrative burdens related to the management of personal data**, and achieves both better protection and free movement of data within the EU.
- **Ensure cyber-security of critical infrastructures and digital services to establish the trust needed** for the development and uptake of new connected technologies.

As the European Union prepares its plan for a Digital Single Market, policy-makers must take full account of the fastest growing segment of that market – the app industry**. In fact, currently the heterogeneity of legislation across Europe covering security, privacy, trust, and digital rights is a barrier to entry for ICT SME.**

Recently the **App Developers Alliance published a paper detailing the challenges** app developers face when releasing a new app in Europe – reminding us that **the app ecosystem stands to gain a lot from smart policy-making. What do app-makers need from policy-makers? :**

- First and foremost, **app-makers need a real digital single market.** Unlike competitors in the US and India in particular, European app-makers face a series of hurdles to distribute across our internal market: **language barriers, outdated rules on copyright, lack of open data access, and fragmented approaches to data protection and e-Commerce to name a few.**
- **Second, policymakers must embrace the view that our European economy is digital.** There is no longer a digital economy niche. Apps can be affected by every piece of sector-specific legislation from medical device rules to payments laws, and must be part of those policy developments.

Apps, by their very nature, work across borders, networks and devices and thus contribute to a single market. To support continued growth of the apps ecosystem and the role of apps in relation to the European single market consumers must be able to access and use apps (i.e. apps must not be subject to blocking or anti-competitive discrimination).

Europe needs to reform and forge a true digital single market. This will give European entrepreneurs, who have all the right building blocks, the **incentive to invest and the ability to achieve global scale** at greater speed. Significant political will needs to be mustered to support these changes and **ensure Europe's startups succeed.**

- The industry, research and energy (ITRE) committee's position has been very clear. **The EU needs to move decisively towards a truly integrated European digital market**.
- **Parliament believes it is time to build a connected single market based on ambitious legislation.** We must set up a framework that will allow Europe to stay up to date with the latest technological advancements, as well as market and social developments. We need a long-term strategy that will bring immediate solutions to abolishing roaming fees, boosting further expansion of cloud computing, popularizing borderless mobile data connectivity and simplifying access to information and content. At the same time, we must guarantee net neutrality and full personal data protection for European citizens - especially as TTIP negotiations with the US progress.
- **Building a digital agenda for Europe is certainly not an easy task**, but the commissioners in charge have proven their commitment to the fight against a fragmented Europe

In today's fast-moving world of technology, with converged media and communication services and increasingly innovative offers from a myriad of new players mean that **many rules, and sometimes entire regulatory frameworks, need to be re-considere**d. In view of this, we particularly welcome the emphasis given by the new **European Commission to "better regulation", and to its re-fit exercise for current legislative measures**

- **The ongoing review of the EU Data Protection legal framework** is a unique opportunity to achieve a true level playing field in order to ensure that technologically neutral principles apply to all stakeholders. This is also a key consideration for the debate around the EU Digital Single Market and the need for increased competitiveness. In today's converged world, the distortions between sectors are not justifiable and this particular example of asymmetry needs to be addressed without delay.
- **It is a very interesting period, with a Commission that takes office by setting itself a very clear and ambitious agenda.** It finally gives a central role to digital in its global strategy and is determined to act quickly. This is important because current EU legislation dates back 20 years. It was created at a time when the telecoms industry was dominated by monopolies. The context must now evolve and I believe there is a realization that it is not just marginal adjustments that are required but an in-depth review.
- **As an example, one area of work will be about building trust and confidence.** Both of these are vital if a Digital Single Market is to exist in Europe and function properly. Everyone needs to be at ease about problem-free accessing of services across borders, and as much at ease about doing this online as they are offline. In policy terms, this means moving further on consumer rights, data protection and cyber-security: a very wide range of cross-cutting issues.

Another relates to removing restrictions (and preventing new ones) and particularly to stop blocking of online consumers based on their location or residence. This will be about **reforming copyright rules and getting rid of unjustified curbs on transfer and access to digital assets.**

The digital market not only changes what is being sold and bought, but also the business doing the selling. Hal Varian, chief economist at Google, has coined the term Micro Multinationals to describe small businesses acting on multinational markets. Historically, a company's market has been strongly correlated to its size, meaning that in order to reach new markets the company had to grow and expand. This is not necessarily so anymore. In a digital market, **a small business providing a niche product can access several national markets right from the start.** In fact, it might be necessary for its business model to do so. **Other businesses are entirely digital**, providing social network services, online games or even digital clothes for a digital avatar in a game or online community. A lot has happened since the internet started spreading in 1995. Yet, there are many questions posed by policy makers, academics and business leaders in the second half of the 1990'sthat still remain unanswered. **As the EU intensifies its efforts to establish a Digital Single Market (DSM),** it will be necessary to address and to provide answers to many of these questions

- How do legal systems need to be reformed and harmonized to **apply to cross-border commerce in a single digital market**?
- Does it matter if we are online or offline - can we even tell the difference anymore?
- Should we be able to access the same online content even when we are abroad?

The Digital Agenda is one of the flagship initiatives of the EU 2020 strategy to create growth and jobs in Europe. One of the top **priorities in the strategy is the creation of a digital single market**, whereby **barriers between Member States in the digital area are reduced or removed.**

The issues described in this chapter are believed to be fundamental to furthering a digital single market. Therefore, the priority topics discussed in the next table should be understood in terms of how they can act as drivers to promote wider change and development.

Barrier/ Issue	Issue Background	Policy Approach
Trust	**Trust is a fundamental building block of any market**. However, trust in the digital market is not a policy issue in itself. **In a cross-border context this introduces new challenges when it comes to identification and authentication online**. For instance, most electronic identifications are associated with nationality, sometimes rendering them confusing or insufficient to build trust between consumers in one country and producers in another country. The lack of common coordination of rules and institutions for trade creates and feeds a common uncertainty. **This is a prominent barrier to a digital single market.**	• Harmonize consumer laws and rights. • Coordinate and harmonize the legal framework and incentive models to promote trust services across Europe. For instance, use open, international standards for securely validating e-signatures and e-certificates.
Privacy and Data Protection	**Data privacy rules have a wide range of implications on actors in the digital market place**. First of all, variations in data privacy and **data protection regulation may have effects on how users can access content and services in different countries,** which in turn has effects on businesses' ability to access new markets. The more regulation differs between two countries, the more a specific data-based service will need to be adapted in	• Harmonize data protection and privacy regulation. • Investigate and structure the meaning and demarcation of privacy and the relation between personal data and data about a person.

	order to access both markets. This might also limit synergies and combinations between different data sets and/or users in different countries. Hence differences in **data privacy regulation might risk reinforcing national borders in the digital market place** Furthermore, it is important to **distinguish between an individual's personal data** (information the individual supplies about herself) and **personal information about an individual** (information that others have about the individual or information that is produced as a residue when that individual uses online services, metadata). Harmonized rules and implementation of rules for using, protecting, sharing and deleting data – personal and otherwise –is **believed to promote a better cross-border environment for digital innovations**.	• Adopt open international standards for information security management systems (ISMS) and technical penetration testing in order to harmonize a best practice in information security within Europe. • Investigate what rules and regulations would be affected by the above definition and how to best harmonize them
Public Sector Information and Open Data	Information is a basic resource and an increasingly valuable asset in the digital economy. The public sector has terabytes of it but it is far from always readily available to the public. The European Commission has issued a directive to promote the **re-use of public sector information (PSI) to spur innovation and firm growth**. However, different countries have implemented the PSI-directive in their own different manners, creating a need such data. For this reason, public sector information and open data initiatives should be coordinated with public procurement and in particular innovation-driven procurement. In the latest update of the EU's PSI-directive, it is stated that **public sector information should be made available at no charge or at a marginal cost**. Also, differing rules and frameworks for accessing public data in different countries fragments the market for this data in at least two apparent ways. - First, it is harder to gather data from different countries is regulations and procedures are not the same. - Second, it is more complicated to provide services across borders when different regulations apply to access and use of data in the different countries. - One major issue with public sector information is that it is associated with high barriers to entry. o First, an entrepreneur will need to identify the data she requires and the responsible authority that can provide access to it. o Second, she will have to ask the authority for the data, which often requires the	• Coordinate and benchmark initiatives both regionally, nationally and transnationally to publish public sector information and to work with open data. For instance, focus on shortening response times for inquires for data and improving visualization of available data to raise awareness. • Harmonize the implementation of the EU's PSI-directive and the marginal-cost charges in Europe • Set a plan to increase the scope and amount of data being made available beyond the minimum limits of the PSI-directive. Set a series of deadline and progressively increase the amount of open data. • Establish a European licensing market to enable the cross-border use of data regulated by licenses. • Establish profile test cases for Europe to work with and promote the reuse of public sector information.

	authority to make its own investigation into the possibility of providing access to the data. **This might incur a cost for the entrepreneur**, but it will not guarantee her access to the data. If the responsible authority decides to provide the data in question to the entrepreneur, this is by no means a guarantee that the same data will be more readily available to next entrepreneur asking for it	Suggested areas to prioritize are geographical information systems (GIS), tourism, building permission procedures, city planning and school performance data
Interoperability and Standards	Interoperability and standards coordinate the underlying technology of the digital market place in much the same way as harmonization of consumer rules coordinate actors in that market. **There are several levels to the impact of standards and interoperability in the digital market**. Standardization in business areas such as e-health and e-government are **believed to enable and increase cross-border innovation within Europe**. This is also closely connected to the **need for open standards**. **Proprietary standards risk creating barriers to entry and lock-in effects**, making it harder for new businesses and actors to innovate and compete based on the current technology platforms. Part of the potential in a digital market is to create an even better, even more efficient digital market and evolve the market place itself.	• Coordinate the use of open, international standards for technology and information in the public sector between the countries in the region. Identify priority or pilot areas to promote interoperability in, for instance health, transportation or energy. • Promote open standards in public procurement to promote flexibility, maintain low barriers to entry and stimulate innovation based on the current technology platform. • Identify future standards and future expected requirements and standards and make the information freely available to promote innovation and adaption ahead of time.
Digital Content and Copyright	The use and flow of digital content is crucial to the information economy, but it is also one of **the most prominent sources of friction in the digital market.** Due to **different licenses and differences in copyright legislation,** it may turn out to be cumbersome to provide digital content across borders and in new markets It is not evident that it is sufficient to harmonize copyright simply by including all the specific regulations from each legal system into one set of rules. To sum up, this calls **for an EU-wide copyright reform**. A first crucial step would be to **harmonize licensing for copyrighted material so that it is associated to a person or device**	• Investigate how the terms of copyright can be adapted to the digital market in Europe (terms and length of protection and the structure of licensing agreements for instance). • Harmonize licensing procedures and agreements within Europe

	and is not geographically limited. Thereby, access to **copyrighted material would not be constrained by the national borders within Europe.** This would in turn increase the potential for businesses to provide border-crossing content services.	• Harmonize copyright between the countries in Europe with regard to optimizing innovation of new digital services and products as well as promoting the digital market in general. This needs to be a part of a larger EU-wide initiative.
Cybercrime and Security	**Combating Cybercrime is considered important in order to build and maintain consumer trust.** Cybercrime also incurs costs for consumers and businesses who feel the need to protect themselves. It is evident that **cybercrime causes overall barriers-to-entry in the digital market** Many of the issues associated with cybercrime can be broadly approached within information security and information security management systems (ISMS). Such approaches should aim at establishing and **implementing international, open standards and requirements** rather than having each member state implementing its own nation-specific set of standards and rules.	• Map the intensity and origin of cybercrime in order to estimate the regional nature of the problem. There is already a lot of mapping of cybercrime, making it easy to compare and to benchmark issues, priorities and solutions. • Promote open international standards for information security and information security management systems (ISMS). • Coordinate law enforcement to battle cybercrime that originates within Europe

Table 2 Main Regulatory issues for the Digital Single Market

The scope of the reforms expanded rapidly following the scandal surrounding the US cyber espionage programme, Prism. The American National Security Agency (NSA) was receiving information from large internet companies about their European customers.

If trust is not rebuilt, businesses will not be able to develop the huge potential of the digital economy. The European Court had to step in and take a stance **because Europe lacks modern data protection rules that are fit for the Internet age.** The Heads of State and Government have repeatedly affirmed the importance of adopting 'a strong EU General Data Protection framework by 2015'.

- **Europe is readying implementation of data protection reforms** aimed at harmonising data privacy and security laws for all 28 member states.
- **Given the inherently borderless nature of cloud computing**, it's more important than ever to ensure robust legal frameworks and critically, bodies capable of enforcing appropriate data management through fines and other measures

The legislative package containing one directive and one regulation, proposed in January 2012, was adopted at first reading in the European Parliament in March 2014, just before the European elections. It

includes measures to protect European citizens' data and to restrict its use by businesses and intelligence services.

- **Requests from administrative or judicial authorities from third countries for access to the personal data** of European citizens held by European companies would be subjected to prior checks by the member states' national data protection authorities.
- This would force **Google, Facebook and others to seek the blessing of the relevant national authorities** before sending their users' details abroad.

Additionally, Andrus Ansip, European Commission Vice President responsible for the Digital Single Market, has suggested that Europe's rules on **copyright need** to be updated to make them fit for the digital age, describing copyright as a restriction holding back the full development of the Digital Single Market.

Europe needs to develop a truly connected digital single market, including through swift and ambitious legislative steps in the areas of data protection, telecoms regulation and by modernising and simplifying copyright and consumer rules for online and digital purchases. **The digital single market should address trust and security of online transactions,** interoperability of different technological solutions and access to digital resources and infrastructures (in particular spectrum licencing policies). **The Single Market should be open for new business models, while ensuring that essential public interest objectives are met**. Consumers should be given unhindered access to online content and services across Europe without discrimination based on their nationality or their place of residence.

5 THE EUROPEAN POLICY OPPORTUNITY

The speed of growth from the App Economy and the breadth and depth of wider economic and social benefits in Europe, as well as European competitiveness, **will depend on the policy environment in Europe**. Europe has **a strong base to build on in terms of an established ecosystem of apps developers**, comparatively high levels of smart device take-up, high household penetration of Wi-Fi and an accelerating transition to LTE. However, to realize the full benefits, and to become global leaders in the App Economy, **Europe will need to get the right and common regulatory framework in fast moving industry sectors.**

The plan of the Commission is to develop "a truly connected digital single market" in Europe through swift and ambitious legislative steps in the areas of data protection, telecoms regulation and by modernizing and simplifying copyright and consumer rules for online and digital purchases.

If Europe's single market becomes truly and thoroughly digital, the macroeconomic benefits would be enormous. **Europe's digital businesses no longer would have to get individual licenses to operate in 28 different countries**. If regulatory barriers are removed, startups could directly access half a billion European consumers, a market that's larger than the US, where technology companies have the ability to achieve scale before they expand internationally

Imagine if this vibrant European entrepreneurial scene could benefit from a digital single market, which would end the need for obtaining different national licenses and reduce regulatory red tape. High-growth firms and technology-intensive startups suddenly could scale-up and **compete more vigorously in the global marketplace.**

5.1 Developer Access to European Government data sets

Data held by European governments can support the development of innovative apps that increase the value of such data for citizens and potentially reduce the cost of government service provision. Examples include **mapping, meteorological and real time public transport data, as well as information on schools, education and other community-level services**

Making data available in Europe has a number of benefits:

- App developers have technical expertise and are better placed than governments or public agencies to provide innovative services based on government data.
- Apps extend the ways in which data can be used, and ensure it is available in an appropriate form on mobile devices.
- By making data available rather than putting resources into developing information services, governments may reduce costs while also enhancing service.

To deliver on this vision the following are required:

- Access to government data in a machine readable format with appropriate application programming interfaces (APIs)
- Free non-exclusive access to encourage innovation and competition

Several initiatives to make government information available have been established, notably in the US and some European countries. These initiatives need to be accelerated and extended throughout Europe.

5.2 Completing the European Single Market

Europe has always excelled at innovation. Radio, television, and the standard for second-generation mobile communications, GSM, all are originated in Europe. But past success won't ensure Europe's long tradition of innovation continues. New technologies require more risk-taking and the ability to launch new products with speed and scale. There is no doubt that Europe is poised to embrace the new, digital world but at the same time, **Europe needs to reform and forge a true digital single market** for pan-European Big Data Value services and Applications, based on the following:

- Apps work across borders, networks and devices and thus contribute to a single market.
- Apps open up new markets, compete with existing services, drive innovation and widen choice for consumers and enterprises.
- European and national regulations will have been adapted to the needs of the data-driven economy and society.
    - A modern, **robust and flexible intellectual property rights framework** for handling complex issues related to ownership and licensing in combination with standards and knowledge based approaches will have **facilitated the interoperability and the exchange of data across Europe.**
    - A truly modernized legal framework will have been provided for a **high level of data protection** while leaving sufficient flexibility to business and innovation.

This will give European entrepreneurs, who have all the right building blocks, **the incentive to invest and the ability to achieve global scale at greater speed**. Significant political will needs to be mustered to support these changes and **ensure Europe's startups succeed.**

5.3 Embracing Innovation throughout the EU Economy

Regulation should be appropriate, thoughtful and, above all, **supportive of app-enabled innovation**. Regulations should be reappraised and adapted, sector by sector, to ensure that individuals, firms and **society can benefit from app-driven innovation in every sector and industry**.

Europe has an opportunity in these and other areas to adopt appropriate frameworks that jump start the App Economy. Where regulations may be required (e.g. for health and safety reasons), a multi stakeholder co-regulatory approach should be preferred to ensure that the development of new innovative uses is not hindered.

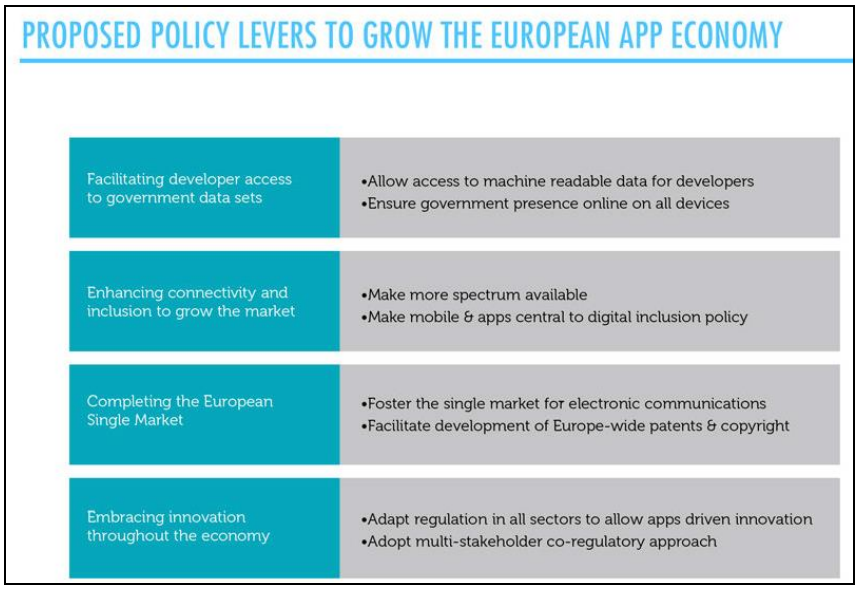

Figure 4: Proposed Policy levers to grow the European App Economy. Plum Consulting.

5.4 Contributing to the European Digital agenda

The Digital Agenda for Europe includes seven policy pillars aimed at enhancing the role of the digital economy in Europe and helping achieve the Lisbon agenda for growth and jobs. Below we illustrate ways in **which the apps ecosystem is contributing to the seven pillars**, and the ways in which delivering the seven pillars can stimulate the apps ecosystem

App Economy Contribution to the Seven Pillars of the European Digital Agenda

Seven pillars	How apps contribute
Digital Single Market	Apps have contributed to the single market, in particular communications apps. A single market for intellectual property including patents and copyright would stimulate apps development.
Interoperability & Standards	Apps improve interoperability since they work across different devices and forms of connectivity. Standards, including APIs for access to government data, would foster development of new kinds of apps.
Trust & Security	Curated app stores contribute to trust and security for consumers. Appropriate measures to promote trust and security could foster new areas for app development including mobile payments.
Fast and ultra-fast Internet access	Apps are driving consumer demand for ubiquitous high speed, high capacity networks. Fast wireless access would stimulate development and use of connected apps and cloud computing.
Research and innovation	Apps support the crowdsourcing of data, citizen science and collaborative research and innovation. Research and innovation in areas including 5G, big data and 'AI' will stimulate apps development.
Enhancing digital literacy, skills and inclusion	Apps solve the problem of relevance and reduce skill barriers to digital literacy, while helping overcome barriers due to disability. Getting more people online will enlarge the market for apps.
ICT-enabled benefits for EU society	Apps development and use is driving a new wave of innovation, growth and jobs for EU society.

Figure 5: App Economy Contribution to the Seven Pillars of the European Digital Agenda. Plum Consulting

One of the areas of high importance in the Digital Agenda is cloud computing. The Digital Agenda aims to promote the right conditions for citizens and businesses to benefit from this. An online consultation has been running in 2011 and feeds the European Cloud Computing Strategy (2012). The survey also seeks **feedback on policy issues such as data protection and liability (in particular in cross-border situations**), legal and technical barriers, standardization and interoperability solutions, uptake of cloud services. The recently published **Cloud strategy includes three key actions: standards, contract terms and conditions**, and European Cloud partnership as well as a number of flanking actions.

- In case of **virtual network provision** or **cloud computing**, routing of connections (and related backup connections) may be subject to legal restrictions concerning traversal of areas under different laws (with respect to, for example, privacy, digital rights management, lawful interception, public emergency handling).
- Another topic regarding **cloud computing includes the risks and benefits of virtual access to information. Stricter privacy requirements that favour local-only storage of data** may be an additional obstacle to the current approach**,** as it would place data even further away from the computational infrastructure.

Trust and consequentially security concerns are one of the top obstacles that hinder Cloud Computing adoption today

5.5 Policy and Regulatory challenges for Future Internet

The Future Internet gives rise to a wide range of new challenges regarding policy, regulation and governance. Making the Future Internet, to a success requires on the one hand the **removal of policy and regulatory bottlenecks** (for example those that hinder innovation), and on the other hand the creation of new policies and regulatory frameworks as well. Especially at the European level there is opportunity and need for **restructured policy and regulatory frameworks.**

Some of the challenges are highly domain-related (e.g. specific Future Internet-related policies and regulations for sectors like media, logistic supply chains, energy or health). **Other challenges are more horizontal and generic**. These horizontal challenges are still quite diverse. They include **security and privacy issues, availability and access to network infrastructure** and to critical parts of the infrastructure, the functioning of **entrepreneurship and innovation ecosystems** etc.

Based on these envisaged Future Internet impacts the following **priorities have to be worked in the domain of policy and regulation.**

- **Policy and regulatory issues**: Emerging frameworks for policy and regulatory conditions such as interoperability, openness, standards, security and privacy
    - **Europe is, however, lagging behind other regions in the take-up of cloud computing**. Moreover, due to a lack of regulatory consistency and due to policies which are technologically conservative, cloud computing in Europe remains fragmented, at times making it difficult for European citizens and businesses to reap the full benefits that the cloud undeniably offers
    - In this **context, data ownership is a major concern that could provide serious gaps across European countries** depending how national regulation processes are supporting the deployment of new technologies. Additionally, data is stored, distributed and analyzed

globally rather than locally, with no clear jurisdiction or established regulatory framework to deal with any disputes

- Data stored in cloud-based systems are vulnerable for **privacy breach** e.g. tracking down individuals. **Establish rules that balance respect for data privacy** with flexibility to support innovation
- While there are already many public administrations offering Open Data, there are several obstacles that prevent a wide use of Open Data, such as poor data quality, privacy risks and deployment limitations. **Increase access to data held by public authorities and the private sector**
- **Ensure global data flows**: Creating a 'Fortress Europe' for data will limit the potential for growth and innovation. The European Union and the United States must redouble efforts to work out common standards for the handling of personal data that allow for the free exchange of data. These standards should cover open data and anonymisation, among other issues. **Step up efforts to agree common EU-US standards** for the handling of personal data.
- **Platform Neutrality**: issues of cross-platform interoperability, data portability, lock-in/lock-out for users, suppliers, competitors are quite parallel

- **Ensuring the impact of Future Internet and create the appropriate Ecosystem**: shaping SME involvement, entrepreneurship and incubation activities.
  - Develop approaches and **policies to stimulate web-entrepreneurs,** working with the web-entrepreneurship initiative
  - **The need for an EU regulatory framework**, which is able to mediate and find suitable legal **collaboration patterns between different stakeholders (and their countries),** while avoiding imposing too strict limitations to the characterizing modus operandi of the marketplace. In fact, it is likely that several issues that are typical of any marketplace (be it digital or in the physical world) would be subject to debate within the EU, in order to find **a viable policy that protects individual rights while encouraging the development of applications in the marketplace.**
  - Regarding the intellectual property there **are two European policy requirements** to address:
    - **Protection of the intellectual property of app developers** to ensure that they are prepared to invest in risky new ventures, and to foster an environment conducive to innovation, creativity and consumer trust.
    - **Copyright, trademarks and patents ought to apply throughout Europe on a common basis**. Application developers need ways of utilizing and paying for content rights throughout Europe without having to incur costs in agreeing rights on a country-by-country basis
  - **Additionally, a thriving startup ecosystem relies on easy access to capital**. Europe needs tax incentives and other proactive measures that make it easier for startups to get funding. Governments should think carefully about the balance between driving growth and taxing capital.

6 Analysis of Policy and Regulation Priorities for the development of Future Internet

Probably the most of relevance for FIWARE is **how to benefit from convergence and at the same time ensure that competition** is fostered increasing the transparency of bundled offers and avoiding customer lock-in and abuse of market power by large operators. A key issue to study here is the ability of end-users to access and distribute information or run applications and services of their choice, to **preserve the openness of the Internet as platform**.

Furthermore, Intellectual property protection and data protection are still largely fragmented. On this aspect, the European Union is trying to act swiftly to avoid fragmentation, but the current situation still creates significant uncertainty for market players, especially as **concerns copyright licensing and patent litigation** and due to the absence of mutually **recognized rules on online data protection** is a potential obstacle for the development of cross border applications. Regarding the use of **Open Data in Smart Cities**, there are **many risks around it and their potential use and this is a specific regulation** issue for the European Commission providing European guidelines and common understanding on what are Open Data and best practices to use them, including privacy aspects

The FIWARE project recognizes these concerns and the involvement of European citizens, policy makers, municipalities and other communities (SMEs, entrepreneurs) in the platform experiments will be crucial. Access to **Open Data will be one of its main attractive aspects** and existing cross-border commercial offers do not include high level services which could be hosted in cloud **because of the heterogeneity between European regulation systems and data privacy rules**. A more robust regulatory regime delineating how data is handled and released is needed. **European cloud strategy should come with common data privacy and management regulation**. In addition to the debate regarding digital privacy legislation, the European Commission created the **European Cloud Partnership last year as part of a broader strategy to promote cloud computing**. It is important that privacy and data protection issues are part of it.

The need to support an efficient EU wide single market for cloud services, based on best practices, a common understanding of regulatory requirements and the most effective way of meeting the needs of specific cloud use cases. Achieving this goal requires actions from a variety of stakeholders, including the **elimination of regulatory and market access barriers at both national and EU level**, but also the identification and promotion of best practices by industry in respect of applicable laws, technical standardization and operational assurances.

Thanks to the open nature of FIWARE specifications, cities and other adopters will be able to **avoid vendor lock-in.** Indeed, FIWARE developers. They will be able to port their applications across different instances of the FIWARE platform, supported by different FIWARE providers. **Decisions to choose a given FIWARE provider will be driven, not only based on costs, but also trust**, e.g. regarding the environment where applications or where data will be hosted. This is particularly relevant when data (e.g. those affecting personal information) have to comply with certain regulations or has to cope with some security and privacy requirements.

The Future Internet gives rise to a wide range of new challenges regarding policy, regulation and governance. Making FIWARE, to a success requires on the one hand the **removal of policy and regulatory bottlenecks** (for example those that hinder innovation), and on the other hand **the creation of new policies and regulatory frameworks as well**. Especially at the European level there is opportunity and need for restructured policy and regulatory frameworks.

Europe has a comprehensive set on regulation that is not yet fully tuned towards the developments of Big Data. Yet discussions are under way to update regulations such as for "data protection" and "access to public data".

- **The General Data Protection Regulation proposal - currently under negotiation - aims to address important privacy aspects stemming out from latest technology developments** (including social media and cloud computing), and provide for harmonization of regulations throughout the EU.
- **Advancements in the area of "access to public data" will include amongst others the creation of a genuine right to re-use public information** (libraries, museums and archives and making data available in machine-readable and open formats

The emergence of multi-sided platforms implies that **policy makers and regulators should not take for granted that simply allowing and facilitating the convergence** between IT, internet, telecommunications and media services and technologies will result in an unbundled, open marketplace in which competition will flourish (Ballon, 2009a). The rise of platforms in ICT markets that invites to **a reappraisal of regulatory frameworks and practices**. Besides inter-organizational collective action, formal law regulations and policies from government and/or regulatory authorities play an important role in enabling the vision of common service platforms.

- One relevant issue in this domain is that **sharing distributed service resources** (i.e. network infrastructure, service platform and devices) may not be in the interest of all involved actors only if there is strong added value or perhaps enforcement from market competition or regulations.
- Moreover, there is a lack of interest from actors to solve **the problem of interoperability** mainly because of related costs, complexity, and reliability or competition concerns.

Under the new Digital Agenda (2010), Europe appears to move further towards regulating platforms in general, i.e. the access to platforms, **the interoperability between platforms**, and so on. New European **interoperability rules** foreseen for the electronic communications industry, **based on antitrust rules related to the abuse of market position, referring to a significant position**. In this case, obligations will be imposed related to licensee interoperability information, **to ensure consumer choice in software as well as hardware**

6.1 Cloud Computing: A Trusted European Cloud

Europe is, however, lagging behind other regions in the take-up of cloud computing. Recent revelations about intelligence services surveillance of **data have the potential to harm trust in cloud-based solutions**. Moreover, due to a lack of regulatory consistency and due to policies which are technologically conservative, cloud computing in Europe remains fragmented, at times making it difficult for European citizens and businesses to reap the full benefits that the cloud undeniably offers

Existing cross-border commercial offers do not include high level services which could be hosted in cloud because of the **heterogeneity between European regulation systems and data privacy rules**. A more robust regulatory regime delineating how data is handled and released is needed. European cloud strategy should come with common data privacy and management regulation. **In addition to the debate regarding digital privacy legislation, the European Commission created the European Cloud Partnership** last year as part of a broader strategy to promote cloud computing. It is important that privacy and data protection issues are part of it.

The need to support an efficient EU wide single market for cloud services, based on best practices, a common understanding of regulatory requirements and the most effective way of meeting the needs of

specific cloud use cases. Achieving this goal requires actions from a variety of stakeholders, including the elimination of regulatory and market access barriers at both national and EU level, but also the identification and promotion of best practices by industry in respect of applicable laws, technical standardization and operational assurances. In this way, a single market for cloud services will be supported, generating benefits for all European stakeholders:

- **On the demand side, European cloud users** (citizens, businesses including SMEs and public administrations) will be able to choose and use cloud services with confidence, knowing that they adhere to European legal norms and international standards, and that data in such clouds is secure.
- **On the supply side, cloud providers** will be able provide their cloud services to European customers, without hindrance from national regulatory barriers

The European cloud market is currently confronted with a significant number of regulatory and market access barriers that impede both development **and commercial exploitation by cloud providers and adoption by cloud users, especially for cross border use cases.** Some of these regulatory and market access barriers are linked to legal issues, whereas others are principally tied to trust concerns, technical control, or operational requirements.

- Privileged information can be protected by legal frameworks that stop cloud adoption or limit use cases. Significant benefits could be realized through **trusted cloud solutions**.
- The **lack of full EU harmonization of data protection** rules is a recurring legal barrier.
- Even outside of formal laws, norms may exist (issued by supervisors, regulators, sector organizations etc.) which stop or **discourage the use of cloud services outside national borders**.
- **Cloud adoption barriers can vary from sector to sector**. Legacy legal frameworks that are not adapted to the global market can cause legal challenges, and operational/business concerns may lead to a strong preference for private clouds

From a European perspective, there is the dual risk that excessively restrictive regulations can place European cloud service providers at a clear competitive disadvantage in relation to their non-European counterparts, and inversely that overly flexible rules could result in serious harm to end users. Ambiguities in the law should at any rate be identified and addressed to ensure that the legal status of cloud computing services and the rights and obligations of each of the stakeholders is clear, especially when **dealing with security and privacy concerns**.

Existing cross-border commercial offers do not include high level services which could be hosted in cloud because of the **heterogeneity between European regulation systems and data privacy rules.** A more robust regulatory regime delineating how data is handled and released is needed. **European cloud strategy should come with common data privacy and management regulation**.

Additionally, **Trust and consequentially security concerns** are one of the top obstacles that hinder Cloud Computing adoption today. **In this post Snowden era**, **cloud environments are under particular scrutiny** and governments are seeking a new balance between privacy protections – wherever data is located – and powers of data access to secure homeland defence. Europe is rising to the challenge, with initiatives to both reassure citizens and create conditions for a secure and **successful future cloud industry**

Cyber-security, data sovereignty and consistent procurement processes are among the issues holding back wider adoption of cloud computing and services, according to a survey on the Trusted Cloud Europe. This is linked to implementation of the **European Cybersecurity Strategy and issues such as identity and access management,** certification, research and innovation, and SME needs.

The **Trusted Cloud Europe framework aims to support a single market for cloud computing in Europe based** on a common understanding of best practices which will enable Europe to become a trusted leader in cloud computing, as both a provider and user of cloud services. **Specific recommendations** directed by the Board towards different stakeholders (i.e. Member States, industry, the Commission) include:

- Creation of **a common framework of legal, operational and technical best practices**
- Review of **formal data location requirements** (that currently still divide cloud architectures up by national jurisdiction) with the aim of replacing them by functional requirements to ensure the same data accessibility and security
- **Encouraging public bodies to consider cloud computing** when procuring IT systems.

At an unprecedented pace, cloud computing has simultaneously transformed business and government, and created new security challenges. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Yet these advances have created new security vulnerabilities, including security issues whose full impact is still emerging. Among the most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers. Although shifting to cloud technologies exclusively is affordable and fast, doing so undermines important business-level security policies, processes, and best practices.

Cyber-security, data sovereignty and consistent procurement processes are among the issues holding back wider adoption of cloud computing and services, according to a survey on the Trusted Cloud Europe.

The Trusted Cloud Europe framework aims to support a single market for cloud computing in Europe based on a common understanding of best practices which will enable Europe to become **a trusted leader in cloud computing, as both a provider and user of cloud services**

6.2 Big Data: One step closer to Europe's future privacy rules let it be a win-win for citizens and businesses

Nowadays a huge amount of data is collected, sometimes without a defined outcome of quantifiable value for either consumers or businesses. **The Internet of Things concept, leveraging data gathered by sensors** embedded in countless devices, potentially enhances the richness of information that can be generated from transactional platforms. These different sources of data are being processed more easily with the **emergence of Big Data Management and new data analytics technologies**, increasing the probability of finding meaningful insights from huge amounts of data generated by myriad applications and sensors.

The abundance, pervasiveness and reproducibility of data will intensify the **debate on data ownership and usage, data protection and privacy, security, liability, cybercrime, Intellectual Property Rights (IPR) and the impact of insolvencies on data rights**. Legal regimes are challenged by these developments on many levels with an effect on civil and criminal as well as European and international laws. In order to keep pace with these cutting-edge changes, **legislators have to become active and adapt the respective laws and legal practices to a new data-driven global environment**.

In the next years, the collection, storage, analysis and usage of personal data will increase. This development will have an effect on all levels of society and influence many parts of our everyday life. However, **without trust in privacy policies of businesses and administrations as well as appropriate data protection rules in place**, benefits from using Big Data will be more difficult to materialize. **A legal**

framework is needed that provides for a high level of data protection for data suppliers and users while leaving sufficient flexibility to researchers and companies.

An increasing number of companies, established global players, SME's and start-ups build their **business models on using and selling data** in raw or augmented form, or even data analysis algorithms. New legal models need to be developed to identify, evaluate and protect ownership of the data itself and the intellectual property associated with it.

In this context, **data ownership is a major concern** that could provide serious **gaps across European countries depending how national regulation processes** are supporting the deployment of new technologies. Additionally, **data is stored, distributed and analyzed globally rather than locally,** with no clear jurisdiction or established regulatory framework to deal with any disputes. Some of the concerns in relation to use of data are the following:

- Access to business data. Key conditions of international trade are related to data. Regulatory approaches related to data (access, privacy, security) are different across countries, which affects companies doing business in such countries.
- Access to Open Data. There are many risks involved around Open Data and their potential use, and this may form a specific policy and regulation issue for both national policy actors and the European Commission providing European guidelines and common understanding on what are the opportunities and potential negative implications are, and to stimulate best practices regarding the use of Open Data including handling of privacy aspects.
- Data and privacy breach. Data stored in cloud-based systems are vulnerable for privacy breach e.g. tracking down individuals.
- Data quality. Quality of data is an issue, especially when data is generated by sensors and people are acting upon this data.

Work is to be done on developing changes in regulatory **frameworks regarding Data Protection ensuring a single set of rules applicable across the EU** and clear rules on when EU law applies to data controllers outside the EU. Here we see two main aspects.

- The first is the review of the EU data protection regulatory framework. The Data Protection Directive[1] is a European Union directive which regulates the processing of personal data within the European Union, with a view to enhancing individuals' confidence and strengthening their rights and the aim of harmonizing the current data protection laws in place across the EU member states. The fact that it is a "regulation" instead of a "directive" means it should be directly applicable to all EU member states without a need for national implementing legislation. Some of the aspects to take into account are:
    - A **clear definition of personal data** is imperative in order to distinguish personal and non-personal data.
    - Moreover, the inference of identity out of **aggregated data coming from different sources** has to be considered as well in the regulation (currently it is not).
    - The **international dimension** is also a very important one since users share data without taking into account national boundaries.

[1] Officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- Additionally, this **directive must be used or revised to include Internet of Things subject. The machine-to-machine (M2M)** market faces not only technical challenges in implementation and interoperability, but also business issues related to pricing, potential breach in user privacy and regulations in different countries. European Union should be flexible to avoid any breakthrough with regulation on this topic in Europe and in other areas around the world.
- The regulatory **framework should cope with the evolving market structure moving from a traditional regulatory framework to a more global one encompassing all ICT related players and services**

- The second addresses the review and update of the 2003 Directive on Re-Use of Public Sector Information (PSI). The update of the PSI Directive has the objective to achieve a Europe-wide consensus in making PSI readily available, which would help bridge the current gap between member states' levels of openness regarding non-personal data that is produced, stored, or harvested by the public sector.
    - **The envisaged PSI update requires European national governments to provide access to all PSI data** ranging from digital maps to weather data to traffic statistics at zero or marginal cost. Also new is the explicit inclusion of cultural institutions, such as museums, libraries, and archives. The expected effect of this new set of guidelines is also to stimulate economic development (EPSI platform, 2013).

For FIWARE this update is relevant in relation to the availability of Open Data across the different cities in which its platforms are being deployed. While there are already many public administrations offering Open Data, there are several obstacles that prevent a wide use of Open Data, such as poor data quality, privacy risks and deployment limitations

In this respect, **it is critical to design a European Data Environment,** capable of amplifying positive externalities and to minimize negative externalities. For this purpose, **individual privacy and public security concerns** must be addressed in order to **convince governments and societal actors to share data more openly,** not only in the public domain but sharing in a restricted manner with other governments or international entities.

So the European Union is soon to implement the **General Data Protection Regulation (GDPR),** which will bring **all 28 countries under a single regime of rules, and penalties for breach**. This is perhaps the greatest opportunity that cloud providers will have seen a chance **to deliver EU wide services under one single operations model.** The purpose of the GDPR is to provide a single law for data protection to cover the whole of the EU. As a Regulation, rather than a Directive, there will be one single set of rules regarding data protection and individual countries will not have the freedom to make choices. As soon as the regulation is passed, each of its provisions will become part of the national legal system of each EU Member State, "as is".

The GDPR will thus make it easier for both European and non-European companies to comply with data protection requirements. In addition to giving a common approach to privacy, unlike the existing Directive, the new Regulation covers both cloud computing and social media, and provides common levels of fines for breaches. It also covers all organisations operating in Europe irrespective of where the data is stored.

So the European Union is soon to implement the General Data Protection Regulation (GDPR), which will bring all 28 countries under a single regime of rules, and penalties for breach. This is perhaps the greatest opportunity that cloud providers will have seen – a chance to deliver EU-wide services under one single operations model.

The purpose of the GDPR is to provide a single law for data protection to cover the whole of the EU. As a Regulation, rather than a Directive, there will be one single set of rules regarding data protection and individual countries will not have the freedom to make choices. As soon as the regulation is passed, each of its provisions will become part of the national legal system of each EU Member State, "as is".

The GDPR will thus make it easier for both European and non-European companies to comply with data protection requirements. In addition to giving a common approach to privacy, unlike the existing Directive, the new Regulation covers both cloud computing and social media, and provides common levels of fines for breaches. It also covers all organisations operating in Europe irrespective of where the data is stored. As proposed, organisations will have to:

- Collect explicit consent to collect data from data subjects (the data subjects must 'opt-in') and facilitate the subject's wish to withdraw that consent
- Be able to delete all customer data at the request of the data subject, a provision known as "Right to Erasure", unless there is a legitimate reason for its retention
- Provide data subjects with a clear privacy policy
- On request, provide data subjects with a copy of their personal data in a format that can be transmitted electronically to another system
- Undertake an annual risk management/analysis, detailing both the risks identified for data breach/loss and steps taken to alleviate those risks
- Establish which is to be the Single Data Protection Authority (DPA) for the organisation. This may be in any member state (it is expected that the UK and Ireland will be most popular because of the use of English language)
- Appoint a lead authority Data Controller to be responsible for all processing operations across Europe
- For public bodies and organisations processing more than 5,000 data subjects, appoint a Data Protection Officer within 12 months of the Regulation being adopted
- Document fully any breach, and notify the appropriate authority 'without undue delay'. It is expected that the authority will decide whether the organisation should notify data subjects if any 'adverse impact' has been determined

In the Commission's proposal for a new General Data Protection Regulation, it said that **whenever a business relies on consent as a valid ground for processing personal data, that consent should be 'explicitly' given.** This would change the current position where consent only need be 'explicit' where a business wants to rely on it as a basis for processing sensitive personal data.

- **New European directives about Data protection and PSI to be approved in the next one to two years** display some uncertainties about the impact on the implementation of Big Data and Open Data initiatives in the public sector. **Specifically, Open Data is set to be a catalyst from the public sector** to the private sector to establish a powerful data industry.
- **Internet of Things** is a dedicated topic for vertical areas where dominant players impose their views and would not share data. In this context, data property is a major concern that could provide serious gaps across European countries depending how national regulation processes would support the deployment of new technologies
- **There are many bodies in public administration** (especially in those which are widely decentralized), so much energy is lost and will remain so until a common strategy is realized for reuse cross technology platforms.

6.3 Open Data: Government can serve as a catalyst for the use of Open data

The use of open data is a relatively recent phenomenon but, as with many technological advances, it is growing in relevance and prevalence in other words, it is becoming the "new normal." Yet while the **benefits of open data are significant, the success of open-data programs is not guaranteed**. For government to serve as an open-data provider, catalyst, user, and policy maker in an effective and sustainable way, it needs to have the right people, tools, and systems in place. **The importance of open data is evident in terms of revenue growth (for both private and public sector) as well as achieving cost savings while increasing transparency (mostly for public sector).**

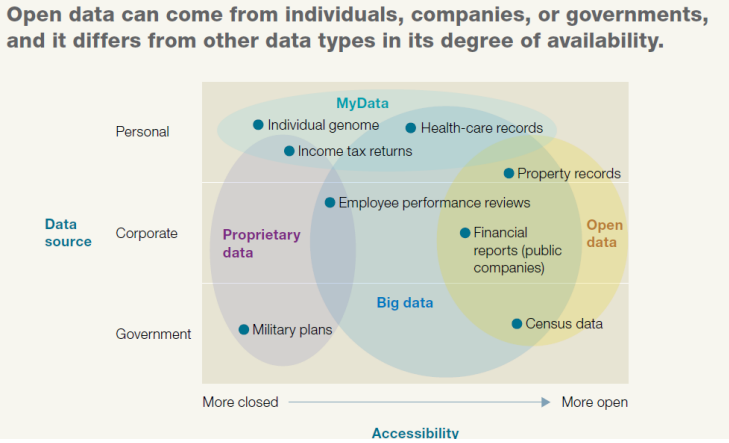

Figure 6: Open Data Sources. Source: Mckinsey

Open Data is a relatively new development but has received a lot of bottom-up as well as policy interest. Many initiatives have been launched by cities and national governments. The UK open data white paper stresses the importance of open data (e.g. geo-data, environmental data, and health-related data) for development of innovative products and services in a wide range of domains. However there still appear to be barriers and drivers of open data policy implementation (Huijboom and Van den Broek, 2011).

There are many risks involved around Open Data and their potential use, and this may form a specific policy and regulation issue for both national policy actors and the European Commission providing European guidelines and common understanding on what are the opportunities and potential negative implications are, and to stimulate best practices regarding the use of Open Data including handling of privacy aspects. While there are already many public administrations offering Open Data, there are several obstacles that prevent a wide use of Open Data, such as poor data quality, privacy risks and deployment limitations.

- **Open data:** Governments should take steps to ensure that data held by public authorities is made available as freely as possible and at minimum cost to users while ensuring that data privacy rules are respected. Companies should share the data they hold that can be used to develop new services for consumers.
    - Action point: Increase access to data held by public authorities and the private sector.
- **Trust and security:** Consumers' and citizens' confidence in how individuals' information is used and protected in the era of big data is essential if the digital economy is to grow. Governments must ensure

that fundamental principles of data privacy are respected while ensuring that rules are flexible enough to allow for innovation. Individuals will never understand the full complexity of the data ecosphere, so giving they control over their data through data vaults or privacy seals could play an important role in contributing to trust.

  - Action point: Establish rules that balance respect for data privacy with flexibility to support innovation

- **Ensure global data flows**: Creating a 'Fortress Europe' for data will limit the potential for growth and innovation. The European Union and the United States must redouble efforts to work out common standards for the handling of personal data that allow for the free exchange of data. These standards should cover open data and anonymisation, among other issues.

  - Action point: Step up efforts to agree common EU-US standards for the handling of personal data

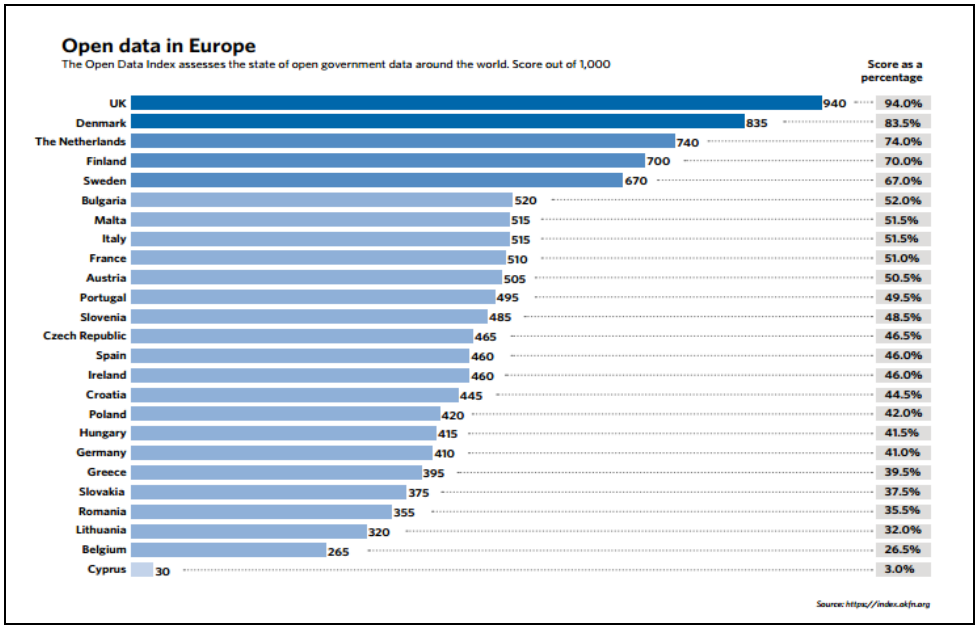

Figure 7: Open Data in Europe

Government can serve as an open-data provider, catalyst, user, and policy maker to create value and mitigate risks.

- **Provider.** Across all levels of government in all regions of the world, millions of individual data records are collected, stored, and analyzed. From tax returns and unemployment claims to hospital reimbursements and energy use, much of this information can be made available electronically and readily shared, enabling third parties to create innovative products and services. By making these data available to enterprising companies and individuals, government is spurring private-sector innovation and increasing transparency two of the most important goals of any open-data initiative. The 2013 G8 Open Data Charter establishes an expectation that all government data be published openly by default, while recognizing that there are legitimate reasons why some data cannot be released.

- **Catalyst.** Government can serve as a catalyst for the use of open data by creating a thriving ecosystem of data users, coders, and application developers. To attract an ecosystem of developers, it can

advertise open-data availability through press releases or other marketing materials, or even engage in individual outreach efforts.

- **User.** There are two key actions that government agencies can take to use open data. First, to optimize the use of public data within their own agencies. Second, governments can apply advanced analytics to improve internal decision making, promote the creation of new services, and increase accountability.. Governments around the world are taking similar steps to integrate data as the new standard for how their agencies operate.
- **Policy maker.** Public-sector leaders are often called on to protect individuals and organizations from the risks of open data while also advancing open data's potential value. Risks include those that fall largely on individuals, such as privacy, security, and personal safety, and those related primarily to organizations, such as confidentiality, liability, and intellectual property. Leaders can draw on their legislative authority and enforcement powers to enhance safety, security, equity, and justice for all members of society. They can also participate in setting technical standards that can significantly increase and scale the benefits of open data.

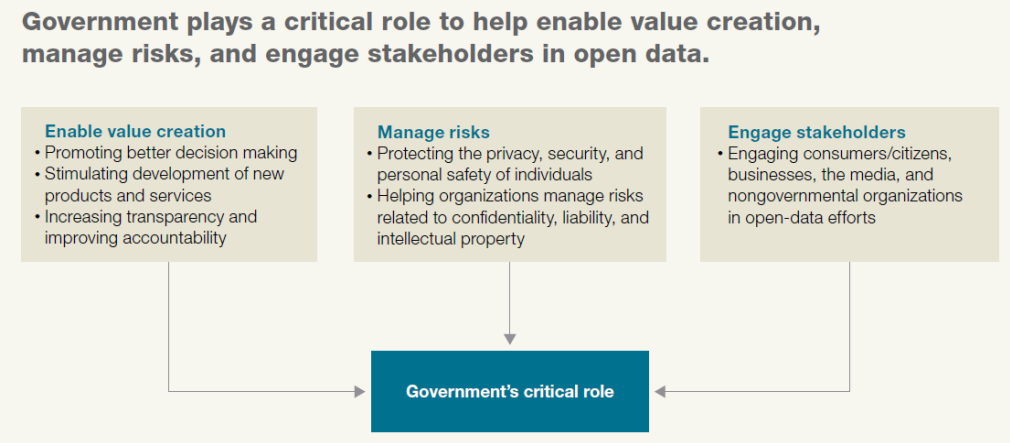

Figure 8: Government Critical Role in Open Data. Source: Mckinsey

In the **domain of Open Data the EC promotes standardisation via Public Sector Information** policies and via its leading role in the development of the European Open Data infrastructure.

- **Directive 2003/98/EC on the re-use of public sector information** (as amended by Directive 2013/37/EU) requests Member States to provide their data preferably in machine-readable formats and, amongst others, encourages the use of standard licences.
- **For the EU Open Data Portal** (http://open-data.europa.eu/en/data/), certain (de facto) standards are recommended (although not prescribed), e.g. concerning data formats (such as the W3C Recommendation RDF), as well as the use of controlled vocabularies. Standardisation efforts will further be promoted in the Pan-European Open Data Portal deployed in the period 2015-2020 as one of the Digital Service Infrastructures under the Connecting Europe Facility programme.

6.4 Security: European Cybersecurity Strategy

At an unprecedented pace, cloud computing has simultaneously transformed business and government, and created new security challenges. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Yet these advances have created new security vulnerabilities, including security issues whose full impact is still emerging. Among the most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers. Although shifting to cloud technologies exclusively is affordable and fast, doing so undermines important business-level security policies, processes, and best practices. **In the absence of these standards, businesses are vulnerable to security breaches** that can quickly erase any gains made by the switch to SaaS. Recognizing both the promise of cloud computing, and the risks associated with it**, the Cloud Security Alliance (CSA)** has pioneered the **creation of industry-wide standards for effective cloud security**. Already, many businesses, organizations, and governments have incorporated this guidance into their cloud strategies. However, CSA recognizes that a central component of managing risks in cloud computing is **to understand the nature of security threats**.

- **On-line relationships between customers and suppliers**, in particular for ensuring **secure on-line transactions**. This would require a reinforced network and information security policy. Existing regulations are very much dependent upon the service provided online from the supplier to the consumer.
- **Cybercrime and cyber law** issues include threats such as phishing, cracking, cyber terrorism. In France, the accessing or remain fraudulently, in whole or part of a "system of automated data processing" is an offense punishable by two years' imprisonment and a 30,000 euro fine (cp. , s. 323-1, paragraph 1) and any attempt is punishable in the same (cp., art. 323-7).

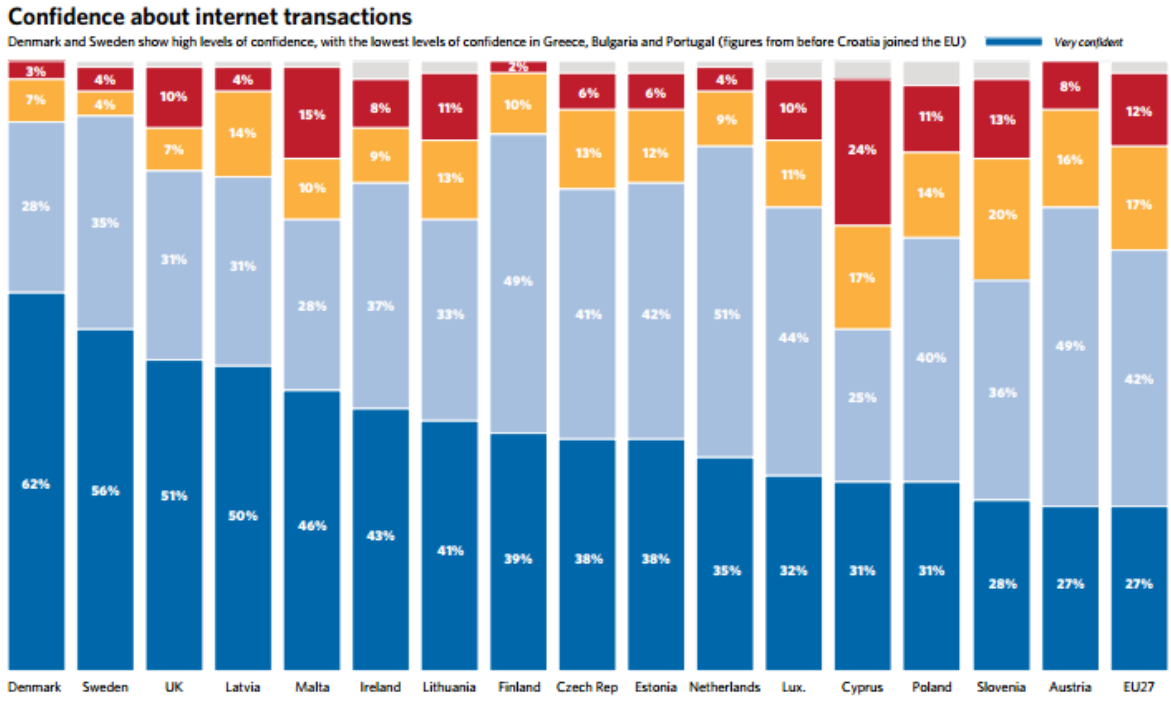

Figure 9: Confidence about Internet Transactions

The situation on EU Cyber Security Strategy is more developed[2]. ENISA and the European Cybercrime Centre (EC3) play key roles.

- **Cisco and Google are seeking to be excluded from a new EU cybersecurity law** that would force them to adopt tough security measures and report serious security breaches to national authorities. The so-called Network and Information Security directive is due to be **finalized in talks between the European Parliament, the European Commission and member states over the coming weeks.**
- **EU lawmakers want the law to cover only sectors that they consider critical**, such as energy, transport and finance. But the Commission and some countries, such as Germany and France, are pushing to **include cloud providers, social networks, search engines and e-commerce platforms because of their widespread use by people and businesses**.

A new EU cybersecurity law that would force them to adopt tough security measures and report serious security breaches to national authorities. The so-called Network and Information Security directive is due to be finalized in talks between the European Parliament, the European Commission and member states over the coming weeks.

- **EU lawmakers want the law to cover only sectors that they consider critical**, such as energy, transport and finance. But the Commission - the EU executive - and some countries, such as Germany and France, are pushing to include cloud providers, social networks, search engines and e-commerce platforms because of their widespread use by people and businesses.
- **Internet companies are firmly opposed to such a move**, which would incur extra compliance costs.

Lack of national coordination can lead to redundant policy and legislation, thereby hindering economic growth and development. The Research produced certain recommendations:

- **Each nation connected to the Internet should have a comprehensive and transparent national cyber strategy** that is integrated and harmonized with the strategies and procedures across all domestic and international policy.
- As each body and organization has a role, it is crucial that the strategies developed incorporate the private and civil sectors, as well as leverage economic and security issues, among other tools, to drive the adoption of initiatives. **The focus on incentives driven by the government** and independent providers should be enhanced.
- Finally, a **competent institution is needed to be responsible for the successful implementation and rollout of the national strategy**. An identifiable, responsible institution will offer transparency to stakeholders in the process. Not having a resource to consult often leads to challenges of ownership, function and action, the research highlighted.

6.5 Third Platform Marketplace: Neutrality, Intellectual Property and Business Models.

In relation to Future Internet, a main issue here is what **the necessary regulatory evolution is to make possible to operate a distributed Future Internet platform across Europe**, with a perspective of an internal market for trusted and secure e-services. **Issues that may potentially be addressed in terms for regulation and policy include the role of core platforms in competition,** access conditions to critical components and

[2] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

interfaces, and business model aspects of exploitation of the core platform. Could such publicly-funded core platforms distort competition? Does it create lock-in conditions?

What they term “Platform Neutrality”, an interesting adaptation of a term usually used in software circles to point to (or away from) lock-in to one or another software “platform” (think Microsoft or SAP). The use of the terminology in fact is similar the Internet (and now mobile) based platforms — Google, Facebook, Twitter, Amazon where similar **issues of cross-platform interoperability, data portability, lock-in/lock-out for users, suppliers, competitors are quite parallel**. Net neutrality enforcement for platforms must do more than just protect consumers’ well-being. It must also protect the well-being of citizens by ensuring that the **Internet’s role as a catalyst for innovation, creation, expression and exchange is not undermined by development strategies that close it off.**

The creation of a third platform marketplace, where several stakeholders need to successfully cooperate while preserving their specificities (in 28 countries), raises potentially critical legal issues at different levels. One crucial aspect regards **intellectual property**. As stated by the European Commission, in our growing knowledge-based economies the protection of intellectual property is important not only for promoting innovation and creativity, but also for developing employment and improving competitiveness (http://ec.europa.eu/internal_market/intellectual-property/). Intellectual property covers two areas: industrial property and copyright.

- **Copyright.** It is important to exercise considerable caution where material is taken from a third party source without permission, as their activities are likely to amount to an infringement of copyright and/or database rights. Copyright infringement will occur if the whole or a substantial part of a copyright work is copied or adapted without the copyright owner's consent.
- **Usage of data.** Data may also be protected by copyright and, additionally or in the alternative, by database rights. Again, this may vary across countries. These aspects should be taken into account when building composite applications.
- **Industrial Property/Patents.** The EU approach is that “a strong industrial property rights system is a driving force for innovation, stimulating R&D investment and facilitating the transfer of knowledge from the laboratory to the marketplace”, (http://ec.europa.eu/internal_market/indprop/rights/index_en.htm). The marketplace and application composition platform should not facilitate IP infringements, quite the opposite. It is therefore important to find a tradeoff between the protection of intellectual property and consumer privacy versus fair-use and the free flow of information through applications.

Another important legal implication comes **from the combination of GEs that follow different business models.**

- **Business models.** As discussed in previous sections, pay-per-use business models have been growing in popularity. When a consumer buys/contracts an application or service; he pays for its usage. Both composite and atomic services must be accounted, rated and charged according to their business model, and each of the service providers must receive their corresponding payment. In other segments, more traditional license-based business models are currently enforced. It may happen that **different types of business models, pay-per-use and license-based, are enforced in the same composite application** because single applications enforce different business models. Therefore, a demanding challenge for enabling the ecosystem of applications is the harmonization of business models, especially within the same composite application**.**

From the above considerations, we can advocate **the need for an EU regulatory framework, which is able to mediate and find suitable legal collaboration patterns between different stakeholders (and their countries**), while avoiding imposing too strict limitations to the characterizing modus operandi of the

marketplace. In fact, it is likely that several issues that are typical of any marketplace (be it digital or in the physical world) would be subject to debate within the EU, in order to find a **viable policy that protects individual rights while encouraging the development of applications in the marketplace**.

Reform of the **current EU framework is urgently needed in order to take account of the new digital context and to introduce more harmonisation across the EU and legal certainty for business**

A first step was, on December, 2012, the European Union sealed an agreement for the creation of a single patent system across 25 countries, bringing to an end decades of argument. The measure aims to boost competitiveness and innovation as it reduces red tape for inventors and brings patent costs in line with other economies like the U.S. and Japan. **The new patent has come into force in 2014,** and a new unified patent court will be set up in Paris with some specialist services located in London and Munich.

If the new **European Commission manages to introduce effective reform, Europe will play a leading role in the global digital economy and be a better place to work and live**.

7 FIWARE Policy Approach

Platforms require a non-traditional business model. New services will be developed in a new value chain and therefore the interaction between a variety of ICT organizations, regulators and sector specific organizations is required. Platform regulation has to overcome a wide number of barriers such as dominance of incumbents, protectionism and entry or interoperation barriers. **Main regulatory concerns from FIWARE include identity and privacy, business data integrity in relation to cloud computing, data protection, open data, security, and copyright**. The message is that traditional regulatory analysis seems not to be sufficiently equipped to deal with platforms as different aspects of openness has to be dealt with (who can use it; who can offer compatible app; who can bundle it with larger platform; who can change the design etc.) and a number of issues have to be **dealt with such as customer lock-in, lock in of service providers, through open standards and business models among different stakeholders** The current situation at EU level is that Europe seems to move towards platform regulation in general.

In this post Snowden era, **cloud environments are under particular scrutiny** and governments are seeking a new balance between privacy protections – wherever data is located – and powers of data access to secure homeland defence. **Europe is rising to the challenge**, with initiatives to both reassure citizens and create conditions for a secure and **successful future cloud industry.**

First of all, we must be clear: the cost and operational benefits of cloud are immensely compelling today. And they will grow in importance with the massive volumes of data we can expect to store and manage in future. **So trust is imperative if we want to take advantage of the personal and business opportunities** that cloud represent for us all.

Successful FIWARE exploitation and business creation is dependent on access to data. These data are of different types. First, data include public data (such as geographical, environmental, traffic, scientific, etc. data) that should be accessible to enable FIWARE applications to make use of them and / or build new applications on basis of these data. **Open data is widely considered as having a lot of potential in this respect.** Conditions under which data are made available for use, however, are still **significantly different across states or regions thus hindering their exploitation**. Another type of data is personal data, which can be very important for business. However exploiting **personal data has a strong link to privacy and data protection; all existing rules must be obeyed.**

Legal barriers can arise in a number of areas, each of which have clear privacy and trust implications, as will be commented on in the sections below. Additionally, a classification of policies and regulations would be helpful as a basis for systematic analysis of approaches to policy and regulation. **It would be recommended to establish relations with external stakeholders in the fields of policy and regulation** (European Parliament, ITU, OECD and other) **and with relevant Commission Directorates and the Digital Agenda initiatives.**

Policy / Regulatory concern	Why is this relevant for FIWARE? or how does this affect FIWARE?	Policy Approach Required and Main Steps taken do far
The need to support an efficient EU wide single market for cloud services	**The European cloud market is currently confronted with a significant number of regulatory and market access barriers** that impede both development and commercial exploitation by cloud providers and adoption by cloud users, especially for cross border use cases. **Some of these regulatory and market**	• A framework, for defining best practice and cloud requirements, linking them to use cases, and applying them in practice, is required • The Steering Board of the European Cloud Partnership (ECP), an advisory body to the European Commission,

	access barriers are linked to legal issues, whereas others are principally tied to trust concerns, technical control, or operational requirements. - The lack of full EU harmonization of data protection rules is a recurring legal barrier. - Even outside of formal laws, norms may exist (issued by supervisors, regulators, sector organizations etc.) which stop or **discourage the use of cloud services outside national borders**. - **Cloud adoption barriers can vary from sector to sector**. Legacy legal frameworks that are not adapted to the global market can cause legal challenges, and operational/business concerns may lead to a strong preference for private clouds	presented its vision for Trusted Cloud Europe in the form of a Report in March 2014. Specific recommendations include: ○ Creation of a common framework of legal, operational and technical best practices ○ Review of formal data location requirements (that currently still divide cloud architectures up by national jurisdiction) with the aim of replacing them by functional requirements to ensure the same data accessibility and security ○ Encouraging public bodies to consider cloud computing when procuring IT systems
Relevance of Privacy and Data Protection in the Future Internet	The use of personal data is often highly relevant for business purposes, e.g. in communication, content and energy markets but also in healthcare, public security and other public domains. Privacy is an important issue in relation to the processing of log files containing personal data, or in using other sources of personal data. This may be subject to **prior authorization, according to national laws.** Sensible data of citizens will have to be stored and processed fulfilling security, integrity and accessibility rules as established by legal and regular frameworks. **Stricter privacy regulation, such as offered by the recent EU privacy regulation, would help to promote the use and adaption of privacy-enhancing technologies.** Whether your organization is based in Europe, you have branch offices in Europe, or you provide services to European residents, there are a wide **range of privacy and cross-border data residency regulations that can impact your IT footprint.** **The EU, which has some of the strictest data protection legislation** in the world, is in the process of revising its rules, **which date back to 1995.**The rules **require prior consent from users** before data can be collected and strict rules on subsequent uses of that data. A fundamental element of the legislation is the	• Europe has a comprehensive set on regulation that is not yet fully tuned towards the developments of Big Data. Yet discussions are under way to update regulations such as for "data protection" and "access to public data". **The General Data Protection Regulation proposal - currently under negotiatio**n - aims to address important privacy aspects stemming out from latest technology developments (including social media and cloud computing), and provide for harmonization of regulations throughout the EU. • **The new PSI directive is currently in the negotiation phase**. The update of the 2003 PSI Directive has the objective to reach a Europe-wide consensus in **making PSI readily available,** which would help bridge the current gap between member states' levels of openness regarding non-personal data that is produced, stored, or harvested by the public sector. • In a joint declaration, adopted with an overwhelming majority, the representatives of the 16 parliaments (Germany, Austria, Belgium, Croatia, France, Greece, Hungary, Lithuania,

	right to be forgotten where users can ask to delete information held about them unless there is a public interest for that information to remain in the public domain	Luxembourg, the Netherlands, Portugal, the Czech Republic, Romania, the United Kingdom, Slovakia and Sweden) called on **European legislators to adopt the legislative package on the reform personal data protection "by 2015**
Internet of Things and personal location data	A relatively new area concerning data protection is Internet of Things, where, given the dominance of key players, **data property is a major concern that could also highlight serious gaps across European countries** depending how national regulation processes would support the deployment of new technologies. As soon **as cross-applications between several usage areas** would appear, privacy and risk management would become the most important topic which could aim to a major risk for Internet of Things: stop the development **E112 rules in Europe will enforce the need of precise positioning provided by Location Platforms**. It is a key enabler for citizen safety by helping emergency services to precisely locate an end-user using its mobile terminal.	• European Legal Framework guaranteeing privacy harmonized across Europe • The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive which regulates the processing of personal data within the European Union. **This directive could be used or revised to include Internet of Things subject** but in the opposite, European Union should be flexible to avoid any breakthrough with regulation on this topic in other areas around the world
One crucial aspect regards **Intellectual** Property/Patents	Regarding the intellectual property there are two European policy requirements to address: - **Protection of the intellectual property of app developers** to ensure that they are prepared to invest in risky new ventures, and to foster an environment conducive to innovation, creativity and consumer trust. - **Copyright, trademarks and patents ought to apply throughout Europe on a common basis.** Application developers need ways of utilizing and paying for content rights throughout Europe without having to incur costs in agreeing rights on a country-by-country basis	• The EU approach is that "a strong industrial property rights system is a driving force for innovation and that the marketplace and application composition platform **should not facilitate IP infringements**, quite the opposite. It is therefore important to find a **tradeoff between the protection of intellectual property and consumer privacy** versus fair-use and the **free flow of information through applications**. • Regarding **patent harmonization,** a first step was, on December, 2012, the European Union sealed an agreement for the creation of a single **patent system across 25 countries**, bringing to an end decades of

		argument. The measure aims to boost competitiveness and innovation as it reduces red tape for inventors and brings patent costs in line with other economies like the U.S. and Japan. **The new patent has come into force in 2014**, and a new unified patent court will be set up in Paris with some specialist services located in London and Munich.
Implementation of **Open Data policies**.	For the public domain, **the specific category of open data** has received a lot of interest; both top down from the policy stakeholders at EU and national levels and bottom up from innovators and entrepreneurs. However there still remain several barriers to implementation of open data policies, related to the **different access models, authorization of use, data release approaches, harmonized licensing models and other**. **Advancements in the area of "access to public data" will include amongst others the creation of a genuine right to re-use public information** (libraries, museums and archives and making data available in machine-readable and open formats. Well-established **conditions for easy access to Open Data** will be most relevant for exploitation of FIWARE and to stimulate innovation and entrepreneurship	• Reviewing the Directive on Re-Use of Public Sector Information, notably its scope and principles on charging for access and use" should give impetus to the developments in the chapter "Data/Context Management" in which the availability of advanced platform functionalities dealing with gathering, processing • **The revised EU Directive on re-use of public sector information (2013**) is now seen as a good framework for minimum **harmonization of national practices and regulations on the reuse of public sector data**, consistent with the relevant access regime; further harmonization may be considered leading to increasing data sharing and improved service delivery and also **European standard license model** would be helpful to align the different licensing models maximizing the potential of using datasets from different data-owners .
Cybercrime	**Combating Cybercrime is considered important in order to build and maintain consumer trust.** Cybercrime also incurs costs for consumers and businesses who feel the need to protect themselves. It is evident that **cybercrime causes overall barriers-to-entry in the digital market** More needs are to be done to ensure effective **cooperation between EU States' authorities**, in particular on preventing cybercrime. FIWARE and European industrial enterprises must to develop cyber security solutions and to	• **Propose EU cyber-security strategy and Directive:** Security and freedom online go hand-in-hand. The EU should offer the world's safest online environments, valuing user freedom and privacy. The Commission will deliver a strategy and proposed Directive to establish a common minimum level of preparedness at national level, including an online platform to prevent and counter cross-border cyber incidents, and incident

	promote interconnections between Cyber Operational Centres FI infrastructure operators must find ways to defend their infrastructure from malicious attacks and to ensure legitimate users will not be harmed if they use the infrastructure (i.e. to make the infrastructure secure and trustworthy).	reporting requirements. This will **stimulate a larger European market for security and privacy-by-design products**

Table 3: FIWARE Policy Approach Consolidation.

Currently there are various different national privacy rules; even worse, they are continuously changing. But we need harmonized privacy rules in Europe at least for the large players like France, Germany, Spain and Italy. It is important **to create sufficient trust for the users** in that there are satisfactory privacy mechanisms for the users to feel comfortable with their privacy. Infrastructure / General Enablers /Use Case owners have to publish their privacy policy and services. Privacy should include the right for users to erase their personal data completely.

The main challenge related to policy/regulation is probably to adhere to existing privacy laws and regulations. As regards the current EU situation, there was a speech by Viviane Reding (EU Justice Commissioner) about the **EU's Data Protection rules and Cyber Security Strategy**, and how they hang together[3]. Data protection rules are still based on a document of 1995 (Reding criticized it for having many national differences). The Commission proposes a reform of the data protection rules[4]. The situation on EU Cyber Security Strategy is more developed[5]. ENISA and the European Cybercrime Centre (EC3) play key roles. Article 29 data Protection Working Party[6] comes probably closest to the state of the art in European data protection work.

In this era of personal data economy, **where personalization and the individualization of services becomes a key winning strategy,** consumers are more aware of their digital footprint and the way in which their data is used. Consumers increasingly face a choice about where and with whom to leave their data.

Rethinking is needed about where strategies should support a portfolio that focuses on services that put the privacy needs of the client at its core. This could also be determining factor in creating **added value for the EU operators versus OTT players** who have already built up a less than favorable reputation when it comes to respect to privacy.

So it is necessary to ensure that consumers can **completely trust that their data** is not going to fall into the wrong hands. **Cyber-security, data sovereignty and consistent procurement processes are among the**

[3] http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm#PR_metaPressRelease_bottom

[4] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[5] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[6] http://ec.europa.eu/justice/data-protection/article-29/

issues holding back wider adoption of cloud computing and services, according to a survey on the Trusted Cloud Europe.

The Trusted Cloud Europe framework aims to support a single market for cloud computing in Europe based on a common understanding of best practices which will enable Europe to become **a trusted leader in cloud computing, as both a provider and user of cloud services**. Examples of expected convergences and alignment opportunities include notably the following:

- **Accelerate cloud computing through public sector buying power:** The Commission will launch pilot actions in the European Cloud Partnership (IP/12/1225), which harnesses public buying power to help create the world's largest cloud-enabled ICT market, dismantling current national fortresses and negative consumer perceptions. **Alignment of procurement rules and practices:** Procurement rules in some Member States can make it difficult to sell cloud solutions to the public sector. This is burdensome to public administrations, which can be barred from technologically and economically advantageous solutions, but also for cloud providers, who are faced with different requirements from country to country. By sharing best practices, Member States can **ensure that their procurement legislation and policies will become cloud enabled**. Furthermore, they could **work towards developing common approaches to public procurement of cloud computing, or towards the mutual recognition of any existing national accreditation schemes,** so that providers do not need to seek different certifications, accreditations or approvals in different Member States. Similarly, Member States can **share effective national budgeting policies to ensure that pay-as-you go models** (moving from capex to opex) can be enabled.
- **Reduction of data location restrictions:** Member State practices and in some instances national laws restrict the possibility of storage and processing of certain data (especially public sector data) outside their territory. If common requirements can be found for similar use cases, **Member States can choose to gradually phase out data location restrictions when they are deemed unnecessary.** This does not imply that data controls should be abandoned; it is often possible and advisable to **replace formal legal requirements** (such as geographic location of the data) **by the corresponding functional requirements** (such as ensuring the accessibility and security of the data). State-of-the art security technologies could be regarded for some use cases as an alternative to data location restriction. This goal oriented approach 12 In some cases, Member States have opted for 'cloud first' policies, which sometimes include stronger support for cloud technologies, e.g. by requiring procurers to prioritize cloud computing purchases where possible, or to justify any decision not to use cloud computing when a suitable cloud solution was available.
- **Propose EU cyber-security strategy and Directive:** Security and freedom online go hand-in-hand. The EU should offer the world's safest online environments, valuing user freedom and privacy. The Commission will deliver a strategy and proposed Directive to establish a common minimum level of preparedness at national level, including an online platform to prevent and counter cross-border cyber incidents, and incident reporting requirements. This will stimulate a larger European market for security and privacy-by-design products.
- **Update EU's Copyright Framework:** Modernizing copyright is key to achieving this Digital Single Market. Therefore the Commission will seek a solution of copyright-related issues where rapid progress is needed via a structured stakeholder dialogue in 2013. In parallel the Commission will complete its on-going effort to review and the modernize the EU copyright legislative framework, with a view to a decision in 2014 on whether to table resulting legislative reform proposals (see MEMO/12/950).

From a European perspective, there is the dual risk that excessively restrictive regulations can place European cloud service providers at a clear competitive disadvantage in relation to their non-European

counterparts, and inversely that overly flexible rules could result in serious harm to end users. Ambiguities in the law should at any rate be identified and addressed to ensure that the legal **status of cloud computing services and the rights and obligations of each of the stakeholders is clear, especially when dealing with security and privacy concerns.**

Thanks to the open nature of FIWARE specifications, cities and other adopters will be able to avoid vendor lock-in. **FIWARE developers will be able to port their applications across different instances of the FIWARE platform,** supported by different FIWARE providers. Decisions to choose a given FIWARE provider will be driven, **not only based on costs, but also trust**, e.g. regarding the environment where applications or where data will be hosted. This is particularly relevant when data (e.g. those affecting personal information) have to comply with **certain regulations or has to cope with some security and privacy requirements.**

8 Conclusions

The key to success in the **Future Internet will be to identify value propositions that attract consumers for profitable (or at least sustainable) services**, where current business, operational or technical barriers can be overcome through the use of Future Internet technology. Overcoming barriers should enable value propositions that are novel and hence more attractive that existing 'current Internet' services. One of the most important considerations is therefore to identify how FIWARE participants will distinguish themselves from current Internet businesses and services, and **what technical capabilities and regulatory and policy challenges they need to overcome barriers to achieving this**

FIWARE aims to achieve a great impact on the Internet community, mainly targeting third party developers and companies willing to exploit its Future Internet core-platform. The experiments and use trials, and the **involvement of European cities, Industry, as potential ecosystems, –and other communities (SMEs, entrepreneurs...)** in the experiments will be crucial**.** Since **SMEs, web developers and other ICT companies are important for the purpose of creating the developers community around FIWARE GE**. As it was anticipated in the strategy, FIWARE will need the experience, contact and **involvement of other associations that can act as interface to a big base of potential users/clients**. These organizations will have additional elements of value to present to their communities, and FIWARE will get access to them, resulting in a win-win situation

Platforms require a non-traditional business model. New services will be developed in a new value chain and therefore the interaction between a variety of ICT organizations, regulators and sector specific organizations is required. Platform regulation has to overcome a wide number of barriers such as dominance of incumbents, protectionism and entry or interoperation barriers. **Main regulatory concerns from FIWARE include identity and privacy, business data integrity in relation to cloud computing, data protection, open data, security, and copyright**. The message is that traditional regulatory analysis seems not to be sufficiently equipped to deal with platforms as different aspects of openness has to be dealt with (who can use it; who can offer compatible app; who can bundle it with larger platform; who can change the design etc.) and a number of issues have to be **dealt with such as customer lock-in, lock in of service providers, through open standards and business models among different stakeholders**.

Europe needs to develop a truly connected digital single market, including through swift and ambitious legislative steps in the areas of data protection, telecoms regulation and by modernising and simplifying copyright and consumer rules for online and digital purchases. **The digital single market should address trust and security of online transactions,** interoperability of different technological solutions and access to digital resources and infrastructures (in particular spectrum licencing policies).

The scope of the reforms expanded rapidly following the scandal surrounding the US cyber espionage programme, Prism. The American National Security Agency (NSA) was receiving information from large internet companies about their European customers.

If trust is not rebuilt, businesses will not be able to develop the huge potential of the digital economy. The European Court had to step in and take a stance **because Europe lacks modern data protection rules that are fit for the Internet age.** The Heads of State and Government have repeatedly affirmed the importance of adopting 'a strong EU General Data Protection framework by 2015'.

Europe is readying implementation of data protection reforms aimed at harmonizing data privacy and security laws for all 28 member states. **Given the inherently borderless nature of cloud computing**, it's more important than ever to ensure robust legal frameworks and critically, bodies capable of enforcing appropriate data management through fines and other measures.

Successful FIWARE exploitation and business creation is dependent on access to data. These data are of different types. First, data include public data (such as geographical, environmental, traffic, scientific, etc. data) that should be accessible to enable FIWARE applications to make use of them and / or build new applications on basis of these data. **Open data is widely considered as having a lot of potential in this respect.** Conditions under which data are made available for use, however, are still **significantly different across states or regions thus hindering their exploitation**. Another type of data is personal data, which can be very important for business. However exploiting **personal data has a strong link to privacy and data protection; all existing rules must be obeyed.**

Thanks to the open nature of FIWARE specifications, cities and other adopters will be able to avoid vendor lock-in. **FIWARE developers will be able to port their applications across different instances of the FIWARE platform,** supported by different FIWARE providers. Decisions to choose a given FIWARE provider will be driven, **not only based on costs, but also trust**, e.g. regarding the environment where applications or where data will be hosted. This is particularly relevant when data (e.g. those affecting personal information) have to comply with **certain regulations or has to cope with some security and privacy requirements.**

9 References

[ETNO] 12 March 2014 , https://www.etno.eu/home/press-corner/etno-press-releases/2014/270

[Cloud] Why the incoming EU data regulations represent a major opportunity for cloud providers 14th Oct 2014

[Atos- Cloud] Should I put my trust in the cloud? February 9th, 2015 Kay Hooghoudt

[Atos-Trust] Trust and transparency are cloud critical…and Europe's got the message. February 5th, 2015 Kay Hooghoudt

[Reding] http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm#PR_metaPressRelease_bottom

[Data] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[Cyber Security] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[Data Protection] http://ec.europa.eu/justice/data-protection/article-29/

[Open Data] Cap Gemini Consulting: The Open Data Economy – Unlocking Economic Value by Opening Government and Public Data (2013)

[Security] Cloud Security Strategy work 2014. Dr.Marnix Dekker. EU Network and Information Security Agency (ENISA) @ ENISA Cloud Security Expert group, November 11th2014

[Neutrality] Platform Neutrality Building an open and sustainable digital environment. Conseil National du numerique. May 2014

[Digital Single Market] Priorities towards a Digital Single Market in the Baltic Sea Region

[GDPR] AIIM white paper on the European General Data Protection Regulations. Mike Davis

[Digital Agenda] Digital Agenda for Europe http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[Europe 2020] http://ec.europa.eu/europe2020/reaching-the-goals/flagship-initiatives/index_en.htm

[Business Model] Ballon, P. (2007b) "Editorial: The Redesign of Mobile Business Models", info: The Journal of Policy Regulation and Strategy for Telecommunications, Information and Media, August 2007, 6-9.

[Platform Rules] Boudreau, K. & A. Hagiu (2009) "Platform Rules: Multi-Sided Platforms as Regulators", in: Gawer, A. (ed.) (2009) Platforms, Markets and Innovation. Cheltenham, UK and Northampton, US: Edward Elgar.

[Policies] Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age", Harvard Journal of Law & Technology, Vol. 17, 1, Fall 2003

[CONCORD] Future Internet PPP: Exploring Policy and Regulatory Challenges- Working Paper – FI-PPP Working Group on Policy, Regulation and Governance. CONCORD